

A B S T R A C T

A L G E B R A

THIRD EDITION

DAVID S. DUMMIT

RICHARD M. FOOTE

*Dedicated to our families
especially
Janice, Evan, and Krysta
and
Zsuzsanna, Peter, Karoline, and Alexandra*

Frequently Used Notation

$f^{-1}(A)$	the inverse image or preimage of A under f
$a \mid b$	a divides b
(a, b)	the greatest common divisor of a, b also the ideal generated by a, b
$ A , x $	the order of the set A , the order of the element x
\mathbb{Z}, \mathbb{Z}^+	the integers, the positive integers
\mathbb{Q}, \mathbb{Q}^+	the rational numbers, the positive rational numbers
\mathbb{R}, \mathbb{R}^+	the real numbers, the positive real numbers
$\mathbb{C}, \mathbb{C}^\times$	the complex numbers, the nonzero complex numbers
$\mathbb{Z}/n\mathbb{Z}$	the integers modulo n
$(\mathbb{Z}/n\mathbb{Z})^\times$	the (multiplicative group of) invertible integers modulo n
$A \times B$	the direct or Cartesian product of A and B
$H \leq G$	H is a subgroup of G
Z_n	the cyclic group of order n
D_{2n}	the dihedral group of order $2n$
S_n, S_Ω	the symmetric group on n letters, and on the set Ω
A_n	the alternating group on n letters
Q_8	the quaternion group of order 8
V_4	the Klein 4-group
\mathbb{F}_N	the finite field of N elements
$GL_n(F), GL(V)$	the general linear groups
$SL_n(F)$	the special linear group
$A \cong B$	A is isomorphic to B
$C_G(A), N_G(A)$	the centralizer, and normalizer in G of A
$Z(G)$	the center of the group G
G_s	the stabilizer in the group G of s
$\langle A \rangle, \langle x \rangle$	the group generated by the set A , and by the element x
$G = \langle \dots \dots \rangle$	generators and relations (a presentation) for G
$\ker \varphi, \text{im } \varphi$	the kernel, and the image of the homomorphism φ
$N \trianglelefteq G$	N is a normal subgroup of G
gH, Hg	the left coset, and right coset of H with coset representative g
$ G : H $	the index of the subgroup H in the group G
$\text{Aut}(G)$	the automorphism group of the group G
$Syl_p(G)$	the set of Sylow p -subgroups of G
n_p	the number of Sylow p -subgroups of G
$[x, y]$	the commutator of x, y
$H \rtimes K$	the semidirect product of H and K
\mathbb{H}	the real Hamilton Quaternions
R^\times	the multiplicative group of units of the ring R
$R[x], R[x_1, \dots, x_n]$	polynomials in x , and in x_1, \dots, x_n with coefficients in R
RG, FG	the group ring of the group G over the ring R , and over the field F
\mathcal{O}_K	the ring of integers in the number field K
$\varprojlim A_i, \varinjlim A_i$	the direct, and the inverse limit of the family of groups A_i
$\mathbb{Z}_p, \mathbb{Q}_p$	the p -adic integers, and the p -adic rationals
$A \oplus B$	the direct sum of A and B

$LT(f)$, $LT(I)$	the leading term of the polynomial f , the ideal of leading terms
$M_n(R)$, $M_{n \times m}(R)$	the $n \times n$, and the $n \times m$ matrices over R
$M_{\mathcal{B}}^{\mathcal{E}}(\varphi)$	the matrix of the linear transformation φ with respect to bases \mathcal{B} (domain) and \mathcal{E} (range)
$\text{tr}(A)$	the trace of the matrix A
$\text{Hom}_R(A, B)$	the R -module homomorphisms from A to B
$\text{End}(M)$	the endomorphism ring of the module M
$\text{Tor}(M)$	the torsion submodule of M
$\text{Ann}(M)$	the annihilator of the module M
$M \otimes_R N$	the tensor product of modules M and N over R
$\mathcal{T}^k(M)$, $\mathcal{T}(M)$	the k^{th} tensor power, and the tensor algebra of M
$\mathcal{S}^k(M)$, $\mathcal{S}(M)$	the k^{th} symmetric power, and the symmetric algebra of M
$\bigwedge^k(M)$, $\bigwedge(M)$	the k^{th} exterior power, and the exterior algebra of M
$m_T(x)$, $c_T(x)$	the minimal, and characteristic polynomial of T
$\text{ch}(F)$	the characteristic of the field F
K/F	the field K is an extension of the field F
$[K : F]$	the degree of the field extension K/F
$F(\alpha)$, $F(\alpha, \beta)$, etc.	the field generated over F by α or α, β , etc.
$m_{\alpha, F}(x)$	the minimal polynomial of α over the field F
$\text{Aut}(K)$	the group of automorphisms of a field K
$\text{Aut}(K/F)$	the group of automorphisms of a field K fixing the field F
$\text{Gal}(K/F)$	the Galois group of the extension K/F
\mathbb{A}^n	affine n -space
$k[\mathbb{A}^n]$, $k[V]$	the coordinate ring of \mathbb{A}^n , and of the affine algebraic set V
$\mathcal{Z}(I)$, $\mathcal{Z}(f)$	the locus or zero set of I , the locus of an element f
$\mathcal{I}(A)$	the ideal of functions that vanish on A
$\text{rad } I$	the radical of the ideal I
$\text{Ass}_R(M)$	the associated primes for the module M
$\text{Supp}(M)$	the support of the module M
$D^{-1}R$	the ring of fractions (localization) of R with respect to D
R_P, R_f	the localization of R at the prime ideal P , and at the element f
$\mathcal{O}_{v, V}, \mathbb{T}_{v, V}$	the local ring, and the tangent space of the variety V at the point v
$\mathfrak{m}_{v, V}$	the unique maximal ideal of $\mathcal{O}_{v, V}$
$\text{Spec } R$, $\text{mSpec } R$	the prime spectrum, and the maximal spectrum of R
\mathcal{O}_X	the structure sheaf of $X = \text{Spec } R$
$\mathcal{O}(U)$	the ring of sections on an open set U in $\text{Spec } R$
\mathcal{O}_P	the stalk of the structure sheaf at P
$\text{Jac } R$	the Jacobson radical of the ring R
$\text{Ext}_R^n(A, B)$	the n^{th} cohomology group derived from Hom_R
$\text{Tor}_n^R(A, B)$	the n^{th} cohomology group derived from the tensor product over R
A^G	the fixed points of G acting on the G -module A
$H^n(G, A)$	the n^{th} cohomology group of G with coefficients in A
Res , Cor	the restriction, and corestriction maps on cohomology
$\text{Stab}(1 \trianglelefteq A \trianglelefteq G)$	the stability group of the series $1 \trianglelefteq A \trianglelefteq G$
$ \theta $	the norm of the character θ
$\text{Ind}_H^G(\psi)$	the character of the representation ψ induced from H to G

ABSTRACT ALGEBRA

Third Edition

David S. Dummit
University of Vermont

Richard M. Foote
University of Vermont



John Wiley & Sons, Inc.

ASSOCIATE PUBLISHER	Laurie Rosatone
ASSISTANT EDITOR	Jennifer Battista
FREELANCE DEVELOPMENTAL EDITOR	Anne Scanlan-Rohrer
SENIOR MARKETING MANAGER	Julie Z. Lindstrom
SENIOR PRODUCTION EDITOR	Ken Santor
COVER DESIGNER	Michael Jung

This book was typeset using the Y&Y TeX System with DVIWindo. The text was set in Times Roman using *MathTime* from Y&Y, Inc. Titles were set in OceanSans. This book was printed by Malloy Inc. and the cover was printed by Phoenix Color Corporation.

This book is printed on acid-free paper.

Copyright © 2004 John Wiley and Sons, Inc. All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, (508) 750-8400, fax (508) 750-4470. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201)748-6011, fax (201)748-6008, E-mail: PERMREQ@WILEY.COM.

To order books or for customer service please call 1-800-CALL WILEY (225-5945).

ISBN 0-471-43334-9

WIE 0-471-45234-3

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

*Dedicated to our families
especially
Janice, Evan, and Krysta
and
Zsuzsanna, Peter, Karoline, and Alexandra*

Contents

Preface xi

Preliminaries 1

- 0.1 Basics 1
- 0.2 Properties of the Integers 4
- 0.3 $\mathbb{Z}/n\mathbb{Z}$: The Integers Modulo n 8

Part I – GROUP THEORY 13

Chapter 1 Introduction to Groups 16

- 1.1 Basic Axioms and Examples 16
- 1.2 Dihedral Groups 23
- 1.3 Symmetric Groups 29
- 1.4 Matrix Groups 34
- 1.5 The Quaternion Group 36
- 1.6 Homomorphisms and Isomorphisms 36
- 1.7 Group Actions 41

Chapter 2 Subgroups 46

- 2.1 Definition and Examples 46
- 2.2 Centralizers and Normalizers, Stabilizers and Kernels 49
- 2.3 Cyclic Groups and Cyclic Subgroups 54
- 2.4 Subgroups Generated by Subsets of a Group 61
- 2.5 The Lattice of Subgroups of a Group 66

Chapter 3	Quotient Groups and Homomorphisms	73
3.1	Definitions and Examples	73
3.2	More on Cosets and Lagrange's Theorem	89
3.3	The Isomorphism Theorems	97
3.4	Composition Series and the Hölder Program	101
3.5	Transpositions and the Alternating Group	106

Chapter 4	Group Actions	112
4.1	Group Actions and Permutation Representations	112
4.2	Groups Acting on Themselves by Left Multiplication—Cayley's Theorem	118
4.3	Groups Acting on Themselves by Conjugation—The Class Equation	122
4.4	Automorphisms	133
4.5	The Sylow Theorems	139
4.6	The Simplicity of A_n	149

Chapter 5	Direct and Semidirect Products and Abelian Groups	152
5.1	Direct Products	152
5.2	The Fundamental Theorem of Finitely Generated Abelian Groups	158
5.3	Table of Groups of Small Order	167
5.4	Recognizing Direct Products	169
5.5	Semidirect Products	175

Chapter 6	Further Topics in Group Theory	188
6.1	p -groups, Nilpotent Groups, and Solvable Groups	188
6.2	Applications in Groups of Medium Order	201
6.3	A Word on Free Groups	215

Part II – RING THEORY 222

Chapter 7	Introduction to Rings	223
7.1	Basic Definitions and Examples	223
7.2	Examples: Polynomial Rings, Matrix Rings, and Group Rings	233
7.3	Ring Homomorphisms and Quotient Rings	239
7.4	Properties of Ideals	251
7.5	Rings of Fractions	260
7.6	The Chinese Remainder Theorem	265

Chapter 8 Euclidean Domains, Principal Ideal Domains and Unique Factorization Domains 270

- 8.1 Euclidean Domains 270
- 8.2 Principal Ideal Domains (P.I.D.s) 279
- 8.3 Unique Factorization Domains (U.F.D.s) 283

Chapter 9 Polynomial Rings 295

- 9.1 Definitions and Basic Properties 295
- 9.2 Polynomial Rings over Fields I 299
- 9.3 Polynomial Rings that are Unique Factorization Domains 303
- 9.4 Irreducibility Criteria 307
- 9.5 Polynomial Rings over Fields II 313
- 9.6 Polynomials in Several Variables over a Field and Gröbner Bases 315

Part III – MODULES AND VECTOR SPACES 336

Chapter 10 Introduction to Module Theory 337

- 10.1 Basic Definitions and Examples 337
- 10.2 Quotient Modules and Module Homomorphisms 345
- 10.3 Generation of Modules, Direct Sums, and Free Modules 351
- 10.4 Tensor Products of Modules 359
- 10.5 Exact Sequences—Projective, Injective, and Flat Modules 378

Chapter 11 Vector Spaces 408

- 11.1 Definitions and Basic Theory 408
- 11.2 The Matrix of a Linear Transformation 415
- 11.3 Dual Vector Spaces 431
- 11.4 Determinants 435
- 11.5 Tensor Algebras, Symmetric and Exterior Algebras 441

Chapter 12 Modules over Principal Ideal Domains 456

- 12.1 The Basic Theory 458
- 12.2 The Rational Canonical Form 472
- 12.3 The Jordan Canonical Form 491

Chapter 13 Field Theory 510

- 13.1 Basic Theory of Field Extensions 510
- 13.2 Algebraic Extensions 520
- 13.3 Classical Straightedge and Compass Constructions 531
- 13.4 Splitting Fields and Algebraic Closures 536
- 13.5 Separable and Inseparable Extensions 545
- 13.6 Cyclotomic Polynomials and Extensions 552

Chapter 14 Galois Theory 558

- 14.1 Basic Definitions 558
- 14.2 The Fundamental Theorem of Galois Theory 567
- 14.3 Finite Fields 585
- 14.4 Composite Extensions and Simple Extensions 591
- 14.5 Cyclotomic Extensions and Abelian Extensions over \mathbb{Q} 596
- 14.6 Galois Groups of Polynomials 606
- 14.7 Solvable and Radical Extensions: Insolvability of the Quintic 625
- 14.8 Computation of Galois Groups over \mathbb{Q} 640
- 14.9 Transcendental Extensions, Inseparable Extensions, Infinite Galois Groups 645

**Part V – AN INTRODUCTION TO COMMUTATIVE RINGS,
ALGEBRAIC GEOMETRY, AND
HOMOLOGICAL ALGEBRA 655**

Chapter 15 Commutative Rings and Algebraic Geometry 656

- 15.1 Noetherian Rings and Affine Algebraic Sets 656
- 15.2 Radicals and Affine Varieties 673
- 15.3 Integral Extensions and Hilbert's Nullstellensatz 691
- 15.4 Localization 706
- 15.5 The Prime Spectrum of a Ring 731

**Chapter 16 Artinian Rings, Discrete Valuation Rings, and
Dedekind Domains 750**

- 16.1 Artinian Rings 750
- 16.2 Discrete Valuation Rings 755
- 16.3 Dedekind Domains 764

Chapter 17 Introduction to Homological Algebra and Group Cohomology 776

- 17.1 Introduction to Homological Algebra—Ext and Tor 777
- 17.2 The Cohomology of Groups 798
- 17.3 Crossed Homomorphisms and $H^1(G, A)$ 814
- 17.4 Group Extensions, Factor Sets and $H^2(G, A)$ 824

Part VI – INTRODUCTION TO THE REPRESENTATION THEORY OF FINITE GROUPS 839

Chapter 18 Representation Theory and Character Theory 840

- 18.1 Linear Actions and Modules over Group Rings 840
- 18.2 Wedderburn's Theorem and Some Consequences 854
- 18.3 Character Theory and the Orthogonality Relations 864

Chapter 19 Examples and Applications of Character Theory 880

- 19.1 Characters of Groups of Small Order 880
- 19.2 Theorems of Burnside and Hall 886
- 19.3 Introduction to the Theory of Induced Characters 892

Appendix I: Cartesian Products and Zorn's Lemma 905

Appendix II: Category Theory 911

Index 919

Preface to the Third Edition

The principal change from the second edition is the addition of Gröbner bases to this edition. The basic theory is introduced in a new Section 9.6. Applications to solving systems of polynomial equations (elimination theory) appear at the end of this section, rounding it out as a self-contained foundation in the topic. Additional applications and examples are then woven into the treatment of affine algebraic sets and k -algebra homomorphisms in Chapter 15. Although the theory in the latter chapter remains independent of Gröbner bases, the new applications, examples and computational techniques significantly enhance the development, and we recommend that Section 9.6 be read either as a segue to or in parallel with Chapter 15. A wealth of exercises involving Gröbner bases, both computational and theoretical in nature, have been added in Section 9.6 and Chapter 15. Preliminary exercises on Gröbner bases can (and should, as an aid to understanding the algorithms) be done by hand, but more extensive computations, and in particular most of the use of Gröbner bases in the exercises in Chapter 15, will likely require computer assisted computation.

Other changes include a streamlining of the classification of simple groups of order 168 (Section 6.2), with the addition of a uniqueness proof via the projective plane of order 2. Some other proofs or portions of the text have been revised slightly. A number of new exercises have been added throughout the book, primarily at the ends of sections in order to preserve as much as possible the numbering schemes of earlier editions. In particular, exercises have been added on free modules over noncommutative rings (10.3), on Krull dimension (15.3), and on flat modules (10.5 and 17.1).

As with previous editions, the text contains substantially more than can normally be covered in a one year course. A basic introductory (one year) course should probably include Part I up through Section 5.3, Part II through Section 9.5, Sections 10.1, 10.2, 10.3, 11.1, 11.2 and Part IV. Chapter 12 should also be covered, either before or after Part IV. Additional topics from Chapters 5, 6, 9, 10 and 11 may be interspersed in such a course, or covered at the end as time permits.

Sections 10.4 and 10.5 are at a slightly higher level of difficulty than the initial sections of Chapter 10, and can be deferred on a first reading for those following the text sequentially. The latter section on properties of exact sequences, although quite long, maintains coherence through a parallel treatment of three basic functors in respective subsections.

Beyond the core material, the third edition provides significant flexibility for students and instructors wishing to pursue a number of important areas of modern algebra,

either in the form of independent study or courses. For example, well integrated one-semester courses for students with some prior algebra background might include the following: Section 9.6 and Chapters 15 and 16; or Chapters 10 and 17; or Chapters 5, 6 and Part VI. Each of these would also provide a solid background for a follow-up course delving more deeply into one of many possible areas: algebraic number theory, algebraic topology, algebraic geometry, representation theory, Lie groups, etc.

The choice of new material and the style for developing and integrating it into the text are in consonance with a basic theme in the book: the power and beauty that accrues from a rich interplay between different areas of mathematics. The emphasis throughout has been to motivate the introduction and development of important algebraic concepts using as many examples as possible. We have not attempted to be encyclopedic, but have tried to touch on many of the central themes in elementary algebra in a manner suggesting the very natural development of these ideas.

A number of important ideas and results appear in the exercises. This is not because they are not significant, rather because they did not fit easily into the flow of the text but were too important to leave out entirely. Sequences of exercises on one topic are prefaced with some remarks and are structured so that they may be read without actually doing the exercises. In some instances, new material is introduced first in the exercises—often a few sections before it appears in the text—so that students may obtain an easier introduction to it by doing these exercises (e.g., Lagrange’s Theorem appears in the exercises in Section 1.7 and in the text in Section 3.2). All the exercises are within the scope of the text and hints are given [in brackets] where we felt they were needed. Exercises we felt might be less straightforward are usually phrased so as to provide the answer to the exercise; as well many exercises have been broken down into a sequence of more routine exercises in order to make them more accessible.

We have also purposely minimized the functorial language in the text in order to keep the presentation as elementary as possible. We have refrained from providing specific references for additional reading when there are many fine choices readily available. Also, while we have endeavored to include as many fundamental topics as possible, we apologize if for reasons of space or personal taste we have neglected any of the reader’s particular favorites.

We are deeply grateful to and would like here to thank the many students and colleagues around the world who, over more than 15 years, have offered valuable comments, insights and encouragement—their continuing support and interest have motivated our writing of this third edition.

David Dummit
Richard Foote
June, 2003

Preliminaries

Some results and notation that are used throughout the text are collected in this chapter for convenience. Students may wish to review this chapter quickly at first and then read each section more carefully again as the concepts appear in the course of the text.

0.1 BASICS

The basics of set theory: sets, \cap , \cup , \in , etc. should be familiar to the reader. Our notation for subsets of a given set A will be

$$B = \{a \in A \mid \dots \text{ (conditions on } a) \dots\}.$$

The *order* or *cardinality* of a set A will be denoted by $|A|$. If A is a finite set the order of A is simply the number of elements of A .

It is important to understand how to test whether a particular $x \in A$ lies in a subset B of A (cf. Exercises 1-4). The *Cartesian product* of two sets A and B is the collection $A \times B = \{(a, b) \mid a \in A, b \in B\}$, of ordered pairs of elements from A and B .

We shall use the following notation for some common sets of numbers:

- (1) $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$ denotes the *integers* (the \mathbb{Z} is for the German word for numbers: “Zahlen”).
- (2) $\mathbb{Q} = \{a/b \mid a, b \in \mathbb{Z}, b \neq 0\}$ denotes the *rational numbers* (or *rationals*).
- (3) $\mathbb{R} = \{\text{all decimal expansions } \pm d_1d_2\dots d_n.a_1a_2a_3\dots\}$ denotes the *real numbers* (or *reals*).
- (4) $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}, i^2 = -1\}$ denotes the *complex numbers*.
- (5) $\mathbb{Z}^+, \mathbb{Q}^+$ and \mathbb{R}^+ will denote the positive (nonzero) elements in \mathbb{Z} , \mathbb{Q} and \mathbb{R} , respectively.

We shall use the notation $f : A \rightarrow B$ or $A \xrightarrow{f} B$ to denote a function f from A to B and the value of f at a is denoted $f(a)$ (i.e., we shall apply all our functions on the left). We use the words *function* and *map* interchangeably. The set A is called the *domain* of f and B is called the *codomain* of f . The notation $f : a \mapsto b$ or $a \mapsto b$ if f is understood indicates that $f(a) = b$, i.e., the function is being specified on *elements*.

If the function f is not specified on elements it is important in general to check that f is *well defined*, i.e., is unambiguously determined. For example, if the set A is the union of two subsets A_1 and A_2 then one can try to specify a function from A

to the set $\{0, 1\}$ by declaring that f is to map everything in A_1 to 0 and is to map everything in A_2 to 1. This unambiguously defines f unless A_1 and A_2 have elements in common (in which case it is not clear whether these elements should map to 0 or to 1). Checking that this f is well defined therefore amounts to checking that A_1 and A_2 have no intersection.

The set

$$f(A) = \{b \in B \mid b = f(a), \text{ for some } a \in A\}$$

is a subset of B , called the *range* or *image* of f (or the *image of A under f*). For each subset C of B the set

$$f^{-1}(C) = \{a \in A \mid f(a) \in C\}$$

consisting of the elements of A mapping into C under f is called the *preimage* or *inverse image* of C under f . For each $b \in B$, the preimage of $\{b\}$ under f is called the *fiber* of f over b . Note that f^{-1} is not in general a function and that the fibers of f generally contain many elements since there may be many elements of A mapping to the element b .

If $f : A \rightarrow B$ and $g : B \rightarrow C$, then the composite map $g \circ f : A \rightarrow C$ is defined by

$$(g \circ f)(a) = g(f(a)).$$

Let $f : A \rightarrow B$.

- (1) f is *injective* or is an *injection* if whenever $a_1 \neq a_2$, then $f(a_1) \neq f(a_2)$.
- (2) f is *surjective* or is a *surjection* if for all $b \in B$ there is some $a \in A$ such that $f(a) = b$, i.e., the image of f is *all* of B . Note that since a function always maps onto its range (by definition) it is necessary to specify the codomain B in order for the question of surjectivity to be meaningful.
- (3) f is *bijective* or is a *bijection* if it is both injective and surjective. If such a bijection f exists from A to B , we say A and B are in *bijective correspondence*.
- (4) f has a *left inverse* if there is a function $g : B \rightarrow A$ such that $g \circ f : A \rightarrow A$ is the identity map on A , i.e., $(g \circ f)(a) = a$, for all $a \in A$.
- (5) f has a *right inverse* if there is a function $h : B \rightarrow A$ such that $f \circ h : B \rightarrow B$ is the identity map on B .

Proposition 1. Let $f : A \rightarrow B$.

- (1) The map f is injective if and only if f has a left inverse.
- (2) The map f is surjective if and only if f has a right inverse.
- (3) The map f is a bijection if and only if there exists $g : B \rightarrow A$ such that $f \circ g$ is the identity map on B and $g \circ f$ is the identity map on A .
- (4) If A and B are finite sets with the same number of elements (i.e., $|A| = |B|$), then $f : A \rightarrow B$ is bijective if and only if f is injective if and only if f is surjective.

Proof: Exercise.

In the situation of part (3) of the proposition above the map g is necessarily unique and we shall say g is the *2-sided inverse* (or simply the *inverse*) of f .

A *permutation* of a set A is simply a bijection from A to itself.

If $A \subseteq B$ and $f : B \rightarrow C$, we denote the *restriction* of f to A by $f|_A$. When the domain we are considering is understood we shall occasionally denote $f|_A$ again simply as f even though these are formally different functions (their domains are different).

If $A \subseteq B$ and $g : A \rightarrow C$ and there is a function $f : B \rightarrow C$ such that $f|_A = g$, we shall say f is an *extension* of g to B (such a map f need not exist nor be unique).

Let A be a nonempty set.

- (1) A *binary relation* on a set A is a subset R of $A \times A$ and we write $a \sim b$ if $(a, b) \in R$.
- (2) The relation \sim on A is said to be:
 - (a) *reflexive* if $a \sim a$, for all $a \in A$,
 - (b) *symmetric* if $a \sim b$ implies $b \sim a$ for all $a, b \in A$,
 - (c) *transitive* if $a \sim b$ and $b \sim c$ implies $a \sim c$ for all $a, b, c \in A$.
- (3) A relation is an *equivalence relation* if it is reflexive, symmetric and transitive.
- (4) If \sim defines an equivalence relation on A , then the *equivalence class* of $a \in A$ is defined to be $\{x \in A \mid x \sim a\}$. Elements of the equivalence class of a are said to be *equivalent* to a . If C is an equivalence class, any element of C is called a *representative* of the class C .
- (4) A *partition* of A is any collection $\{A_i \mid i \in I\}$ of nonempty subsets of A (I some indexing set) such that
 - (a) $A = \bigcup_{i \in I} A_i$, and
 - (b) $A_i \cap A_j = \emptyset$, for all $i, j \in I$ with $i \neq j$
i.e., A is the disjoint union of the sets in the partition.

The notions of an equivalence relation on A and a partition of A are the same:

Proposition 2. Let A be a nonempty set.

- (1) If \sim defines an equivalence relation on A then the set of equivalence classes of \sim form a partition of A .
- (2) If $\{A_i \mid i \in I\}$ is a partition of A then there is an equivalence relation on A whose equivalence classes are precisely the sets A_i , $i \in I$.

Proof: Omitted.

Finally, we shall assume the reader is familiar with proofs by induction.

EXERCISES

In Exercises 1 to 4 let \mathcal{A} be the set of 2×2 matrices with real number entries. Recall that matrix multiplication is defined by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} ap + br & aq + bs \\ cp + dr & cq + ds \end{pmatrix}$$

Let

$$M = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

and let

$$\mathcal{B} = \{X \in \mathcal{A} \mid MX = XM\}.$$

1. Determine which of the following elements of \mathcal{A} lie in \mathcal{B} :

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

2. Prove that if $P, Q \in \mathcal{B}$, then $P + Q \in \mathcal{B}$ (where $+$ denotes the usual sum of two matrices).

3. Prove that if $P, Q \in \mathcal{B}$, then $P \cdot Q \in \mathcal{B}$ (where \cdot denotes the usual product of two matrices).

4. Find conditions on p, q, r, s which determine precisely when $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathcal{B}$.

5. Determine whether the following functions f are well defined:

- (a) $f : \mathbb{Q} \rightarrow \mathbb{Z}$ defined by $f(a/b) = a$.
(b) $f : \mathbb{Q} \rightarrow \mathbb{Q}$ defined by $f(a/b) = a^2/b^2$.

6. Determine whether the function $f : \mathbb{R}^+ \rightarrow \mathbb{Z}$ defined by mapping a real number r to the first digit to the right of the decimal point in a decimal expansion of r is well defined.

7. Let $f : A \rightarrow B$ be a surjective map of sets. Prove that the relation

$$a \sim b \text{ if and only if } f(a) = f(b)$$

is an equivalence relation whose equivalence classes are the fibers of f .

0.2 PROPERTIES OF THE INTEGERS

The following properties of the integers \mathbb{Z} (many familiar from elementary arithmetic) will be proved in a more general context in the ring theory of Chapter 8, but it will be necessary to use them in Part I (of course, none of the ring theory proofs of these properties will rely on the group theory).

- (1) (Well Ordering of \mathbb{Z}) If A is any nonempty subset of \mathbb{Z}^+ , there is some element $m \in A$ such that $m \leq a$, for all $a \in A$ (m is called a *minimal element* of A).
- (2) If $a, b \in \mathbb{Z}$ with $a \neq 0$, we say a divides b if there is an element $c \in \mathbb{Z}$ such that $b = ac$. In this case we write $a | b$; if a does not divide b we write $a \nmid b$.
- (3) If $a, b \in \mathbb{Z} - \{0\}$, there is a unique positive integer d , called the *greatest common divisor of a and b* (or g.c.d. of a and b), satisfying:
(a) $d | a$ and $d | b$ (so d is a common divisor of a and b), and
(b) if $e | a$ and $e | b$, then $e | d$ (so d is the greatest such divisor).
The g.c.d. of a and b will be denoted by (a, b) . If $(a, b) = 1$, we say that a and b are *relatively prime*.
- (4) If $a, b \in \mathbb{Z} - \{0\}$, there is a unique positive integer l , called the *least common multiple of a and b* (or l.c.m. of a and b), satisfying:
(a) $a | l$ and $b | l$ (so l is a common multiple of a and b), and
(b) if $a | m$ and $b | m$, then $l | m$ (so l is the least such multiple).
The connection between the greatest common divisor d and the least common multiple l of two integers a and b is given by $dl = ab$.
- (5) The *Division Algorithm*: if $a, b \in \mathbb{Z} - \{0\}$, then there exist unique $q, r \in \mathbb{Z}$ such that

$$a = qb + r \quad \text{and} \quad 0 \leq r < |b|,$$

where q is the *quotient* and r the *remainder*. This is the usual “long division” familiar from elementary arithmetic.

- (6) The *Euclidean Algorithm* is an important procedure which produces a greatest common divisor of two integers a and b by iterating the Division Algorithm: if $a, b \in \mathbb{Z} - \{0\}$, then we obtain a sequence of quotients and remainders

$$a = q_0 b + r_0 \quad (0)$$

$$b = q_1 r_0 + r_1 \quad (1)$$

$$r_0 = q_2 r_1 + r_2 \quad (2)$$

$$r_1 = q_3 r_2 + r_3 \quad (3)$$

⋮

$$r_{n-2} = q_n r_{n-1} + r_n \quad (n)$$

$$r_{n-1} = q_{n+1} r_n \quad (n+1)$$

where r_n is the last nonzero remainder. Such an r_n exists since $|b| > |r_0| > |r_1| > \dots > |r_n|$ is a decreasing sequence of strictly positive integers if the remainders are nonzero and such a sequence cannot continue indefinitely. Then r_n is the g.c.d. (a, b) of a and b .

Example

Suppose $a = 57970$ and $b = 10353$. Then applying the Euclidean Algorithm we obtain:

$$57970 = (5)10353 + 6205$$

$$10353 = (1)6205 + 4148$$

$$6205 = (1)4148 + 2057$$

$$4148 = (2)2057 + 34$$

$$2057 = (60)34 + 17$$

$$34 = (2)17$$

which shows that $(57970, 10353) = 17$.

- (7) One consequence of the Euclidean Algorithm which we shall use regularly is the following: if $a, b \in \mathbb{Z} - \{0\}$, then there exist $x, y \in \mathbb{Z}$ such that

$$(a, b) = ax + by$$

that is, *the g.c.d. of a and b is a \mathbb{Z} -linear combination of a and b* . This follows by recursively writing the element r_n in the Euclidean Algorithm in terms of the previous remainders (namely, use equation (n) above to solve for $r_n = r_{n-2} - q_n r_{n-1}$ in terms of the remainders r_{n-1} and r_{n-2} , then use equation $(n-1)$ to write r_{n-1} in terms of the remainders r_{n-2} and r_{n-3} , etc., eventually writing r_n in terms of a and b).

Example

Suppose $a = 57970$ and $b = 10353$, whose greatest common divisor we computed above to be 17. From the fifth equation (the next to last equation) in the Euclidean Algorithm applied to these two integers we solve for their greatest common divisor: $17 = 2057 - (60)34$. The fourth equation then shows that $34 = 4148 - (2)2057$, so substituting this expression for the previous remainder 34 gives the equation $17 = 2057 - (60)[4148 - (2)2057]$, i.e., $17 = (121)2057 - (60)4148$. Solving the third equation for 2057 and substituting gives $17 = (121)[6205 - (1)4148] - (60)4148 = (121)6205 - (181)4148$. Using the second equation to solve for 4148 and then the first equation to solve for 6205 we finally obtain

$$17 = (302)57970 - (1691)10353$$

as can easily be checked directly. Hence the equation $ax + by = (a, b)$ for the greatest common divisor of a and b in this example has the solution $x = 302$ and $y = -1691$. Note that it is relatively unlikely that this relation would have been found simply by guessing.

The integers x and y in (7) above are not unique. In the example with $a = 57970$ and $b = 10353$ we determined one solution to be $x = 302$ and $y = -1691$, for instance, and it is relatively simple to check that $x = -307$ and $y = 1719$ also satisfy $57970x + 10353y = 17$. The general solution for x and y is known (cf. the exercises below and in Chapter 8).

- (8) An element p of \mathbb{Z}^+ is called a *prime* if $p > 1$ and the only positive divisors of p are 1 and p (initially, the word prime will refer only to positive integers). An integer $n > 1$ which is not prime is called *composite*. For example, 2, 3, 5, 7, 11, 13, 17, 19, ... are primes and 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, ... are composite.

An important property of primes (which in fact can be used to *define* the primes (cf. Exercise 3)) is the following: if p is a prime and $p \mid ab$, for some $a, b \in \mathbb{Z}$, then either $p \mid a$ or $p \mid b$.

- (9) The *Fundamental Theorem of Arithmetic* says: if $n \in \mathbb{Z}$, $n > 1$, then n can be factored uniquely into the product of primes, i.e., there are distinct primes p_1, p_2, \dots, p_s and positive integers $\alpha_1, \alpha_2, \dots, \alpha_s$ such that

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}.$$

This factorization is unique in the sense that if q_1, q_2, \dots, q_t are any distinct primes and $\beta_1, \beta_2, \dots, \beta_t$ positive integers such that

$$n = q_1^{\beta_1} q_2^{\beta_2} \cdots q_t^{\beta_t},$$

then $s = t$ and if we arrange the two sets of primes in increasing order, then $q_i = p_i$ and $\alpha_i = \beta_i$, $1 \leq i \leq s$. For example, $n = 1852423848 = 2^3 3^2 11^2 19^3 31$ and this decomposition into the product of primes is unique.

Suppose the positive integers a and b are expressed as products of prime powers:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}, \quad b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}$$

where p_1, p_2, \dots, p_s are distinct and the exponents are ≥ 0 (we allow the exponents to be 0 here so that the products are taken over the same set of primes — the exponent will be 0 if that prime is not actually a divisor). Then the greatest common divisor of a and b is

$$(a, b) = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \cdots p_s^{\min(\alpha_s, \beta_s)}$$

(and the least common multiple is obtained by instead taking the maximum of the α_i and β_i instead of the minimum).

Example

In the example above, $a = 57970$ and $b = 10353$ can be factored as $a = 2 \cdot 5 \cdot 11 \cdot 17 \cdot 31$ and $b = 3 \cdot 7 \cdot 17 \cdot 29$, from which we can immediately conclude that their greatest common divisor is 17. Note, however, that for large integers it is extremely difficult to determine their prime factorizations (several common codes in current use are based on this difficulty, in fact), so that this is not an effective method to determine greatest common divisors in general. The Euclidean Algorithm will produce greatest common divisors quite rapidly without the need for the prime factorization of a and b .

- (10)** The *Euler φ -function* is defined as follows: for $n \in \mathbb{Z}^+$ let $\varphi(n)$ be the number of positive integers $a \leq n$ with a relatively prime to n , i.e., $(a, n) = 1$. For example, $\varphi(12) = 4$ since 1, 5, 7 and 11 are the only positive integers less than or equal to 12 which have no factors in common with 12. Similarly, $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$, etc. For primes p , $\varphi(p) = p - 1$, and, more generally, for all $a \geq 1$ we have the formula

$$\varphi(p^a) = p^a - p^{a-1} = p^{a-1}(p - 1).$$

The function φ is *multiplicative* in the sense that

$$\varphi(ab) = \varphi(a)\varphi(b) \quad \text{if } (a, b) = 1$$

(note that it is important here that a and b be relatively prime). Together with the formula above this gives a general formula for the values of φ : if $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$, then

$$\begin{aligned}\varphi(n) &= \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \dots \varphi(p_s^{\alpha_s}) \\ &= p_1^{\alpha_1-1}(p_1 - 1)p_2^{\alpha_2-1}(p_2 - 1) \dots p_s^{\alpha_s-1}(p_s - 1).\end{aligned}$$

For example, $\varphi(12) = \varphi(2^2)\varphi(3) = 2^1(2 - 1)3^0(3 - 1) = 4$. The reader should note that we shall use the letter φ for many different functions throughout the text so when we want this letter to denote Euler's function we shall be careful to indicate this explicitly.

EXERCISES

- For each of the following pairs of integers a and b , determine their greatest common divisor, their least common multiple, and write their greatest common divisor in the form $ax + by$ for some integers x and y .
 - $a = 20, b = 13$.
 - $a = 69, b = 372$.
 - $a = 792, b = 275$.
 - $a = 11391, b = 5673$.
 - $a = 1761, b = 1567$.
 - $a = 507885, b = 60808$.
- Prove that if the integer k divides the integers a and b then k divides $as + bt$ for every pair of integers s and t .

3. Prove that if n is composite then there are integers a and b such that n divides ab but n does not divide either a or b .

4. Let a, b and N be fixed integers with a and b nonzero and let $d = (a, b)$ be the greatest common divisor of a and b . Suppose x_0 and y_0 are particular solutions to $ax + by = N$ (i.e., $ax_0 + by_0 = N$). Prove for any integer t that the integers

$$x = x_0 + \frac{b}{d}t \quad \text{and} \quad y = y_0 - \frac{a}{d}t$$

are also solutions to $ax + by = N$ (this is in fact the general solution).

5. Determine the value $\varphi(n)$ for each integer $n \leq 30$ where φ denotes the Euler φ -function.

6. Prove the Well Ordering Property of \mathbb{Z} by induction and prove the minimal element is unique.

7. If p is a prime prove that there do not exist nonzero integers a and b such that $a^2 = pb^2$ (i.e., \sqrt{p} is not a rational number).

8. Let p be a prime, $n \in \mathbb{Z}^+$. Find a formula for the largest power of p which divides $n! = n(n-1)(n-2)\dots 2 \cdot 1$ (it involves the greatest integer function).

9. Write a computer program to determine the greatest common divisor (a, b) of two integers a and b and to express (a, b) in the form $ax + by$ for some integers x and y .

10. Prove for any given positive integer N there exist only finitely many integers n with $\varphi(n) = N$ where φ denotes Euler's φ -function. Conclude in particular that $\varphi(n)$ tends to infinity as n tends to infinity.

11. Prove that if d divides n then $\varphi(d)$ divides $\varphi(n)$ where φ denotes Euler's φ -function.

0.3 $\mathbb{Z}/n\mathbb{Z}$: THE INTEGERS MODULO n

Let n be a fixed positive integer. Define a relation on \mathbb{Z} by

$$a \sim b \text{ if and only if } n \mid (b - a).$$

Clearly $a \sim a$, and $a \sim b$ implies $b \sim a$ for any integers a and b , so this relation is trivially reflexive and symmetric. If $a \sim b$ and $b \sim c$ then n divides $a - b$ and n divides $b - c$ so n also divides the sum of these two integers, i.e., n divides $(a - b) + (b - c) = a - c$, so $a \sim c$ and the relation is transitive. Hence this is an equivalence relation. Write $a \equiv b \pmod{n}$ (read: a is *congruent to b mod n*) if $a \sim b$. For any $k \in \mathbb{Z}$ we shall denote the equivalence class of a by \bar{a} — this is called the *congruence class* or *residue class* of a mod n and consists of the integers which differ from a by an integral multiple of n , i.e.,

$$\begin{aligned}\bar{a} &= \{a + kn \mid k \in \mathbb{Z}\} \\ &= \{a, a \pm n, a \pm 2n, a \pm 3n, \dots\}.\end{aligned}$$

There are precisely n distinct equivalence classes mod n , namely

$$\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}$$

determined by the possible remainders after division by n and these residue classes partition the integers \mathbb{Z} . The set of equivalence classes under this equivalence relation

will be denoted by $\mathbb{Z}/n\mathbb{Z}$ and called the *integers modulo n* (or the *integers mod n*). The motivation for this notation will become clearer when we discuss quotient groups and quotient rings. Note that for different n 's the equivalence relation and equivalence classes are different so we shall always be careful to fix n first before using the bar notation. The process of finding the equivalence class mod n of some integer a is often referred to as *reducing a mod n*. This terminology also frequently refers to finding the smallest nonnegative integer congruent to a mod n (the *least residue of a mod n*).

We can define an addition and a multiplication for the elements of $\mathbb{Z}/n\mathbb{Z}$, defining *modular arithmetic* as follows: for $\bar{a}, \bar{b} \in \mathbb{Z}/n\mathbb{Z}$, define their sum and product by

$$\bar{a} + \bar{b} = \overline{a + b} \quad \text{and} \quad \bar{a} \cdot \bar{b} = \overline{ab}.$$

What this means is the following: given any two elements \bar{a} and \bar{b} in $\mathbb{Z}/n\mathbb{Z}$, to compute their sum (respectively, their product) take *any representative* integer a in the *class* \bar{a} and *any representative* integer b in the *class* \bar{b} and add (respectively, multiply) the integers a and b as usual in \mathbb{Z} and then take the equivalence class containing the result. The following Theorem 3 asserts that this is well defined, i.e., does not depend on the choice of representatives taken for the elements \bar{a} and \bar{b} of $\mathbb{Z}/n\mathbb{Z}$.

Example

Suppose $n = 12$ and consider $\mathbb{Z}/12\mathbb{Z}$, which consists of the twelve residue classes

$$\bar{0}, \bar{1}, \bar{2}, \dots, \bar{11}$$

determined by the twelve possible remainders of an integer after division by 12. The elements in the residue class $\bar{5}$, for example, are the integers which leave a remainder of 5 when divided by 12 (the integers *congruent to 5 mod 12*). Any integer congruent to 5 mod 12 (such as 5, 17, 29, ... or $-7, -19, \dots$) will serve as a representative for the residue class $\bar{5}$. Note that $\mathbb{Z}/12\mathbb{Z}$ consists of the twelve *elements* above (and each of these elements of $\mathbb{Z}/12\mathbb{Z}$ consists of an infinite number of usual integers).

Suppose now that $\bar{a} = \bar{5}$ and $\bar{b} = \bar{8}$. The most obvious representative for \bar{a} is the integer 5 and similarly 8 is the most obvious representative for \bar{b} . Using *these* representatives for the residue classes we obtain $\bar{5} + \bar{8} = \bar{13} = \bar{1}$ since 13 and 1 lie in the same class modulo $n = 12$. Had we instead taken the representative 17, say, for \bar{a} (note that 5 and 17 do lie in the same residue class modulo 12) and the representative -28 , say, for \bar{b} , we would obtain $\bar{5} + \bar{8} = \overline{(17 - 28)} = \bar{-11} = \bar{1}$ and as we mentioned the result does not depend on the choice of representatives chosen. The product of these two classes is $\bar{a} \cdot \bar{b} = \bar{5} \cdot \bar{8} = \bar{40} = \bar{4}$, also independent of the representatives chosen.

Theorem 3. The operations of addition and multiplication on $\mathbb{Z}/n\mathbb{Z}$ defined above are both well defined, that is, they do not depend on the choices of representatives for the classes involved. More precisely, if $a_1, a_2 \in \mathbb{Z}$ and $b_1, b_2 \in \mathbb{Z}$ with $\overline{a_1} = \overline{b_1}$ and $\overline{a_2} = \overline{b_2}$, then $\overline{a_1 + a_2} = \overline{b_1 + b_2}$ and $\overline{a_1 a_2} = \overline{b_1 b_2}$, i.e., if

$$a_1 \equiv b_1 \pmod{n} \quad \text{and} \quad a_2 \equiv b_2 \pmod{n}$$

then

$$a_1 + a_2 \equiv b_1 + b_2 \pmod{n} \quad \text{and} \quad a_1 a_2 \equiv b_1 b_2 \pmod{n}.$$

Proof: Suppose $a_1 \equiv b_1 \pmod{n}$, i.e., $a_1 - b_1$ is divisible by n . Then $a_1 = b_1 + sn$ for some integer s . Similarly, $a_2 \equiv b_2 \pmod{n}$ means $a_2 = b_2 + tn$ for some integer t . Then $a_1 + a_2 = (b_1 + b_2) + (s+t)n$ so that $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$, which shows that the sum of the residue classes is independent of the representatives chosen. Similarly, $a_1 a_2 = (b_1 + sn)(b_2 + tn) = b_1 b_2 + (b_1 t + b_2 s + stn)n$ shows that $a_1 a_2 \equiv b_1 b_2 \pmod{n}$ and so the product of the residue classes is also independent of the representatives chosen, completing the proof.

We shall see later that the process of adding equivalence classes by adding their representatives is a special case of a more general construction (the construction of a *quotient*). This notion of adding equivalence classes is already a familiar one in the context of adding rational numbers: each rational number a/b is really a class of expressions: $a/b = 2a/2b = -3a/-3b$ etc. and we often change representatives (for instance, take common denominators) in order to add two fractions (for example $1/2 + 1/3$ is computed by taking instead the equivalent representatives $3/6$ for $1/2$ and $2/6$ for $1/3$ to obtain $1/2 + 1/3 = 3/6 + 2/6 = 5/6$). The notion of modular arithmetic is also familiar: to find the hour of day after adding or subtracting some number of hours we reduce mod 12 and find the least residue.

It is important to be able to think of the equivalence classes of some equivalence relation as *elements* which can be manipulated (as we do, for example, with fractions) rather than as sets. Consistent with this attitude, we shall frequently denote the elements of $\mathbb{Z}/n\mathbb{Z}$ simply by $\{0, 1, \dots, n-1\}$ where addition and multiplication are *reduced mod n*. It is important to remember, however, that the elements of $\mathbb{Z}/n\mathbb{Z}$ are *not* integers, but rather collections of usual integers, and the arithmetic is quite different. For example, $5+8$ is not 1 in the integers \mathbb{Z} as it was in the example of $\mathbb{Z}/12\mathbb{Z}$ above.

The fact that one can define arithmetic in $\mathbb{Z}/n\mathbb{Z}$ has many important applications in elementary number theory. As one simple example we compute the last two digits in the number 2^{1000} . First observe that the last two digits give the remainder of 2^{1000} after we divide by 100 so we are interested in the residue class mod 100 containing 2^{1000} . We compute $2^{10} = 1024 \equiv 24 \pmod{100}$, so then $2^{20} = (2^{10})^2 \equiv 24^2 = 576 \equiv 76 \pmod{100}$. Then $2^{40} = (2^{20})^2 \equiv 76^2 = 5776 \equiv 76 \pmod{100}$. Similarly $2^{80} \equiv 2^{160} \equiv 2^{320} \equiv 2^{640} \equiv 76 \pmod{100}$. Finally, $2^{1000} = 2^{640}2^{320}2^{40} \equiv 76 \cdot 76 \cdot 76 \equiv 76 \pmod{100}$ so the final two digits are 76.

An important subset of $\mathbb{Z}/n\mathbb{Z}$ consists of the collection of residue classes which have a multiplicative inverse in $\mathbb{Z}/n\mathbb{Z}$:

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \text{there exists } \bar{c} \in \mathbb{Z}/n\mathbb{Z} \text{ with } \bar{a} \cdot \bar{c} = \bar{1}\}.$$

Some of the following exercises outline a proof that $(\mathbb{Z}/n\mathbb{Z})^\times$ is also the collection of residue classes whose representatives are relatively prime to n , which proves the following proposition.

Proposition 4. $(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid (a, n) = 1\}$.

It is easy to see that if *any* representative of \bar{a} is relatively prime to n then *all* representatives are relatively prime to n so that the set on the right in the proposition is well defined.

Example

For $n = 9$ we obtain $(\mathbb{Z}/9\mathbb{Z})^\times = \{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\}$ from the proposition. The multiplicative inverses of these elements are $\{\bar{1}, \bar{5}, \bar{7}, \bar{2}, \bar{4}, \bar{8}\}$, respectively.

If a is an integer relatively prime to n then the Euclidean Algorithm produces integers x and y satisfying $ax + ny = 1$, hence $ax \equiv 1 \pmod{n}$, so that \bar{x} is the multiplicative inverse of \bar{a} in $\mathbb{Z}/n\mathbb{Z}$. This gives an efficient method for computing multiplicative inverses in $\mathbb{Z}/n\mathbb{Z}$.

Example

Suppose $n = 60$ and $a = 17$. Applying the Euclidean Algorithm we obtain

$$60 = (3)17 + 9$$

$$17 = (1)9 + 8$$

$$9 = (1)8 + 1$$

so that a and n are relatively prime, and $(-7)17 + (2)60 = 1$. Hence $\bar{-7} = \bar{53}$ is the multiplicative inverse of $\bar{17}$ in $\mathbb{Z}/60\mathbb{Z}$.

EXERCISES

1. Write down explicitly all the elements in the residue classes of $\mathbb{Z}/18\mathbb{Z}$.
2. Prove that the distinct equivalence classes in $\mathbb{Z}/n\mathbb{Z}$ are precisely $\bar{0}, \bar{1}, \bar{2}, \dots, \bar{n-1}$ (use the Division Algorithm).
3. Prove that if $a = a_n 10^n + a_{n-1} 10^{n-1} + \dots + a_1 10 + a_0$ is any positive integer then $a \equiv a_n + a_{n-1} + \dots + a_1 + a_0 \pmod{9}$ (note that this is the usual arithmetic rule that the remainder after division by 9 is the same as the sum of the decimal digits mod 9 – in particular an integer is divisible by 9 if and only if the sum of its digits is divisible by 9) [note that $10 \equiv 1 \pmod{9}$].
4. Compute the remainder when 37^{100} is divided by 29.
5. Compute the last two digits of 9^{1500} .
6. Prove that the squares of the elements in $\mathbb{Z}/4\mathbb{Z}$ are just $\bar{0}$ and $\bar{1}$.
7. Prove for any integers a and b that $a^2 + b^2$ never leaves a remainder of 3 when divided by 4 (use the previous exercise).
8. Prove that the equation $a^2 + b^2 = 3c^2$ has no solutions in nonzero integers a , b and c . [Consider the equation mod 4 as in the previous two exercises and show that a , b and c would all have to be divisible by 2. Then each of a^2 , b^2 and c^2 has a factor of 4 and by dividing through by 4 show that there would be a smaller set of solutions to the original equation. Iterate to reach a contradiction.]
9. Prove that the square of any odd integer always leaves a remainder of 1 when divided by 8.
10. Prove that the number of elements of $(\mathbb{Z}/n\mathbb{Z})^\times$ is $\varphi(n)$ where φ denotes the Euler φ -function.
11. Prove that if $\bar{a}, \bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$, then $\bar{a} \cdot \bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$.

- 12.** Let $n \in \mathbb{Z}$, $n > 1$, and let $a \in \mathbb{Z}$ with $1 \leq a \leq n$. Prove if a and n are not relatively prime, there exists an integer b with $1 \leq b < n$ such that $ab \equiv 0 \pmod{n}$ and deduce that there cannot be an integer c such that $ac \equiv 1 \pmod{n}$.
- 13.** Let $n \in \mathbb{Z}$, $n > 1$, and let $a \in \mathbb{Z}$ with $1 \leq a \leq n$. Prove that if a and n are relatively prime then there is an integer c such that $ac \equiv 1 \pmod{n}$ [use the fact that the g.c.d. of two integers is a \mathbb{Z} -linear combination of the integers].
- 14.** Conclude from the previous two exercises that $(\mathbb{Z}/n\mathbb{Z})^\times$ is the set of elements \bar{a} of $\mathbb{Z}/n\mathbb{Z}$ with $(a, n) = 1$ and hence prove Proposition 4. Verify this directly in the case $n = 12$.
- 15.** For each of the following pairs of integers a and n , show that a is relatively prime to n and determine the multiplicative inverse of \bar{a} in $\mathbb{Z}/n\mathbb{Z}$.
- (a) $a = 13, n = 20$.
 - (b) $a = 69, n = 89$.
 - (c) $a = 1891, n = 3797$.
 - (d) $a = 6003722857, n = 77695236973$. [The Euclidean Algorithm requires only 3 steps for these integers.]
- 16.** Write a computer program to add and multiply mod n , for any n given as input. The output of these operations should be the least residues of the sums and products of two integers. Also include the feature that if $(a, n) = 1$, an integer c between 1 and $n - 1$ such that $\bar{a} \cdot \bar{c} = \bar{1}$ may be printed on request. (Your program should not, of course, simply quote “mod” functions already built into many systems).

Part I

GROUP THEORY

The modern treatment of abstract algebra begins with the disarmingly simple abstract definition of a *group*. This simple definition quickly leads to difficult questions involving the structure of such objects. There are many specific examples of groups and the power of the abstract point of view becomes apparent when results for *all* of these examples are obtained by proving a *single* result for the abstract group.

The notion of a group did not simply spring into existence, however, but is rather the culmination of a long period of mathematical investigation, the first formal definition of an abstract group in the form in which we use it appearing in 1882.¹ The definition of an abstract group has its origins in extremely old problems in algebraic equations, number theory, and geometry, and arose because very similar techniques were found to be applicable in a variety of situations. As Otto Hölder (1859–1937) observed, one of the essential characteristics of mathematics is that after applying a certain algorithm or method of proof one then considers the scope and limits of the method. As a result, properties possessed by a number of interesting objects are frequently abstracted and the question raised: can one determine *all* the objects possessing these properties? Attempting to answer such a question also frequently adds considerable understanding of the original objects under consideration. It is in this fashion that the definition of an abstract group evolved into what is, for us, the starting point of abstract algebra.

We illustrate with a few of the disparate situations in which the ideas later formalized into the notion of an abstract group were used.

- (1) In number theory the very object of study, the set of integers, is an example of a group. Consider for example what we refer to as “Euler’s Theorem” (cf. Exercise 22 of Section 3.2), one extremely simple example of which is that a^{40} has last two digits 01 if a is any integer not divisible by 2 nor by 5. This was proved in 1761 by Leonhard Euler (1707–1783) using “group-theoretic” ideas of Joseph Louis Lagrange (1736–1813), long before the first formal definition of a group. From our perspective, one now proves “Lagrange’s Theorem” (cf. Theorem 8 of Section 3.2), applying these techniques abstracted to an arbitrary group, and then *recovers* Euler’s Theorem (and many others) as a *special case*.

¹For most of the historical comments below, see the excellent book *A History of Algebra*, by B. L. van der Waerden, Springer-Verlag, 1980 and the references there, particularly *The Genesis of the Abstract Group Concept: A Contribution to the History of the Origin of Abstract Group Theory* (translated from the German by Abe Shenitzer), by H. Wussing, MIT Press, 1984. See also *Number Theory, An Approach Through History from Hammurapai to Legendre*, by A. Weil, Birkhäuser, 1984.

- (2) Investigations into the question of rational solutions to algebraic equations of the form $y^2 = x^3 - 2x$ (there are infinitely many, for example $(0, 0)$, $(-1, 1)$, $(2, 2)$, $(9/4, -21/8)$, $(-1/169, 239/2197)$) showed that connecting any two solutions by a straight line and computing the intersection of this line with the curve $y^2 = x^3 - 2x$ produces another solution. Such “Diophantine equations,” among others, were considered by Pierre de Fermat (1601–1655) (this one was solved by him in 1644), by Euler, by Lagrange around 1777, and others. In 1730 Euler raised the question of determining the indefinite integral $\int dx/\sqrt{1-x^4}$ of the “lemniscatic differential” $dx/\sqrt{1-x^4}$, used in determining the arc length along an ellipse (the question had also been considered by Gottfried Wilhelm Leibniz (1646–1716) and Johannes Bernoulli (1667–1748)). In 1752 Euler proved a “multiplication formula” for such elliptic integrals (using ideas of G.C. di Fagnano (1682–1766), received by Euler in 1751), which shows how two elliptic integrals give rise to a third, bringing into existence the theory of elliptic functions in analysis. In 1834 Carl Gustav Jacob Jacobi (1804–1851) observed that the work of Euler on solving certain Diophantine equations amounted to writing the multiplication formula for certain elliptic integrals. Today the curve above is referred to as an “elliptic curve” and these questions are viewed as two different aspects of the same thing — the fact that this geometric operation on points can be used to give the set of points on an elliptic curve the structure of a group. The study of the “arithmetic” of these groups is an active area of current research.²
- (3) By 1824 it was known that there are formulas giving the roots of quadratic, cubic and quartic equations (extending the familiar quadratic formula for the roots of $ax^2 + bx + c = 0$). In 1824, however, Niels Henrik Abel (1802–1829) proved that such a formula for the roots of a quintic is impossible (cf. Corollary 40 of Section 14.7). The proof is based on the idea of examining what happens when the roots are permuted amongst themselves (for example, interchanging two of the roots). The collection of such permutations has the structure of a group (called, naturally enough, a “permutation group”). This idea culminated in the beautiful work of Evariste Galois (1811–1832) in 1830–32, working with explicit groups of “substitutions.” Today this work is referred to as Galois Theory (and is the subject of the fourth part of this text). Similar explicit groups were being used in geometry as collections of geometric transformations (translations, reflections, etc.) by Arthur Cayley (1821–1895) around 1850, Camille Jordan (1838–1922) around 1867, Felix Klein (1849–1925) around 1870, etc., and the application of groups to geometry is still extremely active in current research into the structure of 3-space, 4-space, etc. The same group arising in the study of the solvability of the quintic arises in the study of the rigid motions of an icosahedron in geometry and in the study of elliptic functions in analysis.

The precursors of today’s abstract group can be traced back many years, even before the groups of “substitutions” of Galois. The formal definition of an abstract group which is our starting point appeared in 1882 in the work of Walter Dyck (1856–1934), an assistant to Felix Klein, and also in the work of Heinrich Weber (1842–1913).

²See *The Arithmetic of Elliptic Curves* by J. Silverman, Springer-Verlag, 1986.

in the same year.

It is frequently the case in mathematics research to find specific application of an idea before having that idea extracted and presented as an item of interest in its own right (for example, Galois used the notion of a “quotient group” implicitly in his investigations in 1830 and the definition of an abstract quotient group is due to Hölder in 1889). It is important to realize, with or without the historical context, that the reason the abstract definitions are made is because it is useful to isolate specific characteristics and consider what structure is imposed on an object having these characteristics. The notion of the structure of an algebraic object (which is made more precise by the concept of an isomorphism — which considers when two apparently different objects are in some sense the same) is a major theme which will recur throughout the text.

CHAPTER 1

Introduction to Groups

1.1 BASIC AXIOMS AND EXAMPLES

In this section the basic algebraic structure to be studied in Part I is introduced and some examples are given.

Definition.

- (1) A *binary operation* \star on a set G is a function $\star : G \times G \rightarrow G$. For any $a, b \in G$ we shall write $a \star b$ for $\star(a, b)$.
- (2) A binary operation \star on a set G is *associative* if for all $a, b, c \in G$ we have $a \star (b \star c) = (a \star b) \star c$.
- (3) If \star is a binary operation on a set G we say elements a and b of G *commute* if $a \star b = b \star a$. We say \star (or G) is *commutative* if for all $a, b \in G$, $a \star b = b \star a$.

Examples

- (1) $+$ (usual addition) is a commutative binary operation on \mathbb{Z} (or on \mathbb{Q} , \mathbb{R} , or \mathbb{C} respectively).
- (2) \times (usual multiplication) is a commutative binary operation on \mathbb{Z} (or on \mathbb{Q} , \mathbb{R} , or \mathbb{C} respectively).
- (3) $-$ (usual subtraction) is a noncommutative binary operation on \mathbb{Z} , where $-(a, b) = a - b$. The map $a \mapsto -a$ is not a binary operation (not binary).
- (4) $-$ is not a binary operation on \mathbb{Z}^+ (nor \mathbb{Q}^+ , \mathbb{R}^+) because for $a, b \in \mathbb{Z}^+$ with $a < b$, $a - b \notin \mathbb{Z}^+$, that is, $-$ does not map $\mathbb{Z}^+ \times \mathbb{Z}^+$ into \mathbb{Z}^+ .
- (5) Taking the vector cross-product of two vectors in 3-space \mathbb{R}^3 is a binary operation which is not associative and not commutative.

Suppose that \star is a binary operation on a set G and H is a subset of G . If the restriction of \star to H is a binary operation on H , i.e., for all $a, b \in H$, $a \star b \in H$, then H is said to be *closed* under \star . Observe that if \star is an associative (respectively, commutative) binary operation on G and \star restricted to some subset H of G is a binary operation on H , then \star is automatically associative (respectively, commutative) on H as well.

Definition.

- (1) A *group* is an ordered pair (G, \star) where G is a set and \star is a binary operation on G satisfying the following axioms:

- (i) $(a \star b) \star c = a \star (b \star c)$, for all $a, b, c \in G$, i.e., \star is *associative*,
 - (ii) there exists an element e in G , called an *identity* of G , such that for all $a \in G$ we have $a \star e = e \star a = a$,
 - (iii) for each $a \in G$ there is an element a^{-1} of G , called an *inverse* of a , such that $a \star a^{-1} = a^{-1} \star a = e$.
- (2) The group (G, \star) is called *abelian* (or *commutative*) if $a \star b = b \star a$ for all $a, b \in G$.

We shall immediately become less formal and say G is a group under \star if (G, \star) is a group (or just G is a group when the operation \star is clear from the context). Also, we say G is a *finite group* if in addition G is a finite set. Note that axiom (ii) ensures that a group is always nonempty.

Examples

- (1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and \mathbb{C} are groups under $+$ with $e = 0$ and $a^{-1} = -a$, for all a .
- (2) $\mathbb{Q} - \{0\}, \mathbb{R} - \{0\}, \mathbb{C} - \{0\}, \mathbb{Q}^+, \mathbb{R}^+$ are groups under \times with $e = 1$ and $a^{-1} = \frac{1}{a}$, for all a . Note however that $\mathbb{Z} - \{0\}$ is *not* a group under \times because although \times is an associative binary operation on $\mathbb{Z} - \{0\}$, the element 2 (for instance) does not have an inverse in $\mathbb{Z} - \{0\}$.

We have glossed over the fact that the associative law holds in these familiar examples. For \mathbb{Z} under $+$ this is a consequence of the axiom of associativity for addition of natural numbers. The associative law for \mathbb{Q} under $+$ follows from the associative law for \mathbb{Z} — a proof of this will be outlined later when we rigorously construct \mathbb{Q} from \mathbb{Z} (cf. Section 7.5). The associative laws for \mathbb{R} and, in turn, \mathbb{C} under $+$ are proved in elementary analysis courses when \mathbb{R} is constructed by completing \mathbb{Q} — ultimately, associativity is again a consequence of associativity for \mathbb{Z} . The associative axiom for multiplication may be established via a similar development, starting first with \mathbb{Z} . Since \mathbb{R} and \mathbb{C} will be used largely for illustrative purposes and we shall not construct \mathbb{R} from \mathbb{Q} (although we shall construct \mathbb{C} from \mathbb{R}) we shall take the associative laws (under $+$ and \times) for \mathbb{R} and \mathbb{C} as given.

Examples (continued)

- (3) The axioms for a vector space V include those axioms which specify that $(V, +)$ is an abelian group (the operation $+$ is called vector addition). Thus any vector space such as \mathbb{R}^n is, in particular, an additive group.
- (4) For $n \in \mathbb{Z}^+$, $\mathbb{Z}/n\mathbb{Z}$ is an abelian group under the operation $+$ of addition of residue classes as described in Chapter 0. We shall prove in Chapter 3 (in a more general context) that this binary operation $+$ is well defined and associative; for now we take this for granted. The identity in this group is the element $\bar{0}$ and for each $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$, the inverse of \bar{a} is $\bar{-a}$. Henceforth, when we talk about the group $\mathbb{Z}/n\mathbb{Z}$ it will be understood that the group operation is addition of classes mod n .
- (5) For $n \in \mathbb{Z}^+$, the set $(\mathbb{Z}/n\mathbb{Z})^\times$ of equivalence classes \bar{a} which have multiplicative inverses mod n is an abelian group under *multiplication* of residue classes as described in Chapter 0. Again, we shall take for granted (for the moment) that this operation is well defined and associative. The identity of this group is the element $\bar{1}$ and, by

The definition of $(\mathbb{Z}/n\mathbb{Z})^\times$, each element has a multiplicative inverse. Henceforth, when we talk about the group $(\mathbb{Z}/n\mathbb{Z})^\times$ it will be understood that the group operation is multiplication of classes mod n .

- (6) If (A, \star) and (B, \diamond) are groups, we can form a new group $A \times B$, called their *direct product*, whose elements are those in the Cartesian product

$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$

and whose operation is defined componentwise:

$$(a_1, b_1)(a_2, b_2) = (a_1 \star a_2, b_1 \diamond b_2).$$

For example, if we take $A = B = \mathbb{R}$ (both operations addition), $\mathbb{R} \times \mathbb{R}$ is the familiar Euclidean plane. The proof that the direct product of two groups is again a group is left as a straightforward exercise (later) — the proof that each group axiom holds in $A \times B$ is a consequence of that axiom holding in both A and B together with the fact that the operation in $A \times B$ is defined componentwise.

There should be no confusion between the groups $\mathbb{Z}/n\mathbb{Z}$ (under addition) and $(\mathbb{Z}/n\mathbb{Z})^\times$ (under multiplication), even though the latter is a subset of the former — the superscript \times will always indicate that the operation is multiplication.

Before continuing with more elaborate examples we prove two basic results which in particular enable us to talk about *the* identity and *the* inverse of an element.

Proposition 1. If G is a group under the operation \star , then

- (1) the identity of G is unique
- (2) for each $a \in G$, a^{-1} is uniquely determined
- (3) $(a^{-1})^{-1} = a$ for all $a \in G$
- (4) $(a \star b)^{-1} = (b^{-1}) \star (a^{-1})$
- (5) for any $a_1, a_2, \dots, a_n \in G$ the value of $a_1 \star a_2 \star \dots \star a_n$ is independent of how the expression is bracketed (this is called the *generalized associative law*).

Proof: (1) If f and g are both identities, then by axiom (ii) of the definition of a group $f \star g = f$ (take $a = f$ and $e = g$). By the same axiom $f \star g = g$ (take $a = g$ and $e = f$). Thus $f = g$, and the identity is unique.

(2) Assume b and c are both inverses of a and let e be the identity of G . By axiom (iii), $a \star b = e$ and $c \star a = e$. Thus

$$\begin{aligned} c &= c \star e && \text{(definition of } e \text{ - axiom (ii))} \\ &= c \star (a \star b) && \text{(since } e = a \star b \text{)} \\ &= (c \star a) \star b && \text{(associative law)} \\ &= e \star b && \text{(since } e = c \star a \text{)} \\ &= b && \text{(axiom (ii)).} \end{aligned}$$

(3) To show $(a^{-1})^{-1} = a$ is exactly the problem of showing a is the inverse of a^{-1} (since by part (2) a has a unique inverse). Reading the definition of a^{-1} , with the roles of a and a^{-1} mentally interchanged shows that a satisfies the defining property for the inverse of a^{-1} , hence a is the inverse of a^{-1} .

(4) Let $c = (a \star b)^{-1}$ so by definition of c , $(a \star b) \star c = e$. By the associative law

$$a \star (b \star c) = e.$$

Multiply both sides on the left by a^{-1} to get

$$a^{-1} \star (a \star (b \star c)) = a^{-1} \star e.$$

The associative law on the left hand side and the definition of e on the right give

$$(a^{-1} \star a) \star (b \star c) = a^{-1}$$

so

$$e \star (b \star c) = a^{-1}$$

hence

$$b \star c = a^{-1}.$$

Now multiply both sides on the left by b^{-1} and simplify similarly:

$$b^{-1} \star (b \star c) = b^{-1} \star a^{-1}$$

$$(b^{-1} \star b) \star c = b^{-1} \star a^{-1}$$

$$e \star c = b^{-1} \star a^{-1}$$

$$c = b^{-1} \star a^{-1},$$

as claimed.

(5) This is left as a good exercise using induction on n . First show the result is true for $n = 1, 2$, and 3 . Next assume for any $k < n$ that any bracketing of a product of k elements, $b_1 \star b_2 \star \cdots \star b_k$ can be reduced (without altering the value of the product) to an expression of the form

$$b_1 \star (b_2 \star (b_3 \star (\cdots \star b_k)) \ldots).$$

Now argue that any bracketing of the product $a_1 \star a_2 \star \cdots \star a_n$ must break into 2 subproducts, say $(a_1 \star a_2 \star \cdots \star a_k) \star (a_{k+1} \star a_{k+2} \star \cdots \star a_n)$, where each sub-product is bracketed in some fashion. Apply the induction assumption to each of these two sub-products and finally reduce the result to the form $a_1 \star (a_2 \star (a_3 \star (\cdots \star a_n)) \ldots)$ to complete the induction.

Note that throughout the proof of Proposition 1 we were careful not to change the *order* of any products (unless permitted by axioms (ii) and (iii)) since G may be non-abelian.

Notation:

- (1) For an abstract group G it is tiresome to keep writing the operation \star throughout our calculations. Henceforth (except when necessary) our abstract groups G , H , etc. will always be written with the operation as \cdot and $a \cdot b$ will always be written as ab . In view of the generalized associative law, products of three or more group elements will not be bracketed (although the operation is still a binary operation). Finally, for an abstract group G (operation \cdot) we denote the identity of G by 1.

- (2) For any group G (operation \cdot implied) and $x \in G$ and $n \in \mathbb{Z}^+$ since the product $xx \cdots x$ (n terms) does not depend on how it is bracketed, we shall denote it by x^n . Denote $x^{-1}x^{-1} \cdots x^{-1}$ (n terms) by x^{-n} . Let $x^0 = 1$, the identity of G .

This new notation is pleasantly concise. Of course, when we are dealing with specific groups, we shall use the natural (given) operation. For example, when the operation is $+$, the identity will be denoted by 0 and for any element a , the inverse a^{-1} will be written $-a$ and $a + a + \cdots + a$ ($n > 0$ terms) will be written na ; $-a - a - \cdots - a$ (n terms) will be written $-na$ and $0a = 0$.

Proposition 2. Let G be a group and let $a, b \in G$. The equations $ax = b$ and $ya = b$ have unique solutions for $x, y \in G$. In particular, the left and right cancellation laws hold in G , i.e.,

- (1) if $au = av$, then $u = v$, and
- (2) if $ub = vb$, then $u = v$.

Proof: We can solve $ax = b$ by multiplying both sides on the left by a^{-1} and simplifying to get $x = a^{-1}b$. The uniqueness of x follows because a^{-1} is unique. Similarly, if $ya = b$, $y = ba^{-1}$. If $au = av$, multiply both sides on the left by a^{-1} and simplify to get $u = v$. Similarly, the right cancellation law holds.

One consequence of Proposition 2 is that if a is any element of G and for some $b \in G$, $ab = e$ or $ba = e$, then $b = a^{-1}$, i.e., we do not have to show both equations hold. Also, if for some $b \in G$, $ab = a$ (or $ba = a$), then b must be the identity of G , i.e., we do not have to check $bx = xb = x$ for all $x \in G$.

Definition. For G a group and $x \in G$ define the *order* of x to be the smallest positive integer n such that $x^n = 1$, and denote this integer by $|x|$. In this case x is said to be of order n . If no positive power of x is the identity, the order of x is defined to be infinity and x is said to be of infinite order.

The symbol for the order of x should not be confused with the absolute value symbol (when $G \subseteq \mathbb{R}$ we shall be careful to distinguish the two). It may seem injudicious to choose the same symbol for order of an element as the one used to denote the cardinality (or order) of a set, however, we shall see that the order of an element in a group is the same as the cardinality of the set of all its (distinct) powers so the two uses of the word “order” are naturally related.

Examples

- (1) An element of a group has order 1 if and only if it is the identity.
- (2) In the additive groups \mathbb{Z} , \mathbb{Q} , \mathbb{R} or \mathbb{C} every nonzero (i.e., nonidentity) element has infinite order.
- (3) In the multiplicative groups $\mathbb{R} - \{0\}$ or $\mathbb{Q} - \{0\}$ the element -1 has order 2 and all other nonidentity elements have infinite order.
- (4) In the additive group $\mathbb{Z}/9\mathbb{Z}$ the element $\bar{6}$ has order 3, since $\bar{6} \neq \bar{0}$, $\bar{6} + \bar{6} = \bar{12} = \bar{3} \neq \bar{0}$, but $\bar{6} + \bar{6} + \bar{6} = \bar{18} = \bar{0}$, the identity in this group. Recall that in an *additive* group the powers of an element are the integer multiples of the element. Similarly, the order of the element $\bar{5}$ is 9, since 45 is the smallest positive multiple of 5 that is divisible by 9.

- (5) In the multiplicative group $(\mathbb{Z}/7\mathbb{Z})^\times$, the powers of the element $\bar{2}$ are $\bar{2}, \bar{4}, \bar{8} = \bar{1}$, the identity in this group, so $\bar{2}$ has order 3. Similarly, the element $\bar{3}$ has order 6, since 3^6 is the smallest positive power of 3 that is congruent to 1 modulo 7.

Definition. Let $G = \{g_1, g_2, \dots, g_n\}$ be a finite group with $g_1 = 1$. The *multiplication table* or *group table* of G is the $n \times n$ matrix whose i, j entry is the group element $g_i g_j$.

For a finite group the multiplication table contains, in some sense, all the information about the group. Computationally, however, it is an unwieldly object (being of size the square of the group order) and visually it is not a very useful object for determining properties of the group. One might think of a group table as the analogue of having a table of all the distances between pairs of cities in the country. Such a table is useful and, in essence, captures all the distance relationships, yet a map (better yet, a map with all the distances labelled on it) is a much easier tool to work with. Part of our initial development of the theory of groups (finite groups in particular) is directed towards a more conceptual way of visualizing the internal structure of groups.

EXERCISES

Let G be a group.

- Determine which of the following binary operations are associative:
 - the operation \star on \mathbb{Z} defined by $a \star b = a - b$
 - the operation \star on \mathbb{R} defined by $a \star b = a + b + ab$
 - the operation \star on \mathbb{Q} defined by $a \star b = \frac{a+b}{5}$
 - the operation \star on $\mathbb{Z} \times \mathbb{Z}$ defined by $(a, b) \star (c, d) = (ad + bc, bd)$
 - the operation \star on $\mathbb{Q} - \{0\}$ defined by $a \star b = \frac{a}{b}$.
- Decide which of the binary operations in the preceding exercise are commutative.
- Prove that addition of residue classes in $\mathbb{Z}/n\mathbb{Z}$ is associative (you may assume it is well defined).
- Prove that multiplication of residue classes in $\mathbb{Z}/n\mathbb{Z}$ is associative (you may assume it is well defined).
- Prove for all $n > 1$ that $\mathbb{Z}/n\mathbb{Z}$ is not a group under multiplication of residue classes.
- Determine which of the following sets are groups under addition:
 - the set of rational numbers (including $0 = 0/1$) in lowest terms whose denominators are odd
 - the set of rational numbers (including $0 = 0/1$) in lowest terms whose denominators are even
 - the set of rational numbers of absolute value < 1
 - the set of rational numbers of absolute value ≥ 1 together with 0
 - the set of rational numbers with denominators equal to 1 or 2
 - the set of rational numbers with denominators equal to 1, 2 or 3.
- Let $G = \{x \in \mathbb{R} \mid 0 \leq x < 1\}$ and for $x, y \in G$ let $x \star y$ be the fractional part of $x + y$ (i.e., $x \star y = x + y - [x + y]$ where $[a]$ is the greatest integer less than or equal to a). Prove that \star is a well defined binary operation on G and that G is an abelian group under \star (called the *real numbers mod 1*).

8. Let $G = \{z \in \mathbb{C} \mid z^n = 1 \text{ for some } n \in \mathbb{Z}^+\}$.
 (a) Prove that G is a group under multiplication (called the group of *roots of unity* in \mathbb{C}).
 (b) Prove that G is not a group under addition.
9. Let $G = \{a + b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Q}\}$.
 (a) Prove that G is a group under addition.
 (b) Prove that the nonzero elements of G are a group under multiplication. [“Rationalize the denominators” to find multiplicative inverses.]
10. Prove that a finite group is abelian if and only if its group table is a symmetric matrix.
11. Find the orders of each element of the additive group $\mathbb{Z}/12\mathbb{Z}$.
12. Find the orders of the following elements of the multiplicative group $(\mathbb{Z}/12\mathbb{Z})^\times$: $\bar{1}, \bar{-1}, \bar{5}, \bar{7}, \bar{-7}, \bar{13}$.
13. Find the orders of the following elements of the additive group $\mathbb{Z}/36\mathbb{Z}$: $\bar{1}, \bar{2}, \bar{6}, \bar{9}, \bar{10}, \bar{12}, \bar{-1}, \bar{-10}, \bar{-18}$.
14. Find the orders of the following elements of the multiplicative group $(\mathbb{Z}/36\mathbb{Z})^\times$: $\bar{1}, \bar{-1}, \bar{5}, \bar{13}, \bar{-13}, \bar{17}$.
15. Prove that $(a_1 a_2 \dots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \dots a_1^{-1}$ for all $a_1, a_2, \dots, a_n \in G$.
16. Let x be an element of G . Prove that $x^2 = 1$ if and only if $|x|$ is either 1 or 2.
17. Let x be an element of G . Prove that if $|x| = n$ for some positive integer n then $x^{-1} = x^{n-1}$.
18. Let x and y be elements of G . Prove that $xy = yx$ if and only if $y^{-1}xy = x$ if and only if $x^{-1}y^{-1}xy = 1$.
19. Let $x \in G$ and let $a, b \in \mathbb{Z}^+$.
 (a) Prove that $x^{a+b} = x^a x^b$ and $(x^a)^b = x^{ab}$.
 (b) Prove that $(x^a)^{-1} = x^{-a}$.
 (c) Establish part (a) for arbitrary integers a and b (positive, negative or zero).
20. For x an element in G show that x and x^{-1} have the same order.
21. Let G be a finite group and let x be an element of G of order n . Prove that if n is odd, then $x = (x^2)^k$ for some k .
22. If x and g are elements of the group G , prove that $|x| = |g^{-1}xg|$. Deduce that $|ab| = |ba|$ for all $a, b \in G$.
23. Suppose $x \in G$ and $|x| = n < \infty$. If $n = st$ for some positive integers s and t , prove that $|x^s| = t$.
24. If a and b are commuting elements of G , prove that $(ab)^n = a^n b^n$ for all $n \in \mathbb{Z}$. [Do this by induction for positive n first.]
25. Prove that if $x^2 = 1$ for all $x \in G$ then G is abelian.
26. Assume H is a nonempty subset of (G, \star) which is closed under the binary operation on G and is closed under inverses, i.e., for all h and $k \in H$, hk and $h^{-1} \in H$. Prove that H is a group under the operation \star restricted to H (such a subset H is called a *subgroup* of G).
27. Prove that if x is an element of the group G then $\{x^n \mid n \in \mathbb{Z}\}$ is a subgroup (cf. the preceding exercise) of G (called the *cyclic subgroup* of G generated by x).
28. Let (A, \star) and (B, \diamond) be groups and let $A \times B$ be their direct product (as defined in Example 6). Verify all the group axioms for $A \times B$:
 (a) prove that the associative law holds: for all $(a_i, b_i) \in A \times B$, $i = 1, 2, 3$

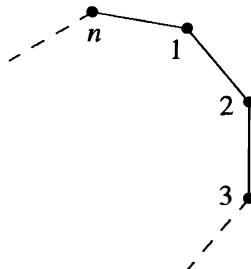
$$(a_1, b_1)[(a_2, b_2)(a_3, b_3)] = [(a_1, b_1)(a_2, b_2)](a_3, b_3),$$

- (b) prove that $(1, 1)$ is the identity of $A \times B$, and
(c) prove that the inverse of (a, b) is (a^{-1}, b^{-1}) .
29. Prove that $A \times B$ is an abelian group if and only if both A and B are abelian.
30. Prove that the elements $(a, 1)$ and $(1, b)$ of $A \times B$ commute and deduce that the order of (a, b) is the least common multiple of $|a|$ and $|b|$.
31. Prove that any finite group G of even order contains an element of order 2. [Let $t(G)$ be the set $\{g \in G \mid g \neq g^{-1}\}$. Show that $t(G)$ has an even number of elements and every nonidentity element of $G - t(G)$ has order 2.]
32. If x is an element of finite order n in G , prove that the elements $1, x, x^2, \dots, x^{n-1}$ are all distinct. Deduce that $|x| \leq |G|$.
33. Let x be an element of finite order n in G .
- Prove that if n is odd then $x^i \neq x^{-i}$ for all $i = 1, 2, \dots, n-1$.
 - Prove that if $n = 2k$ and $1 \leq i < n$ then $x^i = x^{-i}$ if and only if $i = k$.
34. If x is an element of infinite order in G , prove that the elements $x^n, n \in \mathbb{Z}$ are all distinct.
35. If x is an element of finite order n in G , use the Division Algorithm to show that *any* integral power of x equals one of the elements in the set $\{1, x, x^2, \dots, x^{n-1}\}$ (so these are all the distinct elements of the cyclic subgroup (cf. Exercise 27 above) of G generated by x).
36. Assume $G = \{1, a, b, c\}$ is a group of order 4 with identity 1. Assume also that G has no elements of order 4 (so by Exercise 32, every element has order ≤ 3). Use the cancellation laws to show that there is a unique group table for G . Deduce that G is abelian.

1.2 DIHEDRAL GROUPS

An important family of examples of groups is the class of groups whose elements are symmetries of geometric objects. The simplest subclass is when the geometric objects are regular planar figures.

For each $n \in \mathbb{Z}^+, n \geq 3$ let D_{2n} be the set of symmetries of a regular n -gon, where a symmetry is any rigid motion of the n -gon which can be effected by taking a copy of the n -gon, moving this copy in any fashion in 3-space and then placing the copy back on the original n -gon so it exactly covers it. More precisely, we can describe the symmetries by first choosing a labelling of the n vertices, for example as shown in the following figure.

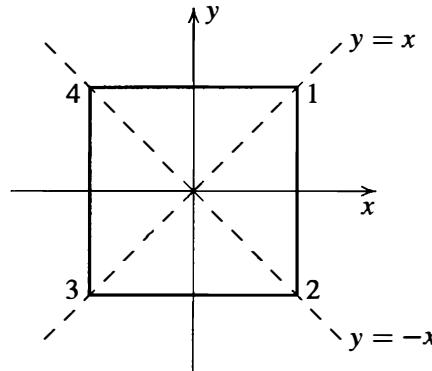


Then each symmetry s can be described uniquely by the corresponding permutation σ of $\{1, 2, 3, \dots, n\}$ where if the symmetry s puts vertex i in the place where vertex j was originally, then σ is the permutation sending i to j . For instance, if s is a rotation of $2\pi/n$ radians clockwise about the center of the n -gon, then σ is the permutation sending i to $i + 1$, $1 \leq i \leq n - 1$, and $\sigma(n) = 1$. Now make D_{2n} into a group by defining st for $s, t \in D_{2n}$ to be the symmetry obtained by first applying t then s to the n -gon (note that we are viewing symmetries as functions on the n -gon, so st is just function composition — read as usual from right to left). If s, t effect the permutations σ, τ , respectively on the vertices, then st effects $\sigma \circ \tau$. The binary operation on D_{2n} is associative since composition of functions is associative. The identity of D_{2n} is the identity symmetry (which leaves all vertices fixed), denoted by 1, and the inverse of $s \in D_{2n}$ is the symmetry which reverses all rigid motions of s (so if s effects permutation σ on the vertices, s^{-1} effects σ^{-1}). In the next paragraph we show

$$|D_{2n}| = 2n$$

and so D_{2n} is called the *dihedral group of order $2n$* . In some texts this group is written D_n ; however, D_{2n} (where the subscript gives the order of the group rather than the number of vertices) is more common in the group theory literature.

To find the order $|D_{2n}|$ observe that given any vertex i , there is a symmetry which sends vertex 1 into position i . Since vertex 2 is adjacent to vertex 1, vertex 2 must end up in position $i + 1$ or $i - 1$ (where $n + 1$ is 1 and $1 - 1$ is n , i.e., the integers labelling the vertices are read mod n). Moreover, by following the first symmetry by a reflection about the line through vertex i and the center of the n -gon one sees that vertex 2 can be sent to either position $i + 1$ or $i - 1$ by some symmetry. Thus there are $n \cdot 2$ positions the ordered pair of vertices 1, 2 may be sent to upon applying symmetries. Since symmetries are rigid motions one sees that once the position of the ordered pair of vertices 1, 2 has been specified, the action of the symmetry on all remaining vertices is completely determined. Thus there are exactly $2n$ symmetries of a regular n -gon. We can, moreover, explicitly exhibit $2n$ symmetries. These symmetries are the n rotations about the center through $2\pi i/n$ radian, $0 \leq i \leq n - 1$, and the n reflections through the n lines of symmetry (if n is odd, each symmetry line passes through a vertex and the mid-point of the opposite side; if n is even, there are $n/2$ lines of symmetry which pass through 2 opposite vertices and $n/2$ which perpendicularly bisect two opposite sides). For example, if $n = 4$ and we draw a square at the origin in an x, y plane, the lines of symmetry are



the lines $x = 0$ (y-axis), $y = 0$ (x -axis), $y = x$ and $y = -x$ (note that “reflection” through the origin is not a reflection but a rotation of π radians).

Since dihedral groups will be used extensively as an example throughout the text we fix some notation and mention some calculations which will simplify future computations and assist in viewing D_{2n} as an abstract group (rather than having to return to the geometric setting at every instance). Fix a regular n -gon centered at the origin in an x, y plane and label the vertices consecutively from 1 to n in a clockwise manner. Let r be the rotation clockwise about the origin through $2\pi/n$ radian. Let s be the reflection about the line of symmetry through vertex 1 and the origin (we use the same letters for each n , but the context will always make n clear). We leave the details of the following calculations as an exercise (for the most part we shall be working with D_6 and D_8 , so the reader may wish to try these exercises for $n = 3$ and $n = 4$ first):

- (1) $1, r, r^2, \dots, r^{n-1}$ are all distinct and $r^n = 1$, so $|r| = n$.
- (2) $|s| = 2$.
- (3) $s \neq r^i$ for any i .
- (4) $sr^i \neq sr^j$, for all $0 \leq i, j \leq n - 1$ with $i \neq j$, so

$$D_{2n} = \{1, r, r^2, \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}\}$$

i.e., each element can be written *uniquely* in the form $s^k r^i$ for some $k = 0$ or 1 and $0 \leq i \leq n - 1$.

- (5) $rs = sr^{-1}$. [First work out what permutation s effects on $\{1, 2, \dots, n\}$ and then work out separately what each side in this equation does to vertices 1 and 2.] This shows in particular that r and s do not commute so that D_{2n} is non-abelian.
- (6) $r^i s = sr^{-i}$, for all $0 \leq i \leq n$. [Proceed by induction on i and use the fact that $r^{i+1}s = r(r^i s)$ together with the preceding calculation.] This indicates how to commute s with powers of r .

Having done these calculations, we now observe that the complete multiplication table of D_{2n} can be written in terms r and s alone, that is, all the elements of D_{2n} have a (unique) representation in the form $s^k r^i$, $k = 0$ or 1 and $0 \leq i \leq n - 1$, and any product of two elements in this form can be reduced to another in the same form using only “relations” (1), (2) and (6) (reducing all exponents mod n). For example, if $n = 12$,

$$(sr^9)(sr^6) = s(r^9s)r^6 = s(sr^{-9})r^6 = s^2r^{-9+6} = r^{-3} = r^9.$$

Generators and Relations

The use of the generators r and s for the dihedral group provides a simple and succinct way of computing in D_{2n} . We can similarly introduce the notions of generators and relations for arbitrary groups. It is useful to have these concepts early (before their formal justification) since they provide simple ways of describing and computing in many groups. Generators will be discussed in greater detail in Section 2.4, and both concepts will be treated rigorously in Section 6.3 when we introduce the notion of free groups.

A subset S of elements of a group G with the property that every element of G can be written as a (finite) product of elements of S and their inverses is called a set of *generators* of G . We shall indicate this notationally by writing $G = \langle S \rangle$ and say G is generated by S or S generates G . For example, the integer 1 is a generator for the additive group \mathbb{Z} of integers since every integer is a sum of a finite number of +1's and -1's, so $\mathbb{Z} = \langle 1 \rangle$. By property (4) of D_{2n} the set $S = \{r, s\}$ is a set of generators of D_{2n} , so $D_{2n} = \langle r, s \rangle$. We shall see later that in a finite group G the set S generates G if every element of G is a finite product of elements of S (i.e., it is not necessary to include the inverses of the elements of S as well).

Any equations in a general group G that the generators satisfy are called *relations* in G . Thus in D_{2n} we have relations: $r^n = 1$, $s^2 = 1$ and $rs = sr^{-1}$. Moreover, in D_{2n} these three relations have the additional property that *any* other relation between elements of the group may be derived from these three (this is not immediately obvious; it follows from the fact that we can determine exactly when two group elements are equal by using only these three relations).

In general, if some group G is generated by a subset S and there is some collection of relations, say R_1, R_2, \dots, R_m (here each R_i is an equation in the elements from $S \cup \{1\}$) such that any relation among the elements of S can be deduced from these, we shall call these generators and relations a *presentation* of G and write

$$G = \langle S \mid R_1, R_2, \dots, R_m \rangle.$$

One presentation for the dihedral group D_{2n} (using the generators and relations above) is then

$$D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle. \quad (1.1)$$

We shall see that using this presentation to describe D_{2n} (rather than always reverting to the original geometric description) will greatly simplify working with these groups.

Presentations give an easy way of describing many groups, but there are a number of subtleties that need to be considered. One of these is that in an arbitrary presentation it may be difficult (or even impossible) to tell when two elements of the group (expressed in terms of the given generators) are equal. As a result it may not be evident what the order of the presented group is, or even whether the group is finite or infinite! For example, one can show that $\langle x_1, y_1 \mid x_1^2 = y_1^2 = (x_1y_1)^2 = 1 \rangle$ is a presentation of a group of order 4, whereas $\langle x_2, y_2 \mid x_2^3 = y_2^3 = (x_2y_2)^3 = 1 \rangle$ is a presentation of an infinite group (cf. the exercises).

Another subtlety is that even in quite simple presentations, some “collapsing” may occur because the relations are intertwined in some unobvious way, i.e., there may be “hidden,” or implicit, relations that are not explicitly given in the presentation but rather are consequences of the specified ones. This collapsing makes it difficult in general to determine even a lower bound for the size of the group being presented. For example, suppose one mimicked the presentation of D_{2n} in an attempt to create another group by defining:

$$X_{2n} = \langle x, y \mid x^n = y^2 = 1, xy = yx^2 \rangle. \quad (1.2)$$

The “commutation” relation $xy = yx^2$ determines how to commute y and x (i.e., how to “move” y from the right of x to the left), so that just as in the group D_{2n} every element in this group can be written in the form y^kx^i with all the powers of y on the left and all

the powers of x on the right. Also, by the first two relations any powers of x and y can be reduced so that i lies between 0 and $n - 1$ and k is 0 or 1. One might therefore suppose that X_{2n} is again a group of order $2n$. This is not the case because in this group there is a “hidden” relation obtained from the relation $x = xy^2$ (since $y^2 = 1$) by applying the commutation relation and the associative law repeatedly to move the y ’s to the left:

$$\begin{aligned}x &= xy^2 = (xy)y = (yx^2)y = (yx)(xy) = (yx)(yx^2) \\&= y(xy)x^2 = y(yx^2)x^2 = y^2x^4 = x^4.\end{aligned}$$

Since $x^4 = x$ it follows by the cancellation laws that $x^3 = 1$ in X_{2n} , and from the discussion above it follows that X_{2n} has order at most 6 for any n . Even more collapsing may occur, depending on the value of n (see the exercises).

As another example, consider the presentation

$$Y = \langle u, v \mid u^4 = v^3 = 1, uv = v^2u^2 \rangle. \quad (1.3)$$

In this case it is tempting to guess that Y is a group of order 12, but again there are additional implicit relations. In fact this group Y degenerates to the trivial group of order 1, i.e., u and v satisfy the additional relations $u = 1$ and $v = 1$ (a proof is outlined in the exercises).

This kind of collapsing does not occur for the presentation of D_{2n} because we showed by independent (geometric) means that there *is* a group of order $2n$ with generators r and s and satisfying the relations in (1). As a result, a group with only these relations must have order at *least* $2n$. On the other hand, it is easy to see (using the same sort of argument for X_{2n} above and the commutation relation $rs = sr^{-1}$) that any group defined by the generators and relations in (1) has order at *most* $2n$. It follows that the group with presentation (1) has order exactly $2n$ and also that this group is indeed the group of symmetries of the regular n -gon.

The additional information we have for the presentation (1) is the existence of a group of known order satisfying this information. In contrast, we have no independent knowledge about any groups satisfying the relations in either (2) or (3). Without such independent “lower bound” information we might not even be able to determine whether a given presentation just describes the trivial group, as in (3).

While in general it is necessary to be extremely careful in prescribing groups by presentations, the use of presentations for known groups is a powerful conceptual and computational tool. Additional results about presentations, including more elaborate examples, appear in Section 6.3.

EXERCISES

In these exercises, D_{2n} has the usual presentation $D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$.

1. Compute the order of each of the elements in the following groups:
 (a) D_6 (b) D_8 (c) D_{10} .
2. Use the generators and relations above to show that if x is any element of D_{2n} which is not a power of r , then $rx = xr^{-1}$.
3. Use the generators and relations above to show that every element of D_{2n} which is not a

power of r has order 2. Deduce that D_{2n} is generated by the two elements s and sr , both of which have order 2.

4. If $n = 2k$ is even and $n \geq 4$, show that $z = r^k$ is an element of order 2 which commutes with all elements of D_{2n} . Show also that z is the only nonidentity element of D_{2n} which commutes with all elements of D_{2n} . [cf. Exercise 33 of Section 1.]
5. If n is odd and $n \geq 3$, show that the identity is the only element of D_{2n} which commutes with all elements of D_{2n} . [cf. Exercise 33 of Section 1.]
6. Let x and y be elements of order 2 in any group G . Prove that if $t = xy$ then $tx = xt^{-1}$ (so that if $n = |xy| < \infty$ then x, t satisfy the same relations in G as s, r do in D_{2n}).
7. Show that $\langle a, b \mid a^2 = b^2 = (ab)^n = 1 \rangle$ gives a presentation for D_{2n} in terms of the two generators $a = s$ and $b = sr$ of order 2 computed in Exercise 3 above. [Show that the relations for r and s follow from the relations for a and b and, conversely, the relations for a and b follow from those for r and s .]
8. Find the order of the cyclic subgroup of D_{2n} generated by r (cf. Exercise 27 of Section 1).

In each of Exercises 9 to 13 you can find the order of the group of rigid motions in \mathbb{R}^3 (also called the group of rotations) of the given Platonic solid by following the proof for the order of D_{2n} : find the number of positions to which an adjacent pair of vertices can be sent. Alternatively, you can find the number of places to which a given face may be sent and, once a face is fixed, the number of positions to which a vertex on that face may be sent.

9. Let G be the group of rigid motions in \mathbb{R}^3 of a tetrahedron. Show that $|G| = 12$.
10. Let G be the group of rigid motions in \mathbb{R}^3 of a cube. Show that $|G| = 24$.
11. Let G be the group of rigid motions in \mathbb{R}^3 of an octahedron. Show that $|G| = 24$.
12. Let G be the group of rigid motions in \mathbb{R}^3 of a dodecahedron. Show that $|G| = 60$.
13. Let G be the group of rigid motions in \mathbb{R}^3 of an icosahedron. Show that $|G| = 60$.
14. Find a set of generators for \mathbb{Z} .
15. Find a set of generators and relations for $\mathbb{Z}/n\mathbb{Z}$.
16. Show that the group $\langle x_1, y_1 \mid x_1^2 = y_1^2 = (x_1y_1)^2 = 1 \rangle$ is the dihedral group D_4 (where x_1 may be replaced by the letter r and y_1 by s). [Show that the last relation is the same as: $x_1y_1 = y_1x_1^{-1}$.]
17. Let X_{2n} be the group whose presentation is displayed in (1.2).
 - (a) Show that if $n = 3k$, then X_{2n} has order 6, and it has the same generators and relations as D_6 when x is replaced by r and y by s .
 - (b) Show that if $(3, n) = 1$, then x satisfies the additional relation: $x = 1$. In this case deduce that X_{2n} has order 2. [Use the facts that $x^n = 1$ and $x^3 = 1$.]
18. Let Y be the group whose presentation is displayed in (1.3).
 - (a) Show that $v^2 = v^{-1}$. [Use the relation: $v^3 = 1$.]
 - (b) Show that v commutes with u^3 . [Show that $v^2u^3v = u^3$ by writing the left hand side as $(v^2u^2)(uv)$ and using the relations to reduce this to the right hand side. Then use part (a).]
 - (c) Show that v commutes with u . [Show that $u^9 = u$ and then use part (b).]
 - (d) Show that $uv = 1$. [Use part (c) and the last relation.]
 - (e) Show that $u = 1$, deduce that $v = 1$, and conclude that $Y = 1$. [Use part (d) and the equation $u^4v^3 = 1$.]

1.3 SYMMETRIC GROUPS

Let Ω be any nonempty set and let S_Ω be the set of all bijections from Ω to itself (i.e., the set of all permutations of Ω). The set S_Ω is a group under function composition: \circ . Note that \circ is a binary operation on S_Ω since if $\sigma : \Omega \rightarrow \Omega$ and $\tau : \Omega \rightarrow \Omega$ are both bijections, then $\sigma \circ \tau$ is also a bijection from Ω to Ω . Since function composition is associative in general, \circ is associative. The identity of S_Ω is the permutation 1 defined by $1(a) = a$, for all $a \in \Omega$. For every permutation σ there is a (2-sided) inverse function, $\sigma^{-1} : \Omega \rightarrow \Omega$ satisfying $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = 1$. Thus, all the group axioms hold for (S_Ω, \circ) . This group is called the *symmetric group on the set Ω* . It is important to recognize that the elements of S_Ω are the *permutations* of Ω , not the elements of Ω itself.

In the special case when $\Omega = \{1, 2, 3, \dots, n\}$, the symmetric group on Ω is denoted S_n , the *symmetric group of degree n* .¹ The group S_n will play an important role throughout the text both as a group of considerable interest in its own right and as a means of illustrating and motivating the general theory.

First we show that the order of S_n is $n!$. The permutations of $\{1, 2, 3, \dots, n\}$ are precisely the injective functions of this set to itself because it is finite (Proposition 0.1) and we can count the number of injective functions. An injective function σ can send the number 1 to any of the n elements of $\{1, 2, 3, \dots, n\}$; $\sigma(2)$ can then be any one of the elements of this set except $\sigma(1)$ (so there are $n - 1$ choices for $\sigma(2)$); $\sigma(3)$ can be any element except $\sigma(1)$ or $\sigma(2)$ (so there are $n - 2$ choices for $\sigma(3)$), and so on. Thus there are precisely $n \cdot (n - 1) \cdot (n - 2) \dots 2 \cdot 1 = n!$ possible injective functions from $\{1, 2, 3, \dots, n\}$ to itself. Hence there are precisely $n!$ permutations of $\{1, 2, 3, \dots, n\}$ so there are precisely $n!$ elements in S_n .

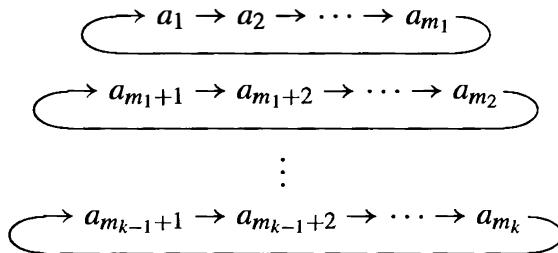
We now describe an efficient notation for writing elements σ of S_n which we shall use throughout the text and which is called the *cycle decomposition*.

A *cycle* is a string of integers which represents the element of S_n which cyclically permutes these integers (and fixes all other integers). The cycle $(a_1 a_2 \dots a_m)$ is the permutation which sends a_i to a_{i+1} , $1 \leq i \leq m - 1$ and sends a_m to a_1 . For example $(2 \ 1 \ 3)$ is the permutation which maps 2 to 1, 1 to 3 and 3 to 2. In general, for each $\sigma \in S_n$ the numbers from 1 to n will be rearranged and grouped into k cycles of the form

$$(a_1 a_2 \dots a_{m_1})(a_{m_1+1} a_{m_1+2} \dots a_{m_2}) \dots (a_{m_{k-1}+1} a_{m_{k-1}+2} \dots a_{m_k})$$

from which the action of σ on any number from 1 to n can easily be read, as follows. For any $x \in \{1, 2, 3, \dots, n\}$ first locate x in the above expression. If x is not followed immediately by a right parenthesis (i.e., x is not at the right end of one of the k cycles), then $\sigma(x)$ is the integer appearing immediately to the right of x . If x is followed by a right parenthesis, then $\sigma(x)$ is the number which is at the start of the cycle ending with x (i.e., if $x = a_{m_i}$, for some i , then $\sigma(x) = a_{m_{i-1}+1}$ (where m_0 is taken to be 0)). We can represent this description of σ by

¹We shall see in Section 6 that the structure of S_Ω depends only on the cardinality of Ω , not on the particular elements of Ω itself, so if Ω is any finite set with n elements, then S_Ω “looks like” S_n .



The product of all the cycles is called the *cycle decomposition* of σ .

We now give an algorithm for computing the cycle decomposition of an element σ of S_n and work through the algorithm with a specific permutation. We defer the proof of this algorithm and full analysis of the uniqueness aspects of the cycle decomposition until Chapter 4.

Let $n = 13$ and let $\sigma \in S_{13}$ be defined by

$$\begin{aligned}\sigma(1) &= 12, & \sigma(2) &= 13, & \sigma(3) &= 3, & \sigma(4) &= 1, & \sigma(5) &= 11, \\ \sigma(6) &= 9, & \sigma(7) &= 5, & \sigma(8) &= 10, & \sigma(9) &= 6, & \sigma(10) &= 4, \\ \sigma(11) &= 7, & \sigma(12) &= 8, & \sigma(13) &= 2.\end{aligned}$$

Cycle Decomposition Algorithm

Method	Example
To start a new cycle pick the smallest element of $\{1, 2, \dots, n\}$ which has not yet appeared in a previous cycle — call it a (if you are just starting, $a = 1$); begin the new cycle: $(a$	(1
Read off $\sigma(a)$ from the given description of σ — call it b . If $b = a$, close the cycle with a right parenthesis (without writing b down); this completes a cycle — return to step 1. If $b \neq a$, write b next to a in this cycle: $(ab$	$\sigma(1) = 12 = b, 12 \neq 1$ so write: (1 12
Read off $\sigma(b)$ from the given description of σ — call it c . If $c = a$, close the cycle with a right parenthesis to complete the cycle — return to step 1. If $c \neq a$, write c next to b in this cycle: $(abc$. Repeat this step using the number c as the new value for b until the cycle closes.	$\sigma(12) = 8, 8 \neq 1$ so continue the cycle as: (1 12 8

Naturally this process stops when all the numbers from $\{1, 2, \dots, n\}$ have appeared in some cycle. For the particular σ in the example this gives

$$\sigma = (1\ 12\ 8\ 10\ 4)(2\ 13)(3)(5\ 11\ 7)(6\ 9).$$

The *length* of a cycle is the number of integers which appear in it. A cycle of length t is called a *t-cycle*. Two cycles are called *disjoint* if they have no numbers in common.

Thus the element σ above is the product of 5 (pairwise) disjoint cycles: a 5-cycle, a 2-cycle, a 1-cycle, a 3-cycle, and another 2-cycle.

Henceforth we adopt the convention that 1-cycles will not be written. Thus if some integer, i , does not appear in the cycle decomposition of a permutation τ it is understood that $\tau(i) = i$, i.e., that τ fixes i . The identity permutation of S_n has cycle decomposition $(1)(2)\dots(n)$ and will be written simply as 1. Hence the final step of the algorithm is:

Cycle Decomposition Algorithm (cont.)

Final Step: Remove all cycles of length 1	
---	--

The cycle decomposition for the particular σ in the example is therefore

$$\sigma = (1 \ 12 \ 8 \ 10 \ 4)(2 \ 13)(5 \ 11 \ 7)(6 \ 9)$$

This convention has the advantage that the cycle decomposition of an element τ of S_n is also the cycle decomposition of the permutation in S_m for $m \geq n$ which acts as τ on $\{1, 2, 3, \dots, n\}$ and fixes each element of $\{n+1, n+2, \dots, m\}$. Thus, for example, $(1 \ 2)$ is the permutation which interchanges 1 and 2 and fixes all larger integers whether viewed in S_2 , S_3 or S_4 , etc.

As another example, the 6 elements of S_3 have the following cycle decompositions:

The group S_3

Values of σ_i	Cycle Decomposition of σ_i
$\sigma_1(1) = 1, \sigma_1(2) = 2, \sigma_1(3) = 3$	1
$\sigma_2(1) = 1, \sigma_2(2) = 3, \sigma_2(3) = 2$	$(2 \ 3)$
$\sigma_3(1) = 3, \sigma_3(2) = 2, \sigma_3(3) = 1$	$(1 \ 3)$
$\sigma_4(1) = 2, \sigma_4(2) = 1, \sigma_4(3) = 3$	$(1 \ 2)$
$\sigma_5(1) = 2, \sigma_5(2) = 3, \sigma_5(3) = 1$	$(1 \ 2 \ 3)$

For any $\sigma \in S_n$, the cycle decomposition of σ^{-1} is obtained by writing the numbers in each cycle of the cycle decomposition of σ in reverse order. For example, if $\sigma = (1 \ 12 \ 8 \ 10 \ 4)(2 \ 13)(5 \ 11 \ 7)(6 \ 9)$ is the element of S_{13} described before then

$$\sigma^{-1} = (4 \ 10 \ 8 \ 12 \ 1)(13 \ 2)(7 \ 11 \ 5)(9 \ 6).$$

Computing products in S_n is straightforward, keeping in mind that when computing $\sigma \circ \tau$ in S_n one reads the permutations from *right to left*. One simply “follows” the elements under the successive permutations. For example, in the product $(1 \ 2 \ 3)(1 \ 2)(3 \ 4)$ the number 1 is sent to 2 by the first permutation, then 2 is sent to 3 by the second permutation, hence the composite maps 1 to 3. To compute the cycle decomposition of the product we need next to see what happens to 3. It is sent first to 4,

then 4 is fixed, so 3 is mapped to 4 by the composite map. Similarly, 4 is first mapped to 3 then 3 is mapped to 1, completing this cycle in the product: $(1\ 3\ 4)$. Finally, 2 is sent to 1, then 1 is sent to 2 so 2 is fixed by this product and so $(1\ 2\ 3) \circ (1\ 2)(3\ 4) = (1\ 3\ 4)$ is the cycle decomposition of the product.

As additional examples,

$$(12) \circ (13) = (1\ 3\ 2) \quad \text{and} \quad (1\ 3) \circ (1\ 2) = (1\ 2\ 3).$$

In particular this shows that

S_n is a non-abelian group for all $n \geq 3$.

Each cycle $(a_1 a_2 \dots a_m)$ in a cycle decomposition can be viewed as the permutation which cyclically permutes a_1, a_2, \dots, a_m and fixes all other integers. Since disjoint cycles permute numbers which lie in disjoint sets it follows that

disjoint cycles commute.

Thus rearranging the cycles in any product of disjoint cycles (in particular, in a cycle decomposition) does not change the permutation.

Also, since a given cycle, $(a_1 a_2 \dots a_m)$, permutes $\{a_1, a_2, \dots, a_m\}$ cyclically, the numbers in the cycle itself can be cyclically permuted without altering the permutation, i.e.,

$$\begin{aligned} (a_1 a_2 \dots a_m) &= (a_2 a_3 \dots a_m a_1) = (a_3 a_4 \dots a_m a_1 a_2) = \dots \\ &= (a_m a_1 a_2 \dots a_{m-1}). \end{aligned}$$

Thus, for instance, $(1\ 2) = (2\ 1)$ and $(1\ 2\ 3\ 4) = (3\ 4\ 1\ 2)$. By convention, the smallest number appearing in the cycle is usually written first.

One must exercise some care working with cycles since a permutation may be written in many ways as an arbitrary product of cycles. For instance, in S_3 , $(1\ 2\ 3) = (1\ 2)(2\ 3) = (1\ 3)(1\ 3\ 2)(1\ 3)$ etc. But, (as we shall prove) the cycle decomposition of each permutation is the *unique* way of expressing a permutation as a product of disjoint cycles (up to rearranging its cycles and cyclically permuting the numbers within each cycle). Reducing an arbitrary product of cycles to a product of disjoint cycles allows us to determine at a glance whether or not two permutations are the same. Another advantage to this notation is that it is an exercise (outlined below) to prove that *the order of a permutation is the l.c.m. of the lengths of the cycles in its cycle decomposition*.

EXERCISES

1. Let σ be the permutation

$$1 \mapsto 3 \quad 2 \mapsto 4 \quad 3 \mapsto 5 \quad 4 \mapsto 2 \quad 5 \mapsto 1$$

and let τ be the permutation

$$1 \mapsto 5 \quad 2 \mapsto 3 \quad 3 \mapsto 2 \quad 4 \mapsto 4 \quad 5 \mapsto 1.$$

Find the cycle decompositions of each of the following permutations: σ , τ , σ^2 , $\sigma\tau$, $\tau\sigma$, and $\tau^2\sigma$.

2. Let σ be the permutation

$$\begin{array}{lllll} 1 \mapsto 13 & 2 \mapsto 2 & 3 \mapsto 15 & 4 \mapsto 14 & 5 \mapsto 10 \\ 6 \mapsto 6 & 7 \mapsto 12 & 8 \mapsto 3 & 9 \mapsto 4 & 10 \mapsto 1 \\ 11 \mapsto 7 & 12 \mapsto 9 & 13 \mapsto 5 & 14 \mapsto 11 & 15 \mapsto 8 \end{array}$$

and let τ be the permutation

$$\begin{array}{lllll} 1 \mapsto 14 & 2 \mapsto 9 & 3 \mapsto 10 & 4 \mapsto 2 & 5 \mapsto 12 \\ 6 \mapsto 6 & 7 \mapsto 5 & 8 \mapsto 11 & 9 \mapsto 15 & 10 \mapsto 3 \\ 11 \mapsto 8 & 12 \mapsto 7 & 13 \mapsto 4 & 14 \mapsto 1 & 15 \mapsto 13. \end{array}$$

Find the cycle decompositions of the following permutations: σ , τ , σ^2 , $\sigma\tau$, $\tau\sigma$, and $\tau^2\sigma$.

3. For each of the permutations whose cycle decompositions were computed in the preceding two exercises compute its order.
4. Compute the order of each of the elements in the following groups: (a) S_3 (b) S_4 .
5. Find the order of $(1\ 12\ 8\ 10\ 4)(2\ 13)(5\ 11\ 7)(6\ 9)$.
6. Write out the cycle decomposition of each element of order 4 in S_4 .
7. Write out the cycle decomposition of each element of order 2 in S_4 .
8. Prove that if $\Omega = \{1, 2, 3, \dots\}$ then S_Ω is an infinite group (do not say $\infty! = \infty$).
9. (a) Let σ be the 12-cycle $(1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12)$. For which positive integers i is σ^i also a 12-cycle?
(b) Let τ be the 8-cycle $(1\ 2\ 3\ 4\ 5\ 6\ 7\ 8)$. For which positive integers i is τ^i also an 8-cycle?
(c) Let ω be the 14-cycle $(1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14)$. For which positive integers i is ω^i also a 14-cycle?
10. Prove that if σ is the m -cycle $(a_1\ a_2\ \dots\ a_m)$, then for all $i \in \{1, 2, \dots, m\}$, $\sigma^i(a_k) = a_{k+i}$, where $k+i$ is replaced by its least residue mod m when $k+i > m$. Deduce that $|\sigma| = m$.
11. Let σ be the m -cycle $(1\ 2\ \dots\ m)$. Show that σ^i is also an m -cycle if and only if i is relatively prime to m .
12. (a) If $\tau = (1\ 2)(3\ 4)(5\ 6)(7\ 8)(9\ 10)$ determine whether there is a n -cycle σ ($n \geq 10$) with $\tau = \sigma^k$ for some integer k .
(b) If $\tau = (1\ 2)(3\ 4\ 5)$ determine whether there is an n -cycle σ ($n \geq 5$) with $\tau = \sigma^k$ for some integer k .
13. Show that an element has order 2 in S_n if and only if its cycle decomposition is a product of commuting 2-cycles.
14. Let p be a prime. Show that an element has order p in S_n if and only if its cycle decomposition is a product of commuting p -cycles. Show by an explicit example that this need not be the case if p is not prime.
15. Prove that the order of an element in S_n equals the least common multiple of the lengths of the cycles in its cycle decomposition. [Use Exercise 10 and Exercise 24 of Section 1.]
16. Show that if $n \geq m$ then the number of m -cycles in S_n is given by

$$\frac{n(n-1)(n-2)\dots(n-m+1)}{m}.$$

[Count the number of ways of forming an m -cycle and divide by the number of representations of a particular m -cycle.]

17. Show that if $n \geq 4$ then the number of permutations in S_n which are the product of two disjoint 2-cycles is $n(n - 1)(n - 2)(n - 3)/8$.
18. Find all numbers n such that S_5 contains an element of order n . [Use Exercise 15.]
19. Find all numbers n such that S_7 contains an element of order n . [Use Exercise 15.]
20. Find a set of generators and relations for S_3 .

1.4 MATRIX GROUPS

In this section we introduce the notion of matrix groups where the coefficients come from fields. This example of a family of groups will be used for illustrative purposes in Part I and will be studied in more detail in the chapters on vector spaces.

A *field* is the “smallest” mathematical structure in which we can perform all the arithmetic operations $+$, $-$, \times , and \div (division by nonzero elements), so in particular every nonzero element must have a multiplicative inverse. We shall study fields more thoroughly later and in this part of the text the only fields F we shall encounter will be \mathbb{Q} , \mathbb{R} and $\mathbb{Z}/p\mathbb{Z}$, where p is a prime. The example $\mathbb{Z}/p\mathbb{Z}$ is a finite field, which, to emphasize that it is a field, we shall denote by \mathbb{F}_p . For the sake of completeness we include here the precise definition of a field.

Definition.

- (1) A *field* is a set F together with two binary operations $+$ and \cdot on F such that $(F, +)$ is an abelian group (call its identity 0) and $(F - \{0\}, \cdot)$ is also an abelian group, and the following *distributive* law holds:

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c), \quad \text{for all } a, b, c \in F.$$

- (2) For any field F let $F^\times = F - \{0\}$.

All the vector space theory, the theory of matrices and linear transformations and the theory of determinants when the scalars come from \mathbb{R} is true, *mutatis mutandis*, when the scalars come from an arbitrary field F . When we use this theory in Part I we shall state explicitly what facts on fields we are assuming.

For each $n \in \mathbb{Z}^+$ let $GL_n(F)$ be the set of all $n \times n$ matrices whose entries come from F and whose determinant is nonzero, i.e.,

$$GL_n(F) = \{A \mid A \text{ is an } n \times n \text{ matrix with entries from } F \text{ and } \det(A) \neq 0\},$$

where the determinant of any matrix A with entries from F can be computed by the same formulas used when $F = \mathbb{R}$. For arbitrary $n \times n$ matrices A and B let AB be the product of these matrices as computed by the same rules as when $F = \mathbb{R}$. This product is associative. Also, since $\det(AB) = \det(A) \cdot \det(B)$, it follows that if $\det(A) \neq 0$ and $\det(B) \neq 0$, then $\det(AB) \neq 0$, so $GL_n(F)$ is closed under matrix multiplication. Furthermore, $\det(A) \neq 0$ if and only if A has a matrix inverse (and this inverse can be computed by the same adjoint formula used when $F = \mathbb{R}$), so each $A \in GL_n(F)$ has an inverse, A^{-1} , in $GL_n(F)$:

$$AA^{-1} = A^{-1}A = I,$$

where I is the $n \times n$ identity matrix. Thus $GL_n(F)$ is a group under matrix multiplication, called the *general linear group of degree n* .

The following results will be proved in Part III but are recorded now for convenience:

- (1) if F is a field and $|F| < \infty$, then $|F| = p^m$ for some prime p and integer m
- (2) if $|F| = q < \infty$, then $|GL_n(F)| = (q^n - 1)(q^n - q)(q^n - q^2) \dots (q^n - q^{n-1})$.

EXERCISES

Let F be a field and let $n \in \mathbb{Z}^+$.

1. Prove that $|GL_2(\mathbb{F}_2)| = 6$.
2. Write out all the elements of $GL_2(\mathbb{F}_2)$ and compute the order of each element.
3. Show that $GL_2(\mathbb{F}_2)$ is non-abelian.
4. Show that if n is not prime then $\mathbb{Z}/n\mathbb{Z}$ is not a field.
5. Show that $GL_n(F)$ is a finite group if and only if F has a finite number of elements.
6. If $|F| = q$ is finite prove that $|GL_n(F)| < q^{n^2}$.
7. Let p be a prime. Prove that the order of $GL_2(\mathbb{F}_p)$ is $p^4 - p^3 - p^2 + p$ (do not just quote the order formula in this section). [Subtract the number of 2×2 matrices which are *not* invertible from the total number of 2×2 matrices over \mathbb{F}_p . You may use the fact that a 2×2 matrix is not invertible if and only if one row is a multiple of the other.]
8. Show that $GL_n(F)$ is non-abelian for any $n \geq 2$ and any F .
9. Prove that the binary operation of matrix multiplication of 2×2 matrices with real number entries is associative.
10. Let $G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{R}, a \neq 0, c \neq 0 \right\}$.
 - (a) Compute the product of $\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix}$ and $\begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix}$ to show that G is closed under matrix multiplication.
 - (b) Find the matrix inverse of $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ and deduce that G is closed under inverses.
 - (c) Deduce that G is a subgroup of $GL_2(\mathbb{R})$ (cf. Exercise 26, Section 1).
 - (d) Prove that the set of elements of G whose two diagonal entries are equal (i.e., $a = c$) is also a subgroup of $GL_2(\mathbb{R})$.

The next exercise introduces the *Heisenberg group* over the field F and develops some of its basic properties. When $F = \mathbb{R}$ this group plays an important role in quantum mechanics and signal theory by giving a group theoretic interpretation (due to H. Weyl) of Heisenberg's Uncertainty Principle. Note also that the Heisenberg group may be defined more generally — for example, with entries in \mathbb{Z} .

11. Let $H(F) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in F \right\}$ — called the *Heisenberg group* over F . Let $X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$ and $Y = \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}$ be elements of $H(F)$.
 - (a) Compute the matrix product XY and deduce that $H(F)$ is closed under matrix multiplication. Exhibit explicit matrices such that $XY \neq YX$ (so that $H(F)$ is always non-abelian).

- (b) Find an explicit formula for the matrix inverse X^{-1} and deduce that $H(F)$ is closed under inverses.
- (c) Prove the associative law for $H(F)$ and deduce that $H(F)$ is a group of order $|F|^3$.
(Do not assume that matrix multiplication is associative.)
- (d) Find the order of each element of the finite group $H(\mathbb{Z}/2\mathbb{Z})$.
- (e) Prove that every nonidentity element of the group $H(\mathbb{R})$ has infinite order.

1.5 THE QUATERNION GROUP

The *quaternion group*, Q_8 , is defined by

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

with product \cdot computed as follows:

$$1 \cdot a = a \cdot 1 = a, \quad \text{for all } a \in Q_8$$

$$(-1) \cdot (-1) = 1, \quad (-1) \cdot a = a \cdot (-1) = -a, \quad \text{for all } a \in Q_8$$

$$i \cdot i = j \cdot j = k \cdot k = -1$$

$$i \cdot j = k, \quad j \cdot i = -k$$

$$j \cdot k = i, \quad k \cdot j = -i$$

$$k \cdot i = j, \quad i \cdot k = -j.$$

As usual, we shall henceforth write ab for $a \cdot b$. It is tedious to check the associative law (we shall prove this later by less computational means), but the other axioms are easily checked. Note that Q_8 is a non-abelian group of order 8.

EXERCISES

1. Compute the order of each of the elements in Q_8 .
2. Write out the group tables for S_3 , D_8 and Q_8 .
3. Find a set of generators and relations for Q_8 .

1.6 HOMOMORPHISMS AND ISOMORPHISMS

In this section we make precise the notion of when two groups “look the same,” that is, have exactly the same group-theoretic structure. This is the notion of an *isomorphism* between two groups. We first define the notion of a *homomorphism* about which we shall have a great deal more to say later.

Definition. Let (G, \star) and (H, \diamond) be groups. A map $\varphi : G \rightarrow H$ such that

$$\varphi(x \star y) = \varphi(x) \diamond \varphi(y), \quad \text{for all } x, y \in G$$

is called a *homomorphism*.

When the group operations for G and H are not explicitly written, the homomorphism condition becomes simply

$$\varphi(xy) = \varphi(x)\varphi(y)$$

but it is important to keep in mind that the product xy on the left is computed in G and the product $\varphi(x)\varphi(y)$ on the right is computed in H . Intuitively, a map φ is a homomorphism if it respects the group structures of its domain and codomain.

Definition. The map $\varphi : G \rightarrow H$ is called an *isomorphism* and G and H are said to be *isomorphic* or of the same *isomorphism type*, written $G \cong H$, if

- (1) φ is a homomorphism (i.e., $\varphi(xy) = \varphi(x)\varphi(y)$), and
- (2) φ is a bijection.

In other words, the groups G and H are isomorphic if there is a bijection between them which preserves the group operations. Intuitively, G and H are the same group except that the elements and the operations may be written differently in G and H . Thus any property which G has which depends only on the group structure of G (i.e., can be derived from the group axioms — for example, commutativity of the group) also holds in H . Note that this formally justifies writing all our group operations as \cdot since changing the symbol of the operation does not change the isomorphism type.

Examples

- (1) For any group G , $G \cong G$. The identity map provides an obvious isomorphism but not, in general, the *only* isomorphism from G to itself. More generally, let \mathcal{G} be any nonempty collection of groups. It is easy to check that the relation \cong is an equivalence relation on \mathcal{G} and the equivalence classes are called *isomorphism classes*. This accounts for the somewhat symmetric wording of the definition of “isomorphism.”
- (2) The exponential map $\exp : \mathbb{R} \rightarrow \mathbb{R}^+$ defined by $\exp(x) = e^x$, where e is the base of the natural logarithm, is an isomorphism from $(\mathbb{R}, +)$ to (\mathbb{R}^+, \times) . \exp is a bijection since it has an inverse function (namely \log_e) and \exp preserves the group operations since $e^{x+y} = e^x e^y$. In this example both the elements and the operations are different yet the two groups are isomorphic, that is, as groups they have identical structures.
- (3) In this example we show that the isomorphism type of a symmetric group depends only on the cardinality of the underlying set being permuted.

Let Δ and Ω be nonempty sets. The symmetric groups S_Δ and S_Ω are isomorphic if $|\Delta| = |\Omega|$. We can see this intuitively as follows: given that $|\Delta| = |\Omega|$, there is a bijection θ from Δ onto Ω . Think of the elements of Δ and Ω as being glued together via θ , i.e., each $x \in \Delta$ is glued to $\theta(x) \in \Omega$. To obtain a map $\varphi : S_\Delta \rightarrow S_\Omega$ let $\sigma \in S_\Delta$ be a permutation of Δ and let $\varphi(\sigma)$ be the permutation of Ω which moves the elements of Ω in the same way σ moves the corresponding glued elements of Δ ; that is, if $\sigma(x) = y$, for some $x, y \in \Delta$, then $\varphi(\sigma)(\theta(x)) = \theta(y)$ in Ω . Since the set bijection θ has an inverse, one can easily check that the map between symmetric groups also has an inverse. The precise technical definition of the map φ and the straightforward, albeit tedious, checking of the properties which ensure φ is an isomorphism are relegated to the following exercises.

Conversely, if $S_\Delta \cong S_\Omega$, then $|\Delta| = |\Omega|$; we prove this only when the underlying

sets are finite (when both Δ and Ω are infinite sets the proof is harder and will be given as an exercise in Chapter 4). Since any isomorphism between two groups G and H is, a priori, a bijection between them, a necessary condition for isomorphism is $|S_\Delta| = |S_\Omega|$. When Δ is a finite set of order n , then $|S_\Delta| = n!$. We actually only proved this for S_n , however the same reasoning applies for S_Δ . Similarly, if Ω is a finite set of order m , then $|S_\Omega| = m!$. Thus if S_Δ and S_Ω are isomorphic then $n! = m!$, so $m = n$, i.e., $|\Delta| = |\Omega|$.

Many more examples of isomorphisms will appear throughout the text. When we study different structures (rings, fields, vector spaces, etc.) we shall formulate corresponding notions of isomorphisms between respective structures. One of the central problems in mathematics is to determine what properties of a structure specify its isomorphism type (i.e., to prove that if G is an object with some structure (such as a group) and G has property \mathcal{P} , then any other similarly structured object (group) X with property \mathcal{P} is isomorphic to G). Theorems of this type are referred to as *classification theorems*. For example, we shall prove that

any non-abelian group of order 6 is isomorphic to S_3

(so here G is the group S_3 and \mathcal{P} is the property “non-abelian and of order 6”). From this classification theorem we obtain $D_6 \cong S_3$ and $GL_2(\mathbb{F}_2) \cong S_3$ without having to find explicit maps between these groups. Note that it is not true that any group of order 6 is isomorphic to S_3 . In fact we shall prove that up to isomorphism there are precisely two groups of order 6: S_3 and $\mathbb{Z}/6\mathbb{Z}$ (i.e., any group of order 6 is isomorphic to one of these two groups and S_3 is not isomorphic to $\mathbb{Z}/6\mathbb{Z}$). Note that the conclusion is less specific (there are two possible types); however, the hypotheses are easier to check (namely, check to see if the order is 6). Results of the latter type are also referred to as classifications. Generally speaking it is subtle and difficult, even in specific instances, to determine whether or not two groups (or other mathematical objects) are isomorphic — constructing an explicit map between them which preserves the group operations or proving no such map exists is, except in tiny cases, computationally unfeasible as indicated already in trying to prove the above classification of groups of order 6 without further theory.

It is occasionally easy to see that two given groups are *not* isomorphic. For example, the exercises below assert that if $\varphi : G \rightarrow H$ is an isomorphism, then, in particular,

- (a) $|G| = |H|$
- (b) G is abelian if and only if H is abelian
- (c) for all $x \in G$, $|x| = |\varphi(x)|$.

Thus S_3 and $\mathbb{Z}/6\mathbb{Z}$ are not isomorphic (as indicated above) since one is abelian and the other is not. Also, $(\mathbb{R} - \{0\}, \times)$ and $(\mathbb{R}, +)$ cannot be isomorphic because in $(\mathbb{R} - \{0\}, \times)$ the element -1 has order 2 whereas $(\mathbb{R}, +)$ has no element of order 2, contrary to (c).

Finally, we record one very useful fact that we shall prove later (when we discuss free groups) dealing with the question of homomorphisms and isomorphisms between two groups given by generators and relations:

Let G be a finite group of order n for which we have a presentation and let $S = \{s_1, \dots, s_m\}$ be the generators. Let H be another group and $\{r_1, \dots, r_m\}$ be elements of H . Suppose that any relation satisfied in G by the s_i is also satisfied in H

when each s_i is replaced by r_i . Then there is a (unique) homomorphism $\varphi : G \rightarrow H$ which maps s_i to r_i . If we have a presentation for G , then we need only check the relations specified by this presentation (since, by definition of a presentation, every relation can be deduced from the relations given in the presentation). If H is generated by the elements $\{r_1, \dots, r_m\}$, then φ is surjective (any product of the r_i 's is the image of the corresponding product of the s_i 's). If, in addition, H has the same (finite) order as G , then any surjective map is necessarily injective, i.e., φ is an isomorphism: $G \cong H$. Intuitively, we can map the generators of G to any elements of H and obtain a homomorphism provided that the relations in G are still satisfied.

Readers may already be familiar with the corresponding statement for vector spaces. Suppose V is a finite dimensional vector space of dimension n with basis S and W is another vector space. Then we can specify a linear transformation from V to W by mapping the elements of S to arbitrary vectors in W (here there are no relations to satisfy). If W is also of dimension n and the chosen vectors in W span W (and so are a basis for W) then this linear transformation is invertible (a vector space isomorphism).

Examples

- (1) Recall that $D_{2n} = \langle r, s \mid r^n = s^2 = 1, sr = r^{-1}s \rangle$. Suppose H is a group containing elements a and b with $a^n = 1, b^2 = 1$ and $ba = a^{-1}b$. Then there is a homomorphism from D_{2n} to H mapping r to a and s to b . For instance, let k be an integer dividing n with $k \geq 3$ and let $D_{2k} = \langle r_1, s_1 \mid r_1^k = s_1^2 = 1, s_1 r_1 = r_1^{-1} s_1 \rangle$. Define

$$\varphi : D_{2n} \rightarrow D_{2k} \quad \text{by} \quad \varphi(r) = r_1 \text{ and } \varphi(s) = s_1.$$

If we write $n = km$, then since $r_1^k = 1$, also $r_1^n = (r_1^k)^m = 1$. Thus the three relations satisfied by r, s in D_{2n} are satisfied by r_1, s_1 in D_{2k} . Thus φ extends (uniquely) to a homomorphism from D_{2n} to D_{2k} . Since $\{r_1, s_1\}$ generates D_{2k} , φ is surjective. This homomorphism is not an isomorphism if $k < n$.

- (2) Following up on the preceding example, let $G = D_6$ be as presented above. Check that in $H = S_3$ the elements $a = (1\ 2\ 3)$ and $b = (1\ 2)$ satisfy the relations: $a^3 = 1$, $b^2 = 1$ and $ba = ab^{-1}$. Thus there is a homomorphism from D_6 to S_3 which sends $r \mapsto a$ and $s \mapsto b$. One may further check that S_3 is generated by a and b , so this homomorphism is surjective. Since D_6 and S_3 both have order 6, this homomorphism is an isomorphism: $D_6 \cong S_3$.

Note that the element a in the examples above need not have *order n* (i.e., n need not be the *smallest* power of a giving the identity in H) and similarly b need not have order 2 (for example b could well be the identity if $a = a^{-1}$). This allows us to more easily construct homomorphisms and is in keeping with the idea that the generators and relations for a group G constitute a complete set of data for the group structure of G .

EXERCISES

Let G and H be groups.

1. Let $\varphi : G \rightarrow H$ be a homomorphism.

- (a) Prove that $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}^+$.
 (b) Do part (a) for $n = -1$ and deduce that $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}$.

- If $\varphi : G \rightarrow H$ is an isomorphism, prove that $|\varphi(x)| = |x|$ for all $x \in G$. Deduce that any two isomorphic groups have the same number of elements of order n for each $n \in \mathbb{Z}^+$. Is the result true if φ is only assumed to be a homomorphism?
- If $\varphi : G \rightarrow H$ is an isomorphism, prove that G is abelian if and only if H is abelian. If $\varphi : G \rightarrow H$ is a homomorphism, what additional conditions on φ (if any) are sufficient to ensure that if G is abelian, then so is H ?
- Prove that the multiplicative groups $\mathbb{R} - \{0\}$ and $\mathbb{C} - \{0\}$ are not isomorphic.
- Prove that the additive groups \mathbb{R} and \mathbb{Q} are not isomorphic.
- Prove that the additive groups \mathbb{Z} and \mathbb{Q} are not isomorphic.
- Prove that D_8 and Q_8 are not isomorphic.
- Prove that if $n \neq m$, S_n and S_m are not isomorphic.
- Prove that D_{24} and S_4 are not isomorphic.

- Fill in the details of the proof that the symmetric groups S_Δ and S_Ω are isomorphic if $|\Delta| = |\Omega|$ as follows: let $\theta : \Delta \rightarrow \Omega$ be a bijection. Define

$$\varphi : S_\Delta \rightarrow S_\Omega \quad \text{by} \quad \varphi(\sigma) = \theta \circ \sigma \circ \theta^{-1} \quad \text{for all } \sigma \in S_\Delta$$

and prove the following:

- φ is well defined, that is, if σ is a permutation of Δ then $\theta \circ \sigma \circ \theta^{-1}$ is a permutation of Ω .
- φ is a bijection from S_Δ onto S_Ω . [Find a 2-sided inverse for φ .]
- φ is a homomorphism, that is, $\varphi(\sigma \circ \tau) = \varphi(\sigma) \circ \varphi(\tau)$.

Note the similarity to the *change of basis* or *similarity* transformations for matrices (we shall see the connections between these later in the text).

- Let A and B be groups. Prove that $A \times B \cong B \times A$.
- Let A , B , and C be groups and let $G = A \times B$ and $H = B \times C$. Prove that $G \times C \cong A \times H$.
- Let G and H be groups and let $\varphi : G \rightarrow H$ be a homomorphism. Prove that the image of φ , $\varphi(G)$, is a subgroup of H (cf. Exercise 26 of Section 1). Prove that if φ is injective then $G \cong \varphi(G)$.
- Let G and H be groups and let $\varphi : G \rightarrow H$ be a homomorphism. Define the *kernel* of φ to be $\{g \in G \mid \varphi(g) = 1_H\}$ (so the kernel is the set of elements in G which map to the identity of H , i.e., is the fiber over the identity of H). Prove that the kernel of φ is a subgroup (cf. Exercise 26 of Section 1) of G . Prove that φ is injective if and only if the kernel of φ is the identity subgroup of G .
- Define a map $\pi : \mathbb{R}^2 \rightarrow \mathbb{R}$ by $\pi((x, y)) = x$. Prove that π is a homomorphism and find the kernel of π (cf. Exercise 14).
- Let A and B be groups and let G be their direct product, $A \times B$. Prove that the maps $\pi_1 : G \rightarrow A$ and $\pi_2 : G \rightarrow B$ defined by $\pi_1((a, b)) = a$ and $\pi_2((a, b)) = b$ are homomorphisms and find their kernels (cf. Exercise 14).
- Let G be any group. Prove that the map from G to itself defined by $g \mapsto g^{-1}$ is a homomorphism if and only if G is abelian.
- Let G be any group. Prove that the map from G to itself defined by $g \mapsto g^2$ is a homomorphism if and only if G is abelian.
- Let $G = \{z \in \mathbb{C} \mid z^n = 1 \text{ for some } n \in \mathbb{Z}^+\}$. Prove that for any fixed integer $k > 1$ the map from G to itself defined by $z \mapsto z^k$ is a surjective homomorphism but is not an isomorphism.

20. Let G be a group and let $\text{Aut}(G)$ be the set of all isomorphisms from G onto G . Prove that $\text{Aut}(G)$ is a group under function composition (called the *automorphism group* of G and the elements of $\text{Aut}(G)$ are called *automorphisms* of G).
21. Prove that for each fixed nonzero $k \in \mathbb{Q}$ the map from \mathbb{Q} to itself defined by $q \mapsto kq$ is an automorphism of \mathbb{Q} (cf. Exercise 20).
22. Let A be an abelian group and fix some $k \in \mathbb{Z}$. Prove that the map $a \mapsto a^k$ is a homomorphism from A to itself. If $k = -1$ prove that this homomorphism is an isomorphism (i.e., is an automorphism of A).
23. Let G be a finite group which possesses an automorphism σ (cf. Exercise 20) such that $\sigma(g) = g$ if and only if $g = 1$. If σ^2 is the identity map from G to G , prove that G is abelian (such an automorphism σ is called *fixed point free* of order 2). [Show that every element of G can be written in the form $x^{-1}\sigma(x)$ and apply σ to such an expression.]
24. Let G be a finite group and let x and y be distinct elements of order 2 in G that generate G . Prove that $G \cong D_{2n}$, where $n = |xy|$. [See Exercise 6 in Section 2.]
25. Let $n \in \mathbb{Z}^+$, let r and s be the usual generators of D_{2n} and let $\theta = 2\pi/n$.
- (a) Prove that the matrix $\begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$ is the matrix of the linear transformation which rotates the x, y plane about the origin in a counterclockwise direction by θ radians.
 - (b) Prove that the map $\varphi : D_{2n} \rightarrow GL_2(\mathbb{R})$ defined on generators by
- $$\varphi(r) = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \quad \text{and} \quad \varphi(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$
- extends to a homomorphism of D_{2n} into $GL_2(\mathbb{R})$.
- (c) Prove that the homomorphism φ in part (b) is injective.
26. Let i and j be the generators of Q_8 described in Section 5. Prove that the map φ from Q_8 to $GL_2(\mathbb{C})$ defined on generators by
- $$\varphi(i) = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix} \quad \text{and} \quad \varphi(j) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$
- extends to a homomorphism. Prove that φ is injective.

1.7 GROUP ACTIONS

In this section we introduce the precise definition of a group acting on a set and present some examples. Group actions will be a powerful tool which we shall use both for proving theorems for abstract groups and for unravelling the structure of specific examples. Moreover, the concept of an “action” is a theme which will recur throughout the text as a method for studying an algebraic object by seeing how it can act on other structures.

Definition. A *group action* of a group G on a set A is a map from $G \times A$ to A (written as $g \cdot a$, for all $g \in G$ and $a \in A$) satisfying the following properties:

- (1) $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$, for all $g_1, g_2 \in G$, $a \in A$, and
- (2) $1 \cdot a = a$, for all $a \in A$.

We shall immediately become less formal and say G is a group acting on a set A . The expression $g \cdot a$ will usually be written simply as ga when there is no danger of confusing this map with, say, the group operation (remember, \cdot is not a binary operation and ga is always a member of A). Note that on the left hand side of the equation in property (1) $g_2 \cdot a$ is an element of A so it makes sense to act on this by g_1 . On the right hand side of this equation the product $(g_1 g_2)$ is taken in G and the resulting group element acts on the set element a .

Before giving some examples of group actions we make some observations. Let the group G act on the set A . For each fixed $g \in G$ we get a map σ_g defined by

$$\begin{aligned}\sigma_g : A &\rightarrow A \\ \sigma_g(a) &= g \cdot a.\end{aligned}$$

We prove two important facts:

- (i) for each fixed $g \in G$, σ_g is a *permutation* of A , and
- (ii) the map from G to S_A defined by $g \mapsto \sigma_g$ is a homomorphism.

To see that σ_g is a permutation of A we show that as a set map from A to A it has a 2-sided inverse, namely $\sigma_{g^{-1}}$ (it is then a permutation by Proposition 1 of Section 0.1). For all $a \in A$

$$\begin{aligned}(\sigma_{g^{-1}} \circ \sigma_g)(a) &= \sigma_{g^{-1}}(\sigma_g(a)) && \text{(by definition of function composition)} \\ &= g^{-1} \cdot (g \cdot a) && \text{(by definition of } \sigma_{g^{-1}} \text{ and } \sigma_g\text{)} \\ &= (g^{-1}g) \cdot a && \text{(by property (1) of an action)} \\ &= 1 \cdot a = a && \text{(by property (2) of an action).}\end{aligned}$$

This proves $\sigma_{g^{-1}} \circ \sigma_g$ is the identity map from A to A . Since g was arbitrary, we may interchange the roles of g and g^{-1} to obtain $\sigma_g \circ \sigma_{g^{-1}}$ is also the identity map on A . Thus σ_g has a 2-sided inverse, hence is a permutation of A .

To check assertion (ii) above let $\varphi : G \rightarrow S_A$ be defined by $\varphi(g) = \sigma_g$. Note that part (i) shows that σ_g is indeed an element of S_A . To see that φ is a homomorphism we must prove $\varphi(g_1 g_2) = \varphi(g_1) \circ \varphi(g_2)$ (recall that S_A is a group under function composition). The permutations $\varphi(g_1 g_2)$ and $\varphi(g_1) \circ \varphi(g_2)$ are equal if and only if their values agree on every element $a \in A$. For all $a \in A$

$$\begin{aligned}\varphi(g_1 g_2)(a) &= \sigma_{g_1 g_2}(a) && \text{(by definition of } \varphi\text{)} \\ &= (g_1 g_2) \cdot a && \text{(by definition of } \sigma_{g_1 g_2}\text{)} \\ &= g_1 \cdot (g_2 \cdot a) && \text{(by property (1) of an action)} \\ &= \sigma_{g_1}(\sigma_{g_2}(a)) && \text{(by definition of } \sigma_{g_1} \text{ and } \sigma_{g_2}\text{)} \\ &= (\varphi(g_1) \circ \varphi(g_2))(a) && \text{(by definition of } \varphi\text{).}\end{aligned}$$

This proves assertion (ii) above.

Intuitively, a group action of G on a set A just means that every element g in G acts as a permutation on A in a manner consistent with the group operations in G ; assertions (i) and (ii) above make this precise. The homomorphism from G to S_A given above is

called the *permutation representation* associated to the given action. It is easy to see that this process is reversible in the sense that if $\varphi : G \rightarrow S_A$ is any homomorphism from a group G to the symmetric group on a set A , then the map from $G \times A$ to A defined by

$$g \cdot a = \varphi(g)(a) \quad \text{for all } g \in G, \text{ and all } a \in A$$

satisfies the properties of a group action of G on A . Thus actions of a group G on a set A and the homomorphisms from G into the symmetric group S_A are in bijective correspondence (i.e., are essentially the same notion, phrased in different terminology).

We should also note that the definition of an action might have been more precisely named a *left* action since the group elements appear on the left of the set elements. We could similarly define the notion of a *right* action.

Examples

Let G be a group and A a nonempty set. In each of the following examples the check of properties (1) and (2) of an action are left as exercises.

- (1) Let $ga = a$, for all $g \in G$, $a \in A$. Properties (1) and (2) of a group action follow immediately. This action is called the *trivial action* and G is said to *act trivially* on A . Note that *distinct* elements of G induce the *same* permutation on A (in this case the identity permutation). The associated permutation representation $G \rightarrow S_A$ is the trivial homomorphism which maps every element of G to the identity.

If G acts on a set B and distinct elements of G induce *distinct* permutations of B , the action is said to be *faithful*. A faithful action is therefore one in which the associated permutation representation is injective.

The *kernel* of the action of G on B is defined to be $\{g \in G \mid gb = b \text{ for all } b \in B\}$, namely the elements of G which fix *all* the elements of B . For the trivial action, the kernel of the action is all of G and this action is not faithful when $|G| > 1$.

- (2) The axioms for a vector space V over a field F include the two axioms that the multiplicative group F^\times act on the set V . Thus vector spaces are familiar examples of actions of multiplicative groups of fields where there is even more structure (in particular, V must be an abelian group) which can be exploited. In the special case when $V = \mathbb{R}^n$ and $F = \mathbb{R}$ the action is specified by

$$\alpha(r_1, r_2, \dots, r_n) = (\alpha r_1, \alpha r_2, \dots, \alpha r_n)$$

for all $\alpha \in \mathbb{R}$, $(r_1, r_2, \dots, r_n) \in \mathbb{R}^n$, where αr_i is just multiplication of two real numbers.

- (3) For any nonempty set A the symmetric group S_A acts on A by $\sigma \cdot a = \sigma(a)$, for all $\sigma \in S_A$, $a \in A$. The associated permutation representation is the identity map from S_A to itself.
- (4) If we fix a labelling of the vertices of a regular n -gon, each element α of D_{2n} gives rise to a permutation σ_α of $\{1, 2, \dots, n\}$ by the way the symmetry α permutes the corresponding vertices. The map of $D_{2n} \times \{1, 2, \dots, n\}$ onto $\{1, 2, \dots, n\}$ defined by $(\alpha, i) \rightarrow \sigma_\alpha(i)$ defines a group action of D_{2n} on $\{1, 2, \dots, n\}$. In keeping with our notation for group actions we can now dispense with the formal and cumbersome notation $\sigma_\alpha(i)$ and write αi in its place. Note that this action is faithful: distinct symmetries of a regular n -gon induce distinct permutations of the vertices.

When $n = 3$ the action of D_6 on the three (labelled) vertices of a triangle gives an injective homomorphism from D_6 to S_3 . Since these groups have the same order, this map must also be surjective, i.e., is an isomorphism: $D_6 \cong S_3$. This is another

proof of the same fact we established via generators and relations in the preceding section. Geometrically it says that any permutation of the vertices of a triangle is a symmetry. The analogous statement is not true for any n -gon with $n \geq 4$ (just by order considerations we cannot have D_{2n} isomorphic to S_n for any $n \geq 4$).

- (5) Let G be any group and let $A = G$. Define a map from $G \times A$ to A by $g \cdot a = ga$, for each $g \in G$ and $a \in A$, where ga on the right hand side is the product of g and a in the group G . This gives a group action of G on itself, where each (fixed) $g \in G$ permutes the elements of G by *left multiplication*:

$$g : a \mapsto ga \quad \text{for all } a \in G$$

(or, if G is written additively, we get $a \mapsto g + a$ and call this *left translation*). This action is called the *left regular action* of G on itself. By the cancellation laws, this action is faithful (check this).

Other examples of actions are given in the exercises.

EXERCISES

1. Let F be a field. Show that the multiplicative group of nonzero elements of F (denoted by F^\times) acts on the set F by $g \cdot a = ga$, where $g \in F^\times$, $a \in F$ and ga is the usual product in F of the two field elements (state clearly which axioms in the definition of a field are used).
2. Show that the additive group \mathbb{Z} acts on itself by $z \cdot a = z + a$ for all $z, a \in \mathbb{Z}$.
3. Show that the additive group \mathbb{R} acts on the x, y plane $\mathbb{R} \times \mathbb{R}$ by $r \cdot (x, y) = (x + ry, y)$.
4. Let G be a group acting on a set A and fix some $a \in A$. Show that the following sets are subgroups of G (cf. Exercise 26 of Section 1):
 - (a) the kernel of the action,
 - (b) $\{g \in G \mid ga = a\}$ — this subgroup is called the *stabilizer* of a in G .
5. Prove that the kernel of an action of the group G on the set A is the same as the kernel of the corresponding permutation representation $G \rightarrow S_A$ (cf. Exercise 14 in Section 6).
6. Prove that a group G acts faithfully on a set A if and only if the kernel of the action is the set consisting only of the identity.
7. Prove that in Example 2 in this section the action is faithful.
8. Let A be a nonempty set and let k be a positive integer with $k \leq |A|$. The symmetric group S_A acts on the set B consisting of all subsets of A of cardinality k by $\sigma \cdot \{a_1, \dots, a_k\} = \{\sigma(a_1), \dots, \sigma(a_k)\}$.
 - (a) Prove that this is a group action.
 - (b) Describe explicitly how the elements $(1 \ 2)$ and $(1 \ 2 \ 3)$ act on the six 2-element subsets of $\{1, 2, 3, 4\}$.
9. Do both parts of the preceding exercise with “ordered k -tuples” in place of “ k -element subsets,” where the action on k -tuples is defined as above but with set braces replaced by parentheses (note that, for example, the 2-tuples $(1, 2)$ and $(2, 1)$ are different even though the sets $\{1, 2\}$ and $\{2, 1\}$ are the same, so the sets being acted upon are different).
10. With reference to the preceding two exercises determine:
 - (a) for which values of k the action of S_n on k -element subsets is faithful, and
 - (b) for which values of k the action of S_n on ordered k -tuples is faithful.

11. Write out the cycle decomposition of the eight permutations in S_4 corresponding to the elements of D_8 given by the action of D_8 on the vertices of a square (where the vertices of the square are labelled as in Section 2).
12. Assume n is an even positive integer and show that D_{2n} acts on the set consisting of pairs of opposite vertices of a regular n -gon. Find the kernel of this action (label vertices as usual).
13. Find the kernel of the left regular action.
14. Let G be a group and let $A = G$. Show that if G is non-abelian then the maps defined by $g \cdot a = ag$ for all $g, a \in G$ do *not* satisfy the axioms of a (left) group action of G on itself.
15. Let G be any group and let $A = G$. Show that the maps defined by $g \cdot a = ag^{-1}$ for all $g, a \in G$ do satisfy the axioms of a (left) group action of G on itself.
16. Let G be any group and let $A = G$. Show that the maps defined by $g \cdot a = gag^{-1}$ for all $g, a \in G$ do satisfy the axioms of a (left) group action (this action of G on itself is called *conjugation*).
17. Let G be a group and let G act on itself by left conjugation, so each $g \in G$ maps G to G by

$$x \mapsto gxg^{-1}.$$

For fixed $g \in G$, prove that conjugation by g is an isomorphism from G onto itself (i.e., is an automorphism of G — cf. Exercise 20, Section 6). Deduce that x and gxg^{-1} have the same order for all x in G and that for any subset A of G , $|A| = |gAg^{-1}|$ (here $gAg^{-1} = \{gag^{-1} \mid a \in A\}$).

18. Let H be a group acting on a set A . Prove that the relation \sim on A defined by

$$a \sim b \quad \text{if and only if} \quad a = hb \quad \text{for some } h \in H$$
 is an equivalence relation. (For each $x \in A$ the equivalence class of x under \sim is called the *orbit* of x under the action of H . The orbits under the action of H partition the set A .)
19. Let H be a subgroup (cf. Exercise 26 of Section 1) of the finite group G and let H act on G (here $A = G$) by left multiplication. Let $x \in G$ and let \mathcal{O} be the orbit of x under the action of H . Prove that the map

$$H \rightarrow \mathcal{O} \quad \text{defined by} \quad h \mapsto hx$$

is a bijection (hence all orbits have cardinality $|H|$). From this and the preceding exercise deduce *Lagrange's Theorem*:

if G is a finite group and H is a subgroup of G then $|H|$ divides $|G|$.

20. Show that the group of rigid motions of a tetrahedron is isomorphic to a subgroup (cf. Exercise 26 of Section 1) of S_4 .
21. Show that the group of rigid motions of a cube is isomorphic to S_4 . [This group acts on the set of four pairs of opposite vertices.]
22. Show that the group of rigid motions of an octahedron is isomorphic to a subgroup (cf. Exercise 26 of Section 1) of S_4 . [This group acts on the set of four pairs of opposite faces.] Deduce that the groups of rigid motions of a cube and an octahedron are isomorphic. (These groups are isomorphic because these solids are “dual” — see *Introduction to Geometry* by H. Coxeter, Wiley, 1961. We shall see later that the groups of rigid motions of the dodecahedron and icosahedron are isomorphic as well — these solids are also dual.)
23. Explain why the action of the group of rigid motions of a cube on the set of three pairs of opposite faces is not faithful. Find the kernel of this action.

CHAPTER 2

Subgroups

2.1 DEFINITION AND EXAMPLES

One basic method for unravelling the structure of any mathematical object which is defined by a set of axioms is to study *subsets* of that object which also *satisfy the same axioms*. We begin this program by discussing subgroups of a group. A second basic method for unravelling structure is to study quotients of an object; the notion of a quotient group, which is a way (roughly speaking) of collapsing one group onto a smaller group, will be dealt with in the next chapter. Both of these themes will recur throughout the text as we study subgroups and quotient groups of a group, subrings and quotient rings of a ring, subspaces and quotient spaces of a vector space, etc.

Definition. Let G be a group. The subset H of G is a *subgroup* of G if H is nonempty and H is closed under products and inverses (i.e., $x, y \in H$ implies $x^{-1} \in H$ and $xy \in H$). If H is a subgroup of G we shall write $H \leq G$.

Subgroups of G are just subsets of G which are themselves groups with respect to the operation defined in G , i.e., the binary operation on G restricts to give a binary operation on H which is associative, has an identity in H , and has inverses in H for all the elements of H .

When we say that H is a subgroup of G we shall always mean that the operation for the group H is the operation on G restricted to H (in general it is possible that the subset H has the structure of a group with respect to some operation other than the operation on G restricted to H , cf. Example 5(a) following). As we have been doing for functions restricted to a subset, we shall denote the operation for G and the operation for the subgroup H by the same symbol. If $H \leq G$ and $H \neq G$ we shall write $H < G$ to emphasize that the containment is proper.

If H is a subgroup of G then, since the operation for H is the operation for G restricted to H , any equation in the subgroup H may also be viewed as an equation in the group G . Thus the cancellation laws for G imply that the identity for H is the same as the identity of G (in particular, every subgroup must contain 1, the identity of G) and the inverse of an element x in H is the same as the inverse of x when considered as an element of G (so the notation x^{-1} is unambiguous).

Examples

- (1) $\mathbb{Z} \leq \mathbb{Q}$ and $\mathbb{Q} \leq \mathbb{R}$ with the operation of addition.
- (2) Any group G has two subgroups: $H = G$ and $H = \{1\}$; the latter is called the *trivial subgroup* and will henceforth be denoted by 1.
- (3) If $G = D_{2n}$ is the dihedral group of order $2n$, let H be $\{1, r, r^2, \dots, r^{n-1}\}$, the set of all rotations in G . Since the product of two rotations is again a rotation and the inverse of a rotation is also a rotation it follows that H is a subgroup of D_{2n} of order n .
- (4) The set of even integers is a subgroup of the group of all integers under addition.
- (5) Some examples of subsets which are *not* subgroups:
 - (a) $\mathbb{Q} - \{0\}$ under multiplication is not a subgroup of \mathbb{R} under addition even though both are groups and $\mathbb{Q} - \{0\}$ is a subset of \mathbb{R} ; the operation of multiplication on $\mathbb{Q} - \{0\}$ is not the restriction of the operation of addition on \mathbb{R} .
 - (b) \mathbb{Z}^+ (under addition) is not a subgroup of \mathbb{Z} (under addition) because although \mathbb{Z}^+ is closed under $+$, it does not contain the identity, 0, of \mathbb{Z} and although each $x \in \mathbb{Z}^+$ has an additive inverse, $-x$, in \mathbb{Z} , $-x \notin \mathbb{Z}^+$, i.e., \mathbb{Z}^+ is not closed under the operation of taking inverses (in particular, \mathbb{Z}^+ is not a group under addition). For analogous reasons, $(\mathbb{Z} - \{0\}, \times)$ is not a subgroup of $(\mathbb{Q} - \{0\}, \times)$.
 - (c) D_6 is not a subgroup of D_8 since the former is not even a subset of the latter.
- (6) The relation “is a subgroup of” is transitive: if H is a subgroup of a group G and K is a subgroup of H , then K is also a subgroup of G .

As we saw in Chapter 1, even for easy examples checking that all the group axioms (especially the associative law) hold for any given binary operation can be tedious at best. Once we know that we have a group, however, checking that a subset of it is (or is not) a subgroup is a much easier task, since all we need to check is closure under multiplication and under taking inverses. The next proposition shows that these can be amalgamated into a single test and also shows that for *finite* groups it suffices to check for closure under multiplication.

Proposition 1. (The Subgroup Criterion) A subset H of a group G is a subgroup if and only if

- (1) $H \neq \emptyset$, and
- (2) for all $x, y \in H$, $xy^{-1} \in H$.

Furthermore, if H is finite, then it suffices to check that H is nonempty and closed under multiplication.

Proof: If H is a subgroup of G , then certainly (1) and (2) hold because H contains the identity of G and the inverse of each of its elements and because H is closed under multiplication.

It remains to show conversely that if H satisfies both (1) and (2), then $H \leq G$. Let x be any element in H (such x exists by property (1)). Let $y = x$ and apply property (2) to deduce that $1 = xx^{-1} \in H$, so H contains the identity of G . Then, again by (2), since H contains 1 and x , H contains the element $1x^{-1}$, i.e., $x^{-1} \in H$ and H is closed under taking inverses. Finally, if x and y are any two elements of H , then H contains x and y^{-1} by what we have just proved, so by (2), H also contains $x(y^{-1})^{-1} = xy$. Hence H is also closed under multiplication, which proves H is a subgroup of G .

Suppose now that H is finite and closed under multiplication and let x be any element in H . Then there are only finitely many distinct elements among x, x^2, x^3, \dots and so $x^a = x^b$ for some integers a, b with $b > a$. If $n = b - a$, then $x^n = 1$ so in particular every element $x \in H$ is of finite order. Then $x^{n-1} = x^{-1}$ is an element of H , so H is automatically also closed under inverses.

EXERCISES

Let G be a group.

1. In each of (a) – (e) prove that the specified subset is a subgroup of the given group:
 - (a) the set of complex numbers of the form $a + ai$, $a \in \mathbb{R}$ (under addition)
 - (b) the set of complex numbers of absolute value 1, i.e., the unit circle in the complex plane (under multiplication)
 - (c) for fixed $n \in \mathbb{Z}^+$ the set of rational numbers whose denominators divide n (under addition)
 - (d) for fixed $n \in \mathbb{Z}^+$ the set of rational numbers whose denominators are relatively prime to n (under addition)
 - (e) the set of nonzero real numbers whose square is a rational number (under multiplication).
2. In each of (a) – (e) prove that the specified subset is *not* a subgroup of the given group:
 - (a) the set of 2-cycles in S_n for $n \geq 3$
 - (b) the set of reflections in D_{2n} for $n \geq 3$
 - (c) for n a composite integer > 1 and G a group containing an element of order n , the set $\{x \in G \mid |x| = n\} \cup \{1\}$
 - (d) the set of (positive and negative) odd integers in \mathbb{Z} together with 0
 - (e) the set of real numbers whose square is a rational number (under addition).
3. Show that the following subsets of the dihedral group D_8 are actually subgroups:
 - (a) $\{1, r^2, s, sr^2\}$,
 - (b) $\{1, r^2, sr, sr^3\}$.
4. Give an explicit example of a group G and an infinite subset H of G that is closed under the group operation but is not a subgroup of G .
5. Prove that G cannot have a subgroup H with $|H| = n - 1$, where $n = |G| > 2$.
6. Let G be an abelian group. Prove that $\{g \in G \mid |g| < \infty\}$ is a subgroup of G (called the *torsion subgroup* of G). Give an explicit example where this set is not a subgroup when G is non-abelian.
7. Fix some $n \in \mathbb{Z}$ with $n > 1$. Find the torsion subgroup (cf. the previous exercise) of $\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})$. Show that the set of elements of infinite order together with the identity is *not* a subgroup of this direct product.
8. Let H and K be subgroups of G . Prove that $H \cup K$ is a subgroup if and only if either $H \subseteq K$ or $K \subseteq H$.
9. Let $G = GL_n(F)$, where F is any field. Define

$$SL_n(F) = \{A \in GL_n(F) \mid \det(A) = 1\}$$
 (called the *special linear group*). Prove that $SL_n(F) \leq GL_n(F)$.
10. (a) Prove that if H and K are subgroups of G then so is their intersection $H \cap K$.

(b) Prove that the intersection of an arbitrary nonempty collection of subgroups of G is again a subgroup of G (do not assume the collection is countable).
11. Let A and B be groups. Prove that the following sets are subgroups of the direct product $A \times B$:

- (a) $\{(a, 1) \mid a \in A\}$
 (b) $\{(1, b) \mid b \in B\}$
 (c) $\{(a, a) \mid a \in A\}$, where here we assume $B = A$ (called the *diagonal subgroup*).
12. Let A be an abelian group and fix some $n \in \mathbb{Z}$. Prove that the following sets are subgroups of A :
- $\{a^n \mid a \in A\}$
 - $\{a \in A \mid a^n = 1\}$.
13. Let H be a subgroup of the additive group of rational numbers with the property that $1/x \in H$ for every nonzero element x of H . Prove that $H = 0$ or \mathbb{Q} .
14. Show that $\{x \in D_{2n} \mid x^2 = 1\}$ is not a subgroup of D_{2n} (here $n \geq 3$).
15. Let $H_1 \leq H_2 \leq \dots$ be an ascending chain of subgroups of G . Prove that $\cup_{i=1}^{\infty} H_i$ is a subgroup of G .
16. Let $n \in \mathbb{Z}^+$ and let F be a field. Prove that the set $\{(a_{ij}) \in GL_n(F) \mid a_{ij} = 0 \text{ for all } i > j\}$ is a subgroup of $GL_n(F)$ (called the group of *upper triangular* matrices).
17. Let $n \in \mathbb{Z}^+$ and let F be a field. Prove that the set $\{(a_{ij}) \in GL_n(F) \mid a_{ij} = 0 \text{ for all } i > j, \text{ and } a_{ii} = 1 \text{ for all } i\}$ is a subgroup of $GL_n(F)$.

2.2 CENTRALIZERS AND NORMALIZERS, STABILIZERS AND KERNELS

We now introduce some important families of subgroups of an arbitrary group G which in particular provide many examples of subgroups. Let A be any nonempty subset of G .

Definition. Define $C_G(A) = \{g \in G \mid gag^{-1} = a \text{ for all } a \in A\}$. This subset of G is called the *centralizer* of A in G . Since $gag^{-1} = a$ if and only if $ga = ag$, $C_G(A)$ is the set of elements of G which commute with every element of A .

We show $C_G(A)$ is a subgroup of G . First of all, $C_G(A) \neq \emptyset$ because $1 \in C_G(A)$: the definition of the identity specifies that $1a = a1$, for all $a \in G$ (in particular, for all $a \in A$) so 1 satisfies the defining condition for membership in $C_G(A)$. Secondly, assume $x, y \in C_G(A)$, that is, for all $a \in A$, $xax^{-1} = a$ and $yay^{-1} = a$ (note that this does *not* mean $xy = yx$). Observe first that since $yay^{-1} = a$, multiplying both sides of this first on the left by y^{-1} , then on the right by y and then simplifying gives $a = y^{-1}ay$, i.e., $y^{-1} \in C_G(A)$ so that $C_G(A)$ is closed under taking inverses. Now

$$\begin{aligned} (xy)a(xy)^{-1} &= (xy)a(y^{-1}x^{-1}) && \text{(by Proposition 1.1(4) applied to } (xy)^{-1} \text{)} \\ &= x(yay^{-1})x^{-1} && \text{(by the associative law)} \\ &= xax^{-1} && \text{(since } y \in C_G(A) \text{)} \\ &= a && \text{(since } x \in C_G(A) \text{)} \end{aligned}$$

so $xy \in C_G(A)$ and $C_G(A)$ is closed under products, hence $C_G(A) \leq G$.

In the special case when $A = \{a\}$ we shall write simply $C_G(a)$ instead of $C_G(\{a\})$. In this case $a^n \in C_G(a)$ for all $n \in \mathbb{Z}$.

For example, in an abelian group G , $C_G(A) = G$, for all subsets A . One can check by inspection that $C_{Q_8}(i) = \{\pm 1, \pm i\}$. Some other examples are specified in the exercises.

We shall shortly discuss how to minimize the calculation of commutativities between single group elements which appears to be inherent in the computation of centralizers (and other subgroups of a similar nature).

Definition. Define $Z(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}$, the set of elements commuting with all the elements of G . This subset of G is called the *center* of G .

Note that $Z(G) = C_G(G)$, so the argument above proves $Z(G) \leq G$ as a special case. As an exercise, the reader may wish to prove $Z(G)$ is a subgroup directly.

Definition. Define $gAg^{-1} = \{gag^{-1} \mid a \in A\}$. Define the *normalizer* of A in G to be the set $N_G(A) = \{g \in G \mid gAg^{-1} = A\}$.

Notice that if $g \in C_G(A)$, then $gag^{-1} = a \in A$ for all $a \in A$ so $C_G(A) \leq N_G(A)$. The proof that $N_G(A)$ is a subgroup of G follows the same steps which demonstrated that $C_G(A) \leq G$ with appropriate modifications.

Examples

- (1) If G is abelian then all the elements of G commute, so $Z(G) = G$. Similarly, $C_G(A) = N_G(A) = G$ for *any* subset A of G since $gag^{-1} = gg^{-1}a = a$ for every $g \in G$ and every $a \in A$.
- (2) Let $G = D_8$ be the dihedral group of order 8 with the usual generators r and s and let $A = \{1, r, r^2, r^3\}$ be the subgroup of rotations in D_8 . We show that $C_{D_8}(A) = A$. Since all powers of r commute with each other, $A \leq C_{D_8}(A)$. Since $sr = r^{-1}s \neq rs$ the element s does not commute with all members of A , i.e., $s \notin C_{D_8}(A)$. Finally, the elements of D_8 that are not in A are all of the form sr^i for some $i \in \{0, 1, 2, 3\}$. If the element sr^i were in $C_{D_8}(A)$ then since $C_{D_8}(A)$ is a *subgroup* which contains r we would also have the element $s = (sr^i)(r^{-i})$ in $C_{D_8}(A)$, a contradiction. This shows $C_{D_8}(A) = A$.
- (3) As in the preceding example let $G = D_8$ and let $A = \{1, r, r^2, r^3\}$. We show that $N_{D_8}(A) = D_8$. Since, in general, the centralizer of a subset is contained in its normalizer, $A \leq N_{D_8}(A)$. Next compute that

$$sAs^{-1} = \{s1s^{-1}, srs^{-1}, sr^2s^{-1}, sr^3s^{-1}\} = \{1, r^3, r^2, r\} = A,$$

so that $s \in N_{D_8}(A)$. (Note that the *set* sAs^{-1} equals the *set* A even though the elements in these two sets appear in different orders — this is because s is in the normalizer of A but not in the centralizer of A .) Now both r and s belong to the *subgroup* $N_{D_8}(A)$ and hence $s^ir^j \in N_{D_8}(A)$ for all integers i and j , that is, every element of D_8 is in $N_{D_8}(A)$ (recall that r and s generate D_8). Since $D_8 \leq N_{D_8}(A)$ we have $N_{D_8}(A) = D_8$ (the reverse containment being obvious from the definition of a normalizer).

- (4) We show that the center of D_8 is the subgroup $\{1, r^2\}$. First observe that the center of any group G is contained in $C_G(A)$ for any subset A of G . Thus by Example 2 above $Z(D_8) \leq C_{D_8}(A) = A$, where $A = \{1, r, r^2, r^3\}$. The calculation in Example 2 shows that r and similarly r^3 are not in $Z(D_8)$, so $Z(D_8) \leq \{1, r^2\}$. To show the

reverse inclusion note that r commutes with r^2 and calculate that s also commutes with r^2 . Since r and s generate D_8 , every element of D_8 commutes with r^2 (and 1), hence $\{1, r^2\} \leq Z(D_8)$ and so equality holds.

- (5) Let $G = S_3$ and let A be the subgroup $\{1, (1\ 2)\}$. We explain why $C_{S_3}(A) = N_{S_3}(A) = A$. One can compute directly that $C_{S_3}(A) = A$, using the ideas in Example 2 above to minimize the calculations. Alternatively, since an element commutes with its powers, $A \leq C_{S_3}(A)$. By Lagrange's Theorem (Exercise 19 in Section 1.7) the order of the subgroup $C_{S_3}(A)$ of S_3 divides $|S_3| = 6$. Also by Lagrange's Theorem applied to the subgroup A of the group $C_{S_3}(A)$ we have that $2 \mid |C_{S_3}(A)|$. The only possibilities are: $|C_{S_3}(A)| = 2$ or 6 . If the latter occurs, $C_{S_3}(A) = S_3$, i.e., $A \leq Z(S_3)$; this is a contradiction because $(1\ 2)$ does not commute with $(1\ 2\ 3)$. Thus $|C_{S_3}(A)| = 2$ and so $A = C_{S_3}(A)$.

Next note that $N_{S_3}(A) = A$ because $\sigma \in N_{S_3}(A)$ if and only if

$$\{\sigma 1\sigma^{-1}, \sigma(1\ 2)\sigma^{-1}\} = \{1, (1\ 2)\}.$$

Since $\sigma 1\sigma^{-1} = 1$, this equality of sets occurs if and only if $\sigma(1\ 2)\sigma^{-1} = (1\ 2)$ as well, i.e., if and only if $\sigma \in C_{S_3}(A)$.

The center of S_3 is the identity because $Z(S_3) \leq C_{S_3}(A) = A$ and $(1\ 2) \notin Z(S_3)$.

Stabilizers and Kernels of Group Actions

The fact that the normalizer of A in G , the centralizer of A in G , and the center of G are all subgroups can be deduced as special cases of results on group actions, indicating that the structure of G is reflected by the sets on which it acts, as follows: if G is a group acting on a set S and s is some fixed element of S , the *stabilizer* of s in G is the set

$$G_s = \{g \in G \mid g \cdot s = s\}$$

(see Exercise 4 in Section 1.7). We show briefly that $G_s \leq G$: first $1 \in G_s$ by axiom (2) of an action. Also, if $y \in G_s$,

$$\begin{aligned} s &= 1 \cdot s = (y^{-1}y) \cdot s \\ &= y^{-1} \cdot (y \cdot s) \quad (\text{by axiom (1) of an action}) \\ &= y^{-1} \cdot s \quad (\text{since } y \in G_s) \end{aligned}$$

so $y^{-1} \in G_s$ as well. Finally, if $x, y \in G_s$, then

$$\begin{aligned} (xy) \cdot s &= x \cdot (y \cdot s) \quad (\text{by axiom (1) of an action}) \\ &= x \cdot s \quad (\text{since } y \in G_s) \\ &= s \quad (\text{since } x \in G_s). \end{aligned}$$

This proves G_s is a subgroup¹ of G . A similar (but easier) argument proves that the *kernel* of an action is a subgroup, where the kernel of the action of G on S is defined as

$$\{g \in G \mid g \cdot s = s, \text{ for all } s \in S\}$$

(see Exercise 1 in Section 1.7).

¹Notice how the steps to prove G_s is a subgroup are the same as those to prove $C_G(A) \leq G$ with axiom (1) of an action taking the place of the associative law.

Examples

- (1) The group $G = D_8$ acts on the set A of four vertices of a square (cf. Example 4 in Section 1.7). The stabilizer of any vertex a is the subgroup $\{1, t\}$ of D_8 , where t is the reflection about the line of symmetry passing through vertex a and the center of the square. The kernel of this action is the identity subgroup since only the identity symmetry fixes every vertex.
- (2) The group $G = D_8$ also acts on the set A whose elements are the two unordered pairs of opposite vertices (in the labelling of Figure 2 in Section 1.2, $A = \{\{1, 3\}, \{2, 4\}\}$). The kernel of the action of D_8 on this set A is the subgroup $\{1, s, r^2, sr^2\}$ and for either element $a \in A$ the stabilizer of a in D_8 equals the kernel of the action.

Finally, we observe that the fact that centralizers, normalizers and kernels are subgroups is a special case of the facts that stabilizers and kernels of actions are subgroups (this will be discussed further in Chapter 4). Let $S = \mathcal{P}(G)$, the collection of all subsets of G , and let G act on S by *conjugation*, that is, for each $g \in G$ and each $B \subseteq G$ let

$$g : B \rightarrow gBg^{-1} \quad \text{where} \quad gBg^{-1} = \{gbg^{-1} \mid b \in B\}$$

(see Exercise 16 in Section 1.7). Under this action, it is easy to check that $N_G(A)$ is precisely the stabilizer of A in G (i.e., $N_G(A) = G_s$ where $s = A \in \mathcal{P}(G)$), so $N_G(A)$ is a subgroup of G .

Next let the group $N_G(A)$ act on the set $S = A$ by conjugation, i.e., for all $g \in N_G(A)$ and $a \in A$

$$g : a \mapsto gag^{-1}.$$

Note that this does map A to A by the definition of $N_G(A)$ and so gives an action on A . Here it is easy to check that $C_G(A)$ is precisely the kernel of this action, hence $C_G(A) \leq N_G(A)$; by transitivity of the relation " \leq ", $C_G(A) \leq G$. Finally, $Z(G)$ is the kernel of G acting on $S = G$ by conjugation, so $Z(G) \leq G$.

EXERCISES

1. Prove that $C_G(A) = \{g \in G \mid g^{-1}ag = a \text{ for all } a \in A\}$.
2. Prove that $C_G(Z(G)) = G$ and deduce that $N_G(Z(G)) = G$.
3. Prove that if A and B are subsets of G with $A \subseteq B$ then $C_G(B)$ is a subgroup of $C_G(A)$.
4. For each of S_3 , D_8 , and Q_8 compute the centralizers of each element and find the center of each group. Does Lagrange's Theorem (Exercise 19 in Section 1.7) simplify your work?
5. In each of parts (a) to (c) show that for the specified group G and subgroup A of G , $C_G(A) = A$ and $N_G(A) = G$.
 - (a) $G = S_3$ and $A = \{1, (1 2 3), (1 3 2)\}$.
 - (b) $G = D_8$ and $A = \{1, s, r^2, sr^2\}$.
 - (c) $G = D_{10}$ and $A = \{1, r, r^2, r^3, r^4\}$.
6. Let H be a subgroup of the group G .
 - (a) Show that $H \leq N_G(H)$. Give an example to show that this is not necessarily true if H is not a subgroup.
 - (b) Show that $H \leq C_G(H)$ if and only if H is abelian.
7. Let $n \in \mathbb{Z}$ with $n \geq 3$. Prove the following:
 - (a) $Z(D_{2n}) = 1$ if n is odd

- (b) $Z(D_{2n}) = \{1, r^k\}$ if $n = 2k$.
8. Let $G = S_n$, fix an $i \in \{1, 2, \dots, n\}$ and let $G_i = \{\sigma \in G \mid \sigma(i) = i\}$ (the stabilizer of i in G). Use group actions to prove that G_i is a subgroup of G . Find $|G_i|$.
9. For any subgroup H of G and any nonempty subset A of G define $N_H(A)$ to be the set $\{h \in H \mid hAh^{-1} = A\}$. Show that $N_H(A) = N_G(A) \cap H$ and deduce that $N_H(A)$ is a subgroup of H (note that A need not be a subset of H).
10. Let H be a subgroup of order 2 in G . Show that $N_G(H) = C_G(H)$. Deduce that if $N_G(H) = G$ then $H \leq Z(G)$.
11. Prove that $Z(G) \leq N_G(A)$ for any subset A of G .
12. Let R be the set of all polynomials with integer coefficients in the independent variables x_1, x_2, x_3, x_4 i.e., the members of R are finite sums of elements of the form $ax_1^{r_1}x_2^{r_2}x_3^{r_3}x_4^{r_4}$, where a is any integer and r_1, \dots, r_4 are nonnegative integers. For example,
- $$12x_1^5x_2^7x_4 - 18x_1^3x_3 + 11x_1^6x_2x_3^3x_4^{23} \quad (*)$$
- is a typical element of R . Each $\sigma \in S_4$ gives a permutation of $\{x_1, \dots, x_4\}$ by defining $\sigma \cdot x_i = x_{\sigma(i)}$. This may be extended to a map from R to R by defining
- $$\sigma \cdot p(x_1, x_2, x_3, x_4) = p(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}, x_{\sigma(4)})$$
- for all $p(x_1, x_2, x_3, x_4) \in R$ (i.e., σ simply permutes the indices of the variables). For example, if $\sigma = (1\ 2\ 3\ 4)$ and $p(x_1, \dots, x_4)$ is the polynomial in $(*)$ above, then
- $$\begin{aligned} \sigma \cdot p(x_1, x_2, x_3, x_4) &= 12x_2^5x_1^7x_3 - 18x_1^3x_4 + 11x_2^6x_1x_4^3x_3^{23} \\ &= 12x_1^7x_2^5x_3 - 18x_1^3x_4 + 11x_1x_2^6x_3^{23}x_4^3. \end{aligned}$$
- (a) Let $p = p(x_1, \dots, x_4)$ be the polynomial in $(*)$ above, let $\sigma = (1\ 2\ 3\ 4)$ and let $\tau = (1\ 2\ 3)$. Compute $\sigma \cdot p$, $\tau \cdot (\sigma \cdot p)$, $(\tau \circ \sigma) \cdot p$, and $(\sigma \circ \tau) \cdot p$.
- (b) Prove that these definitions give a (left) group action of S_4 on R .
- (c) Exhibit all permutations in S_4 that stabilize x_4 and prove that they form a subgroup isomorphic to S_3 .
- (d) Exhibit all permutations in S_4 that stabilize the element $x_1 + x_2$ and prove that they form an abelian subgroup of order 4.
- (e) Exhibit all permutations in S_4 that stabilize the element $x_1x_2 + x_3x_4$ and prove that they form a subgroup isomorphic to the dihedral group of order 8.
- (f) Show that the permutations in S_4 that stabilize the element $(x_1 + x_2)(x_3 + x_4)$ are exactly the same as those found in part (e). (The two polynomials appearing in parts (e) and (f) and the subgroup that stabilizes them will play an important role in the study of roots of quartic equations in Section 14.6.)
13. Let n be a positive integer and let R be the set of all polynomials with integer coefficients in the independent variables x_1, x_2, \dots, x_n , i.e., the members of R are finite sums of elements of the form $ax_1^{r_1}x_2^{r_2} \cdots x_n^{r_n}$, where a is any integer and r_1, \dots, r_n are nonnegative integers. For each $\sigma \in S_n$ define a map
- $$\sigma : R \rightarrow R \quad \text{by} \quad \sigma \cdot p(x_1, x_2, \dots, x_n) = p(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}).$$
- Prove that this defines a (left) group action of S_n on R .
14. Let $H(F)$ be the Heisenberg group over the field F introduced in Exercise 11 of Section 1.4. Determine which matrices lie in the center of $H(F)$ and prove that $Z(H(F))$ is isomorphic to the additive group F .

2.3 CYCLIC GROUPS AND CYCLIC SUBGROUPS

Let G be any group and let x be any element of G . One way of forming a subgroup H of G is by letting H be the set of all integer (positive, negative and zero) powers of x (this guarantees closure under inverses and products at least as far as x is concerned). In this section we study groups which are generated by one element.

Definition. A group H is *cyclic* if H can be generated by a single element, i.e., there is some element $x \in H$ such that $H = \{x^n \mid n \in \mathbb{Z}\}$ (where as usual the operation is multiplication).

In additive notation H is cyclic if $H = \{nx \mid n \in \mathbb{Z}\}$. In both cases we shall write $H = \langle x \rangle$ and say H is *generated* by x (and x is a *generator* of H). A cyclic group may have more than one generator. For example, if $H = \langle x \rangle$, then also $H = \langle x^{-1} \rangle$ because $(x^{-1})^n = x^{-n}$ and as n runs over all integers so does $-n$ so that

$$\{x^n \mid n \in \mathbb{Z}\} = \{(x^{-1})^n \mid n \in \mathbb{Z}\}.$$

We shall shortly show how to determine all generators for a given cyclic group H . One should note that the elements of $\langle x \rangle$ are powers of x (or multiples of x , in groups written additively) and not integers. It is not necessarily true that all powers of x are distinct. Also, by the laws for exponents (Exercise 19 in Section 1.1) cyclic groups are abelian.

Examples

- (1) Let $G = D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$, $n \geq 3$ and let H be the subgroup of all rotations of the n -gon. Thus $H = \langle r \rangle$ and the distinct elements of H are $1, r, r^2, \dots, r^{n-1}$ (these are all the distinct powers of r). In particular, $|H| = n$ and the generator, r , of H has order n . The powers of r “cycle” (forward and backward) with period n , that is,

$$\begin{aligned} r^n &= 1, & r^{n+1} &= r, & r^{n+2} &= r^2, \dots \\ r^{-1} &= r^{n-1}, & r^{-2} &= r^{n-2}, \dots & \text{etc.} \end{aligned}$$

In general, to write any power of r , say r^t , in the form r^k , for some k between 0 and $n - 1$ use the Division Algorithm to write

$$t = nq + k, \quad \text{where } 0 \leq k < n,$$

so that

$$r^t = r^{nq+k} = (r^n)^q r^k = 1^q r^k = r^k.$$

For example, in D_8 , $r^4 = 1$ so $r^{105} = r^{4(26)+1} = r$ and $r^{-42} = r^{4(-11)+2} = r^2$. Observe that D_{2n} itself is not a cyclic group since it is non-abelian.

- (2) Let $H = \mathbb{Z}$ with operation $+$. Thus $H = \langle 1 \rangle$ (here 1 is the integer 1 and the identity of H is 0) and each element in H can be written uniquely in the form $n \cdot 1$, for some $n \in \mathbb{Z}$. In contrast to the preceding example, multiples of the generator are all distinct and we need to take both positive, negative and zero multiples of the generator to obtain all elements of H . In this example $|H|$ and the order of the generator 1 are both ∞ . Note also that $H = \langle -1 \rangle$ since each integer x can be written (uniquely) as $(-x)(-1)$.

Before discussing cyclic groups further we prove that the various properties of finite and infinite cyclic groups we observed in the preceding two examples are generic. This proposition also validates the claim (in Chapter 1) that the use of the terminology for “order” of an element and the use of the symbol $| |$ are consistent with the notion of order of a set.

Proposition 2. If $H = \langle x \rangle$, then $|H| = |x|$ (where if one side of this equality is infinite, so is the other). More specifically

- (1) if $|H| = n < \infty$, then $x^n = 1$ and $1, x, x^2, \dots, x^{n-1}$ are all the distinct elements of H , and
- (2) if $|H| = \infty$, then $x^n \neq 1$ for all $n \neq 0$ and $x^a \neq x^b$ for all $a \neq b$ in \mathbb{Z} .

Proof: Let $|x| = n$ and first consider the case when $n < \infty$. The elements $1, x, x^2, \dots, x^{n-1}$ are distinct because if $x^a = x^b$, with, say, $0 \leq a < b < n$, then $x^{b-a} = x^0 = 1$, contrary to n being the smallest positive power of x giving the identity. Thus H has at least n elements and it remains to show that these are all of them. As we did in Example 1, if x^t is any power of x , use the Division Algorithm to write $t = nq + k$, where $0 \leq k < n$, so

$$x^t = x^{nq+k} = (x^n)^q x^k = 1^q x^k = x^k \in \{1, x, x^2, \dots, x^{n-1}\},$$

as desired.

Next suppose $|x| = \infty$ so no positive power of x is the identity. If $x^a = x^b$, for some a and b with, say, $a < b$, then $x^{b-a} = 1$, a contradiction. Distinct powers of x are distinct elements of H so $|H| = \infty$. This completes the proof of the proposition.

Note that the proof of the proposition gives the method for reducing arbitrary powers of a generator in a finite cyclic group to the “least residue” powers. It is not a coincidence that the calculations of distinct powers of a generator of a cyclic group of order n are carried out via arithmetic in $\mathbb{Z}/n\mathbb{Z}$. Theorem 4 following proves that these two groups are isomorphic.

First we need an easy proposition.

Proposition 3. Let G be an arbitrary group, $x \in G$ and let $m, n \in \mathbb{Z}$. If $x^n = 1$ and $x^m = 1$, then $x^d = 1$, where $d = (m, n)$. In particular, if $x^m = 1$ for some $m \in \mathbb{Z}$, then $|x|$ divides m .

Proof: By the Euclidean Algorithm (see Section 0.2 (6)) there exist integers r and s such that $d = mr + ns$, where d is the g.c.d. of m and n . Thus

$$x^d = x^{mr+ns} = (x^m)^r (x^n)^s = 1^r 1^s = 1.$$

This proves the first assertion.

If $x^m = 1$, let $n = |x|$. If $m = 0$, certainly $n \mid m$, so we may assume $m \neq 0$. Since some nonzero power of x is the identity, $n < \infty$. Let $d = (m, n)$ so by the preceding result $x^d = 1$. Since $0 < d \leq n$ and n is the smallest positive power of x which gives the identity, we must have $d = n$, that is, $n \mid m$, as asserted.

Theorem 4. Any two cyclic groups of the same order are isomorphic. More specifically,

(1) if $n \in \mathbb{Z}^+$ and $\langle x \rangle$ and $\langle y \rangle$ are both cyclic groups of order n , then the map

$$\begin{aligned}\varphi : \langle x \rangle &\rightarrow \langle y \rangle \\ x^k &\mapsto y^k\end{aligned}$$

is well defined and is an isomorphism

(2) if $\langle x \rangle$ is an infinite cyclic group, the map

$$\begin{aligned}\varphi : \mathbb{Z} &\rightarrow \langle x \rangle \\ k &\mapsto x^k\end{aligned}$$

is well defined and is an isomorphism.

Proof: Suppose $\langle x \rangle$ and $\langle y \rangle$ are both cyclic groups of order n . Let $\varphi : \langle x \rangle \rightarrow \langle y \rangle$ be defined by $\varphi(x^k) = y^k$; we must first prove φ is well defined, that is,

$$\text{if } x^r = x^s, \text{ then } \varphi(x^r) = \varphi(x^s).$$

Since $x^{r-s} = 1$, Proposition 3 implies $n \mid r - s$. Write $r = tn + s$ so

$$\begin{aligned}\varphi(x^r) &= \varphi(x^{tn+s}) \\ &= y^{tn+s} \\ &= (y^n)^t y^s \\ &= y^s = \varphi(x^s).\end{aligned}$$

This proves φ is well defined. It is immediate from the laws of exponents that $\varphi(x^a x^b) = \varphi(x^a)\varphi(x^b)$ (check this), that is, φ is a homomorphism. Since the element y^k of $\langle y \rangle$ is the image of x^k under φ , this map is surjective. Since both groups have the same finite order, any surjection from one to the other is a bijection, so φ is an isomorphism (alternatively, φ has an obvious two-sided inverse).

If $\langle x \rangle$ is an infinite cyclic group, let $\varphi : \mathbb{Z} \rightarrow \langle x \rangle$ be defined by $\varphi(k) = x^k$. Note that this map is already well defined since there is no ambiguity in the representation of elements in the domain. Since (by Proposition 2) $x^a \neq x^b$, for all distinct $a, b \in \mathbb{Z}$, φ is injective. By definition of a cyclic group, φ is surjective. As above, the laws of exponents ensure φ is a homomorphism, hence φ is an isomorphism, completing the proof.

We chose to use the rotation group $\langle r \rangle$ as our prototypical example of a finite cyclic group of order n (instead of the isomorphic group $\mathbb{Z}/n\mathbb{Z}$) since we shall usually write our cyclic groups multiplicatively:

Notation: For each $n \in \mathbb{Z}^+$, let Z_n be the cyclic group of order n (written multiplicatively).

Up to isomorphism, Z_n is the unique cyclic group of order n and $Z_n \cong \mathbb{Z}/n\mathbb{Z}$. On occasion when we find additive notation advantageous we shall use the latter group as

our representative of the isomorphism class of cyclic groups of order n . We shall occasionally say “let $\langle x \rangle$ be the infinite cyclic group” (written multiplicatively), however we shall always use \mathbb{Z} (additively) to represent the infinite cyclic group.

As noted earlier, a given cyclic group may have more than one generator. The next two propositions determine precisely which powers of x generate the group $\langle x \rangle$.

Proposition 5. Let G be a group, let $x \in G$ and let $a \in \mathbb{Z} - \{0\}$.

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

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

(3) In particular, if $|x| = n < \infty$ and a is a positive integer dividing n , then $|x^a| = \frac{n}{a}$.

Proof: (1) By way of contradiction assume $|x| = \infty$ but $|x^a| = m < \infty$. By definition of order

$$1 = (x^a)^m = x^{am}.$$

Also,

$$x^{-am} = (x^{am})^{-1} = 1^{-1} = 1.$$

Now one of am or $-am$ is positive (since neither a nor m is 0) so some positive power of x is the identity. This contradicts the hypothesis $|x| = \infty$, so the assumption $|x^a| < \infty$ must be false, that is, (1) holds.

(2) Under the notation of (2) let

$$y = x^a, \quad (n, a) = d \quad \text{and write} \quad n = db, \quad a = dc,$$

for suitable $b, c \in \mathbb{Z}$ with $b > 0$. Since d is the greatest common divisor of n and a , the integers b and c are relatively prime:

$$(b, c) = 1.$$

To establish (2) we must show $|y| = b$. First note that

$$y^b = x^{ab} = x^{dcb} = (x^{db})^c = (x^n)^c = 1^c = 1$$

so, by Proposition 3 applied to $\langle y \rangle$, we see that $|y|$ divides b . Let $k = |y|$. Then

$$x^{ak} = y^k = 1$$

so by Proposition 3 applied to $\langle x \rangle$, $n \mid ak$, i.e., $db \mid dck$. Thus $b \mid ck$. Since b and c have no factors in common, b must divide k . Since b and k are positive integers which divide each other, $b = k$, which proves (2).

(3) This is a special case of (2) recorded for future reference.

Proposition 6. Let $H = \langle x \rangle$.

(1) Assume $|x| = \infty$. Then $H = \langle x^a \rangle$ if and only if $a = \pm 1$.

(2) Assume $|x| = n < \infty$. Then $H = \langle x^a \rangle$ if and only if $(a, n) = 1$. In particular, the number of generators of H is $\varphi(n)$ (where φ is Euler's φ -function).

Proof: We leave (1) as an exercise. In (2) if $|x| = n < \infty$, Proposition 2 says x^a generates a subgroup of H of order $|x^a|$. This subgroup equals all of H if and only if $|x^a| = |x|$. By Proposition 5,

$$|x^a| = |x| \quad \text{if and only if} \quad \frac{n}{(a, n)} = n, \quad \text{i.e. if and only if } (a, n) = 1.$$

Since $\varphi(n)$ is, by definition, the number of $a \in \{1, 2, \dots, n\}$ such that $(a, n) = 1$, this is the number of generators of H .

Example

Proposition 6 tells precisely which residue classes mod n generate $\mathbb{Z}/n\mathbb{Z}$: namely, \bar{a} generates $\mathbb{Z}/n\mathbb{Z}$ if and only if $(a, n) = 1$. For instance, $\bar{1}, \bar{5}, \bar{7}$ and $\bar{11}$ are the generators of $\mathbb{Z}/12\mathbb{Z}$ and $\varphi(12) = 4$.

The final theorem in this section gives the complete subgroup structure of a cyclic group.

Theorem 7. Let $H = \langle x \rangle$ be a cyclic group.

- (1) Every subgroup of H is cyclic. More precisely, if $K \leq H$, then either $K = \{1\}$ or $K = \langle x^d \rangle$, where d is the smallest positive integer such that $x^d \in K$.
- (2) If $|H| = \infty$, then for any distinct nonnegative integers a and b , $\langle x^a \rangle \neq \langle x^b \rangle$. Furthermore, for every integer m , $\langle x^m \rangle = \langle x^{|m|} \rangle$, where $|m|$ denotes the absolute value of m , so that the nontrivial subgroups of H correspond bijectively with the integers $1, 2, 3, \dots$.
- (3) If $|H| = n < \infty$, then for each positive integer a dividing n there is a unique subgroup of H of order a . This subgroup is the cyclic group $\langle x^d \rangle$, where $d = \frac{n}{a}$. Furthermore, for every integer m , $\langle x^m \rangle = \langle x^{(n,m)} \rangle$, so that the subgroups of H correspond bijectively with the positive divisors of n .

Proof: (1) Let $K \leq H$. If $K = \{1\}$, the proposition is true for this subgroup, so we assume $K \neq \{1\}$. Thus there exists some $a \neq 0$ such that $x^a \in K$. If $a < 0$ then since K is a group also $x^{-a} = (x^a)^{-1} \in K$. Hence K always contains some positive power of x . Let

$$\mathcal{P} = \{b \mid b \in \mathbb{Z}^+ \text{ and } x^b \in K\}.$$

By the above, \mathcal{P} is a nonempty set of positive integers. By the Well Ordering Principle (Section 0.2) \mathcal{P} has a minimum element — call it d . Since K is a subgroup and $x^d \in K$, $\langle x^d \rangle \subseteq K$. Since K is a subgroup of H , any element of K is of the form x^a for some integer a . By the Division Algorithm write

$$a = qd + r \quad 0 \leq r < d.$$

Then $x^r = x^{(a-qd)} = x^a(x^d)^{-q}$ is an element of K since both x^a and x^d are elements of K . By the minimality of d it follows that $r = 0$, i.e., $a = qd$ and so $x^a = (x^d)^q \in \langle x^d \rangle$. This gives the reverse containment $K \subseteq \langle x^d \rangle$ which proves (1).

We leave the proof of (2) as an exercise (the reasoning is similar to and easier than the proof of (3) which follows).

(3) Assume $|H| = n < \infty$ and $a \mid n$. Let $d = \frac{n}{a}$ and apply Proposition 5(3) to obtain that $\langle x^d \rangle$ is a subgroup of order a , showing the existence of a subgroup of order a . To show uniqueness, suppose K is any subgroup of H of order a . By part (1) we have

$$K = \langle x^b \rangle$$

where b is the smallest positive integer such that $x^b \in K$. By Proposition 5

$$\frac{n}{d} = a = |K| = |x^b| = \frac{n}{(n, b)},$$

so $d = (n, b)$. In particular, $d \mid b$. Since b is a multiple of d , $x^b \in \langle x^d \rangle$, hence

$$K = \langle x^b \rangle \leq \langle x^d \rangle.$$

Since $|\langle x^d \rangle| = a = |K|$, we have $K = \langle x^d \rangle$.

The final assertion of (3) follows from the observation that $\langle x^m \rangle$ is a subgroup of $\langle x^{(n,m)} \rangle$ (check this) and, it follows from Proposition 5(2) and Proposition 2 that they have the same order. Since (n, m) is certainly a divisor of n , this shows that every subgroup of H arises from a divisor of n , completing the proof.

Examples

(1) We can use Proposition 6 and Theorem 7 to list all the subgroups of $\mathbb{Z}/n\mathbb{Z}$ for any given n . For example, the subgroups of $\mathbb{Z}/12\mathbb{Z}$ are

- (a) $\mathbb{Z}/12\mathbb{Z} = \langle \bar{1} \rangle = \langle \bar{5} \rangle = \langle \bar{7} \rangle = \langle \bar{11} \rangle$ (order 12)
- (b) $\langle \bar{2} \rangle = \langle \bar{10} \rangle$ (order 6)
- (c) $\langle \bar{3} \rangle = \langle \bar{9} \rangle$ (order 4)
- (d) $\langle \bar{4} \rangle = \langle \bar{8} \rangle$ (order 3)
- (e) $\langle \bar{6} \rangle$ (order 2)
- (f) $\langle \bar{0} \rangle$ (order 1).

The inclusions between them are given by

$$\langle \bar{a} \rangle \leq \langle \bar{b} \rangle \quad \text{if and only if } (b, 12) \mid (a, 12), \quad 1 \leq a, b \leq 12.$$

(2) We can also combine the results of this section with those of the preceding one. For example, we can obtain subgroups of a group G by forming $C_G(\langle x \rangle)$ and $N_G(\langle x \rangle)$, for each $x \in G$. One can check that an element g in G commutes with x if and only if g commutes with all powers of x , hence

$$C_G(\langle x \rangle) = C_G(x).$$

As noted in Exercise 6, Section 2, $\langle x \rangle \leq N_G(\langle x \rangle)$ but equality need not hold. For instance, if $G = Q_8$ and $x = i$,

$$C_G(\langle i \rangle) = \{\pm 1, \pm i\} = \langle i \rangle \quad \text{and} \quad N_G(\langle i \rangle) = Q_8.$$

Note that we already observed the first of the above two equalities and the second is most easily computed using the result of Exercise 24 following.

EXERCISES

1. Find all subgroups of $Z_{45} = \langle x \rangle$, giving a generator for each. Describe the containments between these subgroups.
2. If x is an element of the finite group G and $|x| = |G|$, prove that $G = \langle x \rangle$. Give an explicit example to show that this result need not be true if G is an infinite group.
3. Find all generators for $\mathbb{Z}/48\mathbb{Z}$.
4. Find all generators for $\mathbb{Z}/202\mathbb{Z}$.
5. Find the number of generators for $\mathbb{Z}/49000\mathbb{Z}$.
6. In $\mathbb{Z}/48\mathbb{Z}$ write out all elements of $\langle \bar{a} \rangle$ for every \bar{a} . Find all inclusions between subgroups in $\mathbb{Z}/48\mathbb{Z}$.
7. Let $Z_{48} = \langle x \rangle$ and use the isomorphism $\mathbb{Z}/48\mathbb{Z} \cong Z_{48}$ given by $\bar{1} \mapsto x$ to list all subgroups of Z_{48} as computed in the preceding exercise.
8. Let $Z_{48} = \langle x \rangle$. For which integers a does the map φ_a defined by $\varphi_a : \bar{1} \mapsto x^a$ extend to an *isomorphism* from $\mathbb{Z}/48\mathbb{Z}$ onto Z_{48} .
9. Let $Z_{36} = \langle x \rangle$. For which integers a does the map ψ_a defined by $\psi_a : \bar{1} \mapsto x^a$ extend to a *well defined homomorphism* from $\mathbb{Z}/48\mathbb{Z}$ into Z_{36} . Can ψ_a ever be a surjective homomorphism?
10. What is the order of $\overline{30}$ in $\mathbb{Z}/54\mathbb{Z}$? Write out all of the elements and their orders in $\langle \overline{30} \rangle$.
11. Find all cyclic subgroups of D_8 . Find a proper subgroup of D_8 which is not cyclic.
12. Prove that the following groups are *not* cyclic:
 - $\mathbb{Z}_2 \times \mathbb{Z}_2$
 - $\mathbb{Z}_2 \times \mathbb{Z}$
 - $\mathbb{Z} \times \mathbb{Z}$.
13. Prove that the following pairs of groups are *not* isomorphic:
 - $\mathbb{Z} \times \mathbb{Z}_2$ and \mathbb{Z}
 - $\mathbb{Q} \times \mathbb{Z}_2$ and \mathbb{Q} .
14. Let $\sigma = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12)$. For each of the following integers a compute σ^a :
 $a = 13, 65, 626, 1195, -6, -81, -570$ and -1211 .
15. Prove that $\mathbb{Q} \times \mathbb{Q}$ is not cyclic.
16. Assume $|x| = n$ and $|y| = m$. Suppose that x and y *commute*: $xy = yx$. Prove that $|xy|$ divides the least common multiple of m and n . Need this be true if x and y do *not* commute? Give an example of commuting elements x, y such that the order of xy is not equal to the least common multiple of $|x|$ and $|y|$.
17. Find a presentation for Z_n with one generator.
18. Show that if H is any group and h is an element of H with $h^n = 1$, then there is a unique homomorphism from $Z_n = \langle x \rangle$ to H such that $x \mapsto h$.
19. Show that if H is any group and h is an element of H , then there is a unique homomorphism from \mathbb{Z} to H such that $1 \mapsto h$.
20. Let p be a prime and let n be a positive integer. Show that if x is an element of the group G such that $x^{p^n} = 1$ then $|x| = p^m$ for some $m \leq n$.
21. Let p be an odd prime and let n be a positive integer. Use the Binomial Theorem to show that $(1 + p)^{p^{n-1}} \equiv 1 \pmod{p^n}$ but $(1 + p)^{p^{n-2}} \not\equiv 1 \pmod{p^n}$. Deduce that $1 + p$ is an element of order p^{n-1} in the multiplicative group $(\mathbb{Z}/p^n\mathbb{Z})^\times$.

22. Let n be an integer ≥ 3 . Use the Binomial Theorem to show that $(1+2^2)^{2^{n-2}} \equiv 1 \pmod{2^n}$ but $(1+2^2)^{2^{n-3}} \not\equiv 1 \pmod{2^n}$. Deduce that 5 is an element of order 2^{n-2} in the multiplicative group $(\mathbb{Z}/2^n\mathbb{Z})^\times$.
23. Show that $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is not cyclic for any $n \geq 3$. [Find two distinct subgroups of order 2.]
24. Let G be a finite group and let $x \in G$.
- Prove that if $g \in N_G(\langle x \rangle)$ then $gxg^{-1} = x^a$ for some $a \in \mathbb{Z}$.
 - Prove conversely that if $gxg^{-1} = x^a$ for some $a \in \mathbb{Z}$ then $g \in N_G(\langle x \rangle)$. [Show first that $gx^k g^{-1} = (gxg^{-1})^k = x^{ak}$ for any integer k , so that $g \langle x \rangle g^{-1} \leq \langle x \rangle$. If x has order n , show the elements $gx^i g^{-1}$, $i = 0, 1, \dots, n-1$ are distinct, so that $|g \langle x \rangle g^{-1}| = |\langle x \rangle| = n$ and conclude that $g \langle x \rangle g^{-1} = \langle x \rangle$.]
- Note that this cuts down some of the work in computing normalizers of cyclic subgroups since one does not have to check $ghg^{-1} \in \langle x \rangle$ for every $h \in \langle x \rangle$.
25. Let G be a cyclic group of order n and let k be an integer relatively prime to n . Prove that the map $x \mapsto x^k$ is surjective. Use Lagrange's Theorem (Exercise 19, Section 1.7) to prove the same is true for any finite group of order n . (For such k each element has a k^{th} root in G . It follows from Cauchy's Theorem in Section 3.2 that if k is not relatively prime to the order of G then the map $x \mapsto x^k$ is not surjective.)
26. Let Z_n be a cyclic group of order n and for each integer a let

$$\sigma_a : Z_n \rightarrow Z_n \quad \text{by} \quad \sigma_a(x) = x^a \text{ for all } x \in Z_n.$$

- Prove that σ_a is an automorphism of Z_n if and only if a and n are relatively prime (automorphisms were introduced in Exercise 20, Section 1.6).
- Prove that $\sigma_a = \sigma_b$ if and only if $a \equiv b \pmod{n}$.
- Prove that every automorphism of Z_n is equal to σ_a for some integer a .
- Prove that $\sigma_a \circ \sigma_b = \sigma_{ab}$. Deduce that the map $\bar{a} \mapsto \sigma_a$ is an isomorphism of $(\mathbb{Z}/n\mathbb{Z})^\times$ onto the automorphism group of Z_n (so $\text{Aut}(Z_n)$ is an abelian group of order $\varphi(n)$).

2.4 SUBGROUPS GENERATED BY SUBSETS OF A GROUP

The method of forming cyclic subgroups of a given group is a special case of the general technique where one forms the subgroup generated by an arbitrary subset of a group. In the case of cyclic subgroups one takes a singleton subset $\{x\}$ of the group G and forms all integral powers of x , which amounts to closing the set $\{x\}$ under the group operation and the process of taking inverses. The resulting subgroup is the smallest subgroup of G which contains the set $\{x\}$ (smallest in the sense that if H is any subgroup which contains $\{x\}$, then H contains $\langle x \rangle$). Another way of saying this is that $\langle x \rangle$ is the unique minimal element of the set of subgroups of G containing x (ordered under inclusion). In this section we investigate analogues of this when $\{x\}$ is replaced by an arbitrary subset of G .

Throughout mathematics the following theme recurs: given an object G (such as a group, field, vector space, etc.) and a subset A of G , is there a unique minimal subobject of G (subgroup, subfield, subspace, etc.) which contains A and, if so, how are the elements of this subobject computed? Students may already have encountered this question in the study of vector spaces. When G is a vector space (with, say, real number scalars) and $A = \{v_1, v_2, \dots, v_n\}$, then there is a unique smallest subspace of

G which contains A , namely the (linear) span of v_1, v_2, \dots, v_n and each vector in this span can be written as $k_1v_1 + k_2v_2 + \dots + k_nv_n$, for some $k_1, \dots, k_n \in \mathbb{R}$. When A is a single nonzero vector, v , the span of $\{v\}$ is simply the 1-dimensional subspace or line containing v and every element of this subspace is of the form kv for some $k \in \mathbb{R}$. This is the analogue in the theory of vector spaces of cyclic subgroups of a group. Note that the 1-dimensional subspaces contain kv , where $k \in \mathbb{R}$, not just kv , where $k \in \mathbb{Z}$; the reason being that a subspace must be closed under *all* the vector space operations (e.g., scalar multiplication) not just the group operation of vector addition.

Let G be any group and let A be any subset of G . We now make precise the notion of the subgroup of G generated by A . We prove that because the intersection of any set of subgroups of G is also a subgroup of G , the subgroup generated by A is the unique smallest subgroup of G containing A ; it is “smallest” in the sense of being the minimal element of the set of all subgroups containing A . We show that the elements of this subgroup are obtained by closing the given subset under the group operation (and taking inverses). In succeeding parts of the text when we develop the theory of other algebraic objects we shall refer to this section as the paradigm in proving that a given subset is contained in a unique smallest subobject and that the elements of this subobject are obtained by closing the subset under the operations which define the object. Since in the latter chapters the details will be omitted, students should acquire a solid understanding of the process at this point.

In order to proceed we need only the following.

Proposition 8. If \mathcal{A} is any nonempty collection of subgroups of G , then the intersection of all members of \mathcal{A} is also a subgroup of G .

Proof: This is an easy application of the subgroup criterion (see also Exercise 10, Section 1). Let

$$K = \bigcap_{H \in \mathcal{A}} H.$$

Since each $H \in \mathcal{A}$ is a subgroup, $1 \in H$, so $1 \in K$, that is, $K \neq \emptyset$. If $a, b \in K$, then $a, b \in H$, for all $H \in \mathcal{A}$. Since each H is a group, $ab^{-1} \in H$, for all H , hence $ab^{-1} \in K$. Proposition 1 gives that $K \leq G$.

Definition. If A is any subset of the group G define

$$\langle A \rangle = \bigcap_{\substack{A \subseteq H \\ H \leq G}} H.$$

This is called the *subgroup of G generated by A* .

Thus $\langle A \rangle$ is the intersection of all subgroups of G containing A . It is a subgroup of G by Proposition 8 applied to the set $\mathcal{A} = \{H \leq G \mid A \subseteq H\}$ (\mathcal{A} is nonempty since $G \in \mathcal{A}$). Since A lies in each $H \in \mathcal{A}$, A is a subset of their intersection, $\langle A \rangle$. Note that $\langle A \rangle$ is the unique minimal element of \mathcal{A} as follows: $\langle A \rangle$ is a subgroup of G containing A , so $\langle A \rangle \in \mathcal{A}$; and any element of \mathcal{A} contains the intersection of all elements in \mathcal{A} , i.e., contains $\langle A \rangle$.

When A is the finite set $\{a_1, a_2, \dots, a_n\}$ we write $\langle a_1, a_2, \dots, a_n \rangle$ for the group generated by a_1, a_2, \dots, a_n instead of $\langle \{a_1, a_2, \dots, a_n\} \rangle$. If A and B are two subsets of G we shall write $\langle A, B \rangle$ in place of $\langle A \cup B \rangle$.

This “top down” approach to defining $\langle A \rangle$ proves existence and uniqueness of the smallest subgroup of G containing A but is not too enlightening as to how to construct the elements in it. As the word “generates” suggests we now define the set which is the closure of A under the group operation (and the process of taking inverses) and prove this set equals $\langle A \rangle$. Let

$$\overline{A} = \{a_1^{\epsilon_1} a_2^{\epsilon_2} \dots a_n^{\epsilon_n} \mid n \in \mathbb{Z}, n \geq 0 \text{ and } a_i \in A, \epsilon_i = \pm 1 \text{ for each } i\}$$

where $\overline{A} = \{1\}$ if $A = \emptyset$, so that \overline{A} is the set of all finite products (called *words*) of elements of A and inverses of elements of A . Note that the a_i 's need not be distinct, so a^2 is written aa in the notation defining \overline{A} . Note also that A is not assumed to be a finite (or even countable) set.

Proposition 9. $\overline{A} = \langle A \rangle$.

Proof: We first prove \overline{A} is a subgroup. Note that $\overline{A} \neq \emptyset$ (even if $A = \emptyset$). If $a, b \in \overline{A}$ with $a = a_1^{\epsilon_1} a_2^{\epsilon_2} \dots a_n^{\epsilon_n}$ and $b = b_1^{\delta_1} b_2^{\delta_2} \dots b_m^{\delta_m}$, then

$$ab^{-1} = a_1^{\epsilon_1} a_2^{\epsilon_2} \dots a_n^{\epsilon_n} \cdot b_m^{-\delta_m} b_{m-1}^{-\delta_{m-1}} \dots b_1^{-\delta_1}$$

(where we used Exercise 15 of Section 1.1 to compute b^{-1}). Thus ab^{-1} is a product of elements of A raised to powers ± 1 , hence $ab^{-1} \in \overline{A}$. Proposition 1 implies \overline{A} is a subgroup of G .

Since each $a \in A$ may be written a^1 , it follows that $A \subseteq \overline{A}$, hence $\langle A \rangle \subseteq \overline{A}$. But $\langle A \rangle$ is a group containing A and, since it is closed under the group operation and the process of taking inverses, $\langle A \rangle$ contains each element of the form $a_1^{\epsilon_1} a_2^{\epsilon_2} \dots a_n^{\epsilon_n}$, that is, $\overline{A} \subseteq \langle A \rangle$. This completes the proof of the proposition.

We now use $\langle A \rangle$ in place of \overline{A} and may take the definition of \overline{A} as an equivalent definition of $\langle A \rangle$. As noted above, in this equivalent definition of $\langle A \rangle$, products of the form $a \cdot a, a \cdot a \cdot a, a \cdot a^{-1}$, etc. could have been simplified to $a^2, a^3, 1$, etc. respectively, so another way of writing $\langle A \rangle$ is

$$\langle A \rangle = \{a_1^{\alpha_1} a_2^{\alpha_2} \dots a_n^{\alpha_n} \mid \text{for each } i, a_i \in A, \alpha_i \in \mathbb{Z}, a_i \neq a_{i+1} \text{ and } n \in \mathbb{Z}^+\}.$$

In fact, when $A = \{x\}$ this was our definition of $\langle A \rangle$.

If G is *abelian*, we could commute the a_i 's and so collect all powers of a given generator together. For instance, if A were the finite subset $\{a_1, a_2, \dots, a_k\}$ of the abelian group G , one easily checks that

$$\langle A \rangle = \{a_1^{\alpha_1} a_2^{\alpha_2} \dots a_k^{\alpha_k} \mid \alpha_i \in \mathbb{Z} \text{ for each } i\}.$$

If in this situation we further assume that each a_i has finite order d_i , for all i , then since there are exactly d_i distinct powers of a_i , the total number of distinct products of the form $a_1^{\alpha_1} a_2^{\alpha_2} \dots a_k^{\alpha_k}$ is at most $d_1 d_2 \dots d_k$, that is,

$$|\langle A \rangle| \leq d_1 d_2 \dots d_k.$$

It may happen that $a^\alpha b^\beta = a^\gamma b^\delta$ even though $a^\alpha \neq a^\gamma$ and $b^\beta \neq b^\delta$. We shall explore exactly when this happens when we study direct products in Chapter 5.

When G is *non-abelian* the situation is much more complicated. For example, let $G = D_8$ and let r and s be the usual generators of D_8 (note that the notation $D_8 = \langle r, s \rangle$ is consistent with the notation introduced in Section 1.2). Let $a = s$, let $b = rs$ and let $A = \{a, b\}$. Since both s and r ($= rs \cdot s$) belong to $\langle a, b \rangle$, $G = \langle a, b \rangle$, i.e., G is also generated by a and b . Both a and b have order 2, however D_8 has order 8. This means that it is *not* possible to write every element of D_8 in the form $a^\alpha b^\beta$, $\alpha, \beta \in \mathbb{Z}$. More specifically, the product aba cannot be simplified to a product of the form $a^\alpha b^\beta$. In fact, if $G = D_{2n}$ for any $n > 2$, and r, s, a, b are defined in the same way as above, it is still true that

$$|a| = |b| = 2, \quad D_{2n} = \langle a, b \rangle \quad \text{and} \quad |D_{2n}| = 2n.$$

This means that for large n , long products of the form $abab\dots ab$ cannot be further simplified. In particular, this illustrates that, unlike the abelian (or, better yet, cyclic) group case, the order of a (finite) group cannot even be bounded once we know the orders of the elements in some generating set.

Another example of this phenomenon is S_n :

$$S_n = \langle (1\ 2), (1\ 2\ 3\dots n) \rangle.$$

Thus S_n is generated by an element of order 2 together with one of order n , yet $|S_n| = n!$ (we shall prove these statements later after developing some more techniques).

One final example emphasizes the fact that if G is non-abelian, subgroups of G generated by more than one element of G may be quite complicated. Let

$$G = GL_2(\mathbb{R}), \quad a = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad b = \begin{pmatrix} 0 & 2 \\ 1/2 & 0 \end{pmatrix}$$

so $a^2 = b^2 = 1$ but $ab = \begin{pmatrix} 1/2 & 0 \\ 0 & 2 \end{pmatrix}$. It is easy to see that ab has infinite order, so $\langle a, b \rangle$ is an *infinite* subgroup of $GL_2(\mathbb{R})$ which is generated by two elements of order 2.

These examples illustrate that when $|A| \geq 2$ it is difficult, in general, to compute even the order of the subgroup generated by A , let alone any other structural properties. It is therefore impractical to gather much information about subgroups of a non-abelian group created by taking random subsets A and trying to write out the elements of (or other information about) $\langle A \rangle$. For certain “well chosen” subsets A , even of a non-abelian group G , we shall be able to make both theoretical and computational use of the subgroup generated by A . One example of this might be when we want to find a subgroup of G which contains $\langle x \rangle$ properly; we might search for some element y which commutes with x (i.e., $y \in C_G(x)$) and form $\langle x, y \rangle$. It is easy to check that the latter group is abelian, so its order is bounded by $|x||y|$. Alternatively, we might instead take y in $N_G(\langle x \rangle)$ — in this case the same order bound holds and the structure of $\langle x, y \rangle$ is again not too complicated (as we shall see in the next chapter).

The complications which arise for non-abelian groups are generally not quite as serious when we study other basic algebraic systems because of the additional algebraic structure imposed.

EXERCISES

1. Prove that if H is a subgroup of G then $\langle H \rangle = H$.
2. Prove that if A is a subset of B then $\langle A \rangle \leq \langle B \rangle$. Give an example where $A \subseteq B$ with $A \neq B$ but $\langle A \rangle = \langle B \rangle$.
3. Prove that if H is an abelian subgroup of a group G then $\langle H, Z(G) \rangle$ is abelian. Give an explicit example of an abelian subgroup H of a group G such that $\langle H, C_G(H) \rangle$ is not abelian.
4. Prove that if H is a subgroup of G then H is generated by the set $H - \{1\}$.
5. Prove that the subgroup generated by any two distinct elements of order 2 in S_3 is all of S_3 .
6. Prove that the subgroup of S_4 generated by $(1\ 2)$ and $(1\ 2)(3\ 4)$ is a noncyclic group of order 4.
7. Prove that the subgroup of S_4 generated by $(1\ 2)$ and $(1\ 3)(2\ 4)$ is isomorphic to the dihedral group of order 8.
8. Prove that $S_4 = \langle (1\ 2\ 3\ 4), (1\ 2\ 4\ 3) \rangle$.
9. Prove that $SL_2(\mathbb{F}_3)$ is the subgroup of $GL_2(\mathbb{F}_3)$ generated by $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$. [Recall from Exercise 9 of Section 1 that $SL_2(\mathbb{F}_3)$ is the subgroup of matrices of determinant 1. You may assume this subgroup has order 24 — this will be an exercise in Section 3.2.]
10. Prove that the subgroup of $SL_2(\mathbb{F}_3)$ generated by $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ is isomorphic to the quaternion group of order 8. [Use a presentation for Q_8 .]
11. Show that $SL_2(\mathbb{F}_3)$ and S_4 are two nonisomorphic groups of order 24.
12. Prove that the subgroup of upper triangular matrices in $GL_3(\mathbb{F}_2)$ is isomorphic to the dihedral group of order 8 (cf. Exercise 16, Section 1). [First find the order of this subgroup.]
13. Prove that the multiplicative group of positive rational numbers is generated by the set $\{\frac{1}{p} \mid p \text{ is a prime}\}$.
14. A group H is called *finitely generated* if there is a finite set A such that $H = \langle A \rangle$.
 - (a) Prove that every finite group is finitely generated.
 - (b) Prove that \mathbb{Z} is finitely generated.
 - (c) Prove that every finitely generated subgroup of the additive group \mathbb{Q} is cyclic. [If H is a finitely generated subgroup of \mathbb{Q} , show that $H \leq \langle \frac{1}{k} \rangle$, where k is the product of all the denominators which appear in a set of generators for H .]
 - (d) Prove that \mathbb{Q} is not finitely generated.
15. Exhibit a proper subgroup of \mathbb{Q} which is not cyclic.
16. A subgroup M of a group G is called a *maximal subgroup* if $M \neq G$ and the only subgroups of G which contain M are M and G .
 - (a) Prove that if H is a proper subgroup of the finite group G then there is a maximal subgroup of G containing H .
 - (b) Show that the subgroup of all rotations in a dihedral group is a maximal subgroup.
 - (c) Show that if $G = \langle x \rangle$ is a cyclic group of order $n \geq 1$ then a subgroup H is maximal if and only $H = \langle x^p \rangle$ for some prime p dividing n .
17. This is an exercise involving Zorn's Lemma (see Appendix I) to prove that every nontrivial finitely generated group possesses maximal subgroups. Let G be a finitely generated

group, say $G = \langle g_1, g_2, \dots, g_n \rangle$, and let \mathcal{S} be the set of all proper subgroups of G . Then \mathcal{S} is partially ordered by inclusion. Let \mathcal{C} be a chain in \mathcal{S} .

- (a) Prove that the union, H , of all the subgroups in \mathcal{C} is a subgroup of G .
- (b) Prove that H is a *proper* subgroup. [If not, each g_i must lie in H and so must lie in some element of the chain \mathcal{C} . Use the definition of a chain to arrive at a contradiction.]
- (c) Use Zorn's Lemma to show that \mathcal{S} has a maximal element (which is, by definition, a maximal subgroup).

18. Let p be a prime and let $Z = \{z \in \mathbb{C} \mid z^{p^n} = 1 \text{ for some } n \in \mathbb{Z}^+\}$ (so Z is the multiplicative group of all p -power roots of unity in \mathbb{C}). For each $k \in \mathbb{Z}^+$ let $H_k = \{z \in Z \mid z^{p^k} = 1\}$ (the group of p^k th roots of unity). Prove the following:
- (a) $H_k \leq H_m$ if and only if $k \leq m$
 - (b) H_k is cyclic for all k (assume that for any $n \in \mathbb{Z}^+$, $\{e^{2\pi it/n} \mid t = 0, 1, \dots, n-1\}$ is the set of all n^{th} roots of 1 in \mathbb{C})
 - (c) every proper subgroup of Z equals H_k for some $k \in \mathbb{Z}^+$ (in particular, every proper subgroup of Z is finite and cyclic)
 - (d) Z is not finitely generated.
19. A nontrivial abelian group A (written multiplicatively) is called *divisible* iff for each element $a \in A$ and each nonzero integer k there is an element $x \in A$ such that $x^k = a$, i.e., each element has a k^{th} root in A (in additive notation, each element is the k^{th} multiple of some element of A).
- (a) Prove that the additive group of rational numbers, \mathbb{Q} , is divisible.
 - (b) Prove that no finite abelian group is divisible.
20. Prove that if A and B are nontrivial abelian groups, then $A \times B$ is divisible if and only if both A and B are divisible groups.

2.5 THE LATTICE OF SUBGROUPS OF A GROUP

In this section we describe a graph associated with a group which depicts the relationships among its subgroups. This graph, called the lattice² of subgroups of the group, is a good way of “visualizing” a group — it certainly illuminates the structure of a group better than the group table. We shall be using lattice diagrams, or parts of them, to describe both specific groups and certain properties of general groups throughout the chapters on group theory. Moreover, the lattice of subgroups of a group will play an important role in Galois Theory.

The lattice of subgroups of a given finite group G is constructed as follows: plot all subgroups of G starting at the bottom with 1, ending at the top with G and, roughly speaking, with subgroups of larger order positioned higher on the page than those of smaller order. Draw paths upwards between subgroups using the rule that there will be a line upward from A to B if $A \leq B$ and there are no subgroups properly between A and B . Thus if $A \leq B$ there is a path (possibly many paths) upward from A to B passing through a chain of intermediate subgroups (and a path downward from B to A if $B \geq A$). The initial positioning of the subgroups on the page, which is, a priori, somewhat arbitrary, can often (with practice) be chosen to produce a simple picture. Notice that for any pair of subgroups H and K of G the unique smallest subgroup

²The term “lattice” has a precise mathematical meaning in terms of partially ordered sets.

which contains both of them, namely $\langle H, K \rangle$ (called the *join* of H and K), may be read off from the lattice as follows: trace paths upwards from H and K until a common subgroup A which contains H and K is reached (note that G itself always contains all subgroups so at least one such A exists). To ensure that $A = \langle H, K \rangle$ make sure there is no $A_1 \leq A$ (indicated by a downward path from A to A_1) with both H and K contained in A_1 (otherwise replace A with A_1 and repeat the process to see if $A_1 = \langle H, K \rangle$). By a symmetric process one can read off the largest subgroup of G which is contained in both H and K , namely their intersection (which is a subgroup by Proposition 8).

There are some limitations to this process, in particular it cannot be carried out perse for infinite groups. Even for finite groups of relatively small order, lattices can be quite complicated (see the book *Groups of Order 2^n , $n \leq 6$* by M. Hall and J. Senior, Macmillan, 1964, for some hair-raising examples). At the end of this section we shall describe how parts of a lattice may be drawn and used even for infinite groups.

Note that isomorphic groups have the same lattices (i.e., the same directed graphs). Nonisomorphic groups may also have identical lattices (this happens for two groups of order 16 — see the following exercises). Since the lattice of subgroups is only part of the data we shall carry in our descriptors of a group, this will not be a serious drawback (indeed, it might even be useful in seeing when two nonisomorphic groups have some common properties).

Examples

Except for the cyclic groups (Example 1) we have not proved that the following lattices are correct (e.g., contain all subgroups of the given group or have the right joins and intersections). For the moment we shall take these facts as given and, as we build up more theory in the course of the text, we shall assign as exercises the proofs that these are indeed correct.

(1) For $G = \mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$, by Theorem 7 the lattice of subgroups of G is the lattice of divisors of n (that is, the divisors of n are written on a page with n at the bottom, 1 at the top and paths upwards from a to b if $b \mid a$). Some specific examples for various values of n follow.

$$\mathbb{Z}/2\mathbb{Z} = \langle 1 \rangle$$

$$\begin{array}{c} | \\ \langle 2 \rangle = \{0\} \end{array}$$

$$\mathbb{Z}/4\mathbb{Z} = \langle 1 \rangle \quad (\text{note: } \langle 1 \rangle = \langle 3 \rangle)$$

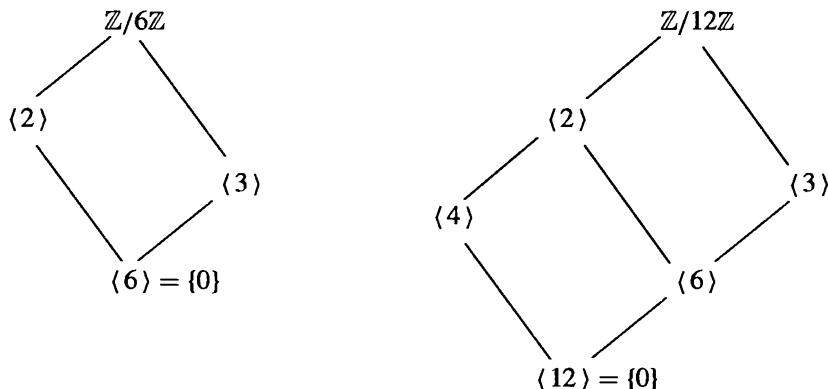
$$\begin{array}{c} | \\ \langle 2 \rangle \\ | \\ \langle 4 \rangle = \{0\} \end{array}$$

$$\mathbb{Z}/8\mathbb{Z} = \langle 1 \rangle \quad (\text{note: } \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle)$$

$$\begin{array}{c} | \\ \langle 2 \rangle \\ | \\ \langle 4 \rangle \\ | \\ \langle 8 \rangle = \{0\} \end{array}$$

In general, if p is a prime, the lattice of $\mathbb{Z}/p^n\mathbb{Z}$ is

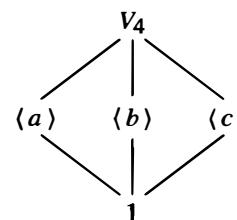
$$\begin{array}{ccc}
 \mathbb{Z}/p^n\mathbb{Z} & = & \langle 1 \rangle \\
 | & & \\
 \langle p \rangle & & \\
 | & & \\
 \langle p^2 \rangle & & \\
 | & & \\
 \langle p^3 \rangle & & \\
 | & & \\
 \vdots & & \\
 | & & \\
 \langle p^{n-1} \rangle & & \\
 | & & \\
 \langle p^n \rangle & = & \{0\}
 \end{array}$$



(2) The *Klein 4-group (Viergruppe)*, V_4 , is the group of order 4 with multiplication table

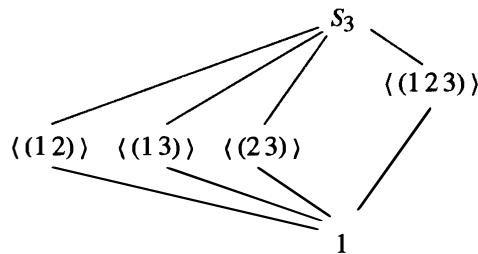
.	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

and lattice

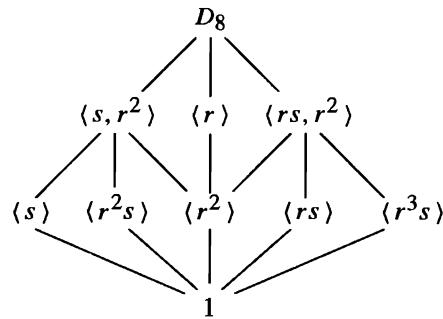


Note that V_4 is abelian and is not isomorphic to Z_4 (why?). We shall see that D_8 has an isomorphic copy of V_4 as a subgroup, so it will not be necessary to check that the associative law holds for the binary operation defined above.

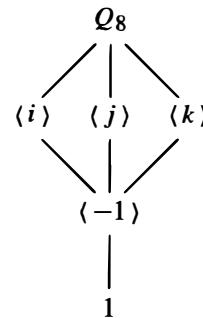
(3) The lattice of S_3 is



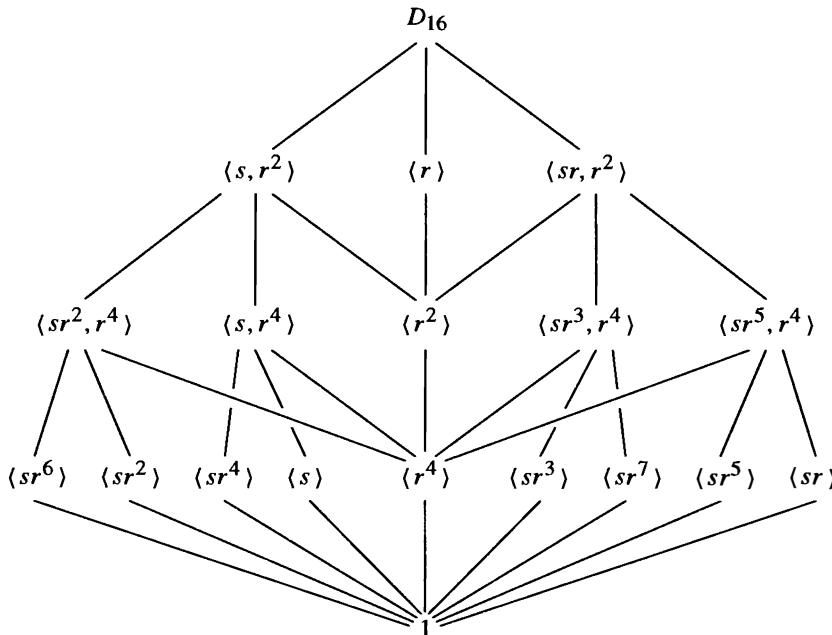
(4) Using our usual notation for $D_8 = \langle r, s \rangle$, the lattice of D_8 is



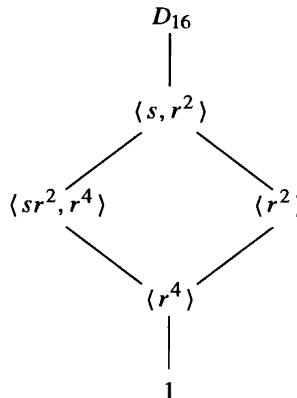
(5) The lattice of subgroups of Q_8 is



- (6) The lattice of D_{16} is not a planar graph (cannot be drawn on a plane without lines crossing). One way of drawing it is



In many instances in both theoretical proofs and specific examples we shall be interested only in information concerning two (or some small number of) subgroups of a given group and their interrelationships. To depict these graphically we shall draw a *sublattice* of the entire group lattice which contains the relevant joins and intersections. An unbroken line in such a sublattice will not, in general, mean that there is no subgroup in between the endpoints of the line. These partial lattices for groups will also be used when we are dealing with infinite groups. For example, if we wished to discuss only the relationship between the subgroups (sr^2, r^4) and (r^2) of D_{16} we would draw the sublattice



Note that $\langle s, r^2 \rangle$ and $\langle r^4 \rangle$ are precisely the join and intersection, respectively, of these two subgroups in D_{16} .

Finally, given the lattice of subgroups of a group, it is relatively easy to compute normalizers and centralizers. For example, in D_8 we can see that $C_{D_8}(s) = \langle s, r^2 \rangle$ because we first calculate that $r^2 \in C_{D_8}(s)$ (see Section 2). This proves $\langle s, r^2 \rangle \leq C_{D_8}(s)$ (note that an element always belongs to its own centralizer). The only subgroups which contain $\langle s, r^2 \rangle$ are that subgroup itself and all of D_8 . We cannot have $C_{D_8}(s) = D_8$ because r does not commute with s (i.e., $r \notin C_{D_8}(s)$). This leaves only the claimed possibility for $C_{D_8}(s)$.

EXERCISES

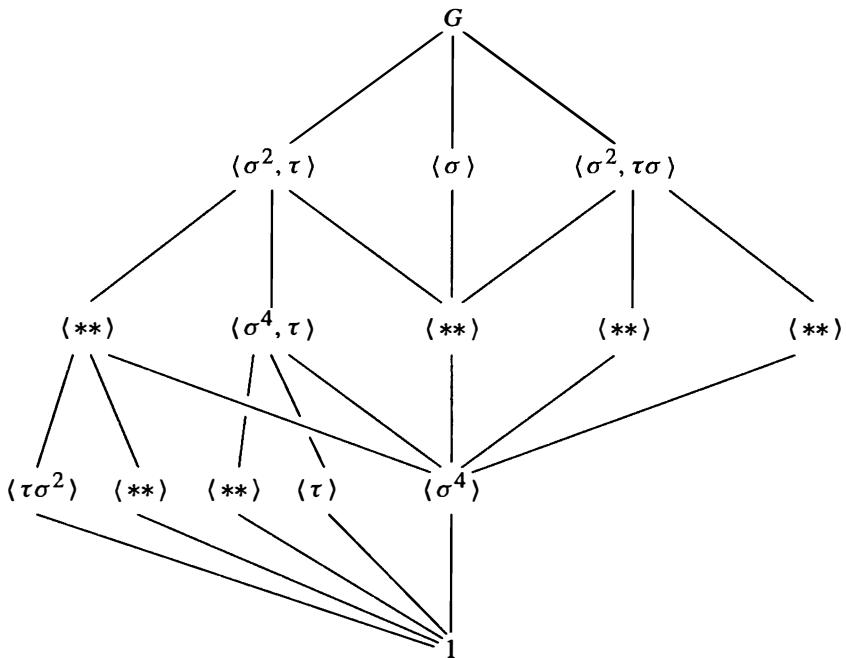
1. Let H and K be subgroups of G . Exhibit all possible sublattices which show only G , 1, H , K and their joins and intersections. What distinguishes the different drawings?
2. In each of (a) to (d) list all subgroups of D_{16} that satisfy the given condition.
 - (a) Subgroups that are contained in $\langle sr^2, r^4 \rangle$
 - (b) Subgroups that are contained in $\langle sr^7, r^4 \rangle$
 - (c) Subgroups that contain $\langle r^4 \rangle$
 - (d) Subgroups that contain $\langle s \rangle$.
3. Show that the subgroup $\langle s, r^2 \rangle$ of D_8 is isomorphic to V_4 .
4. Use the given lattice to find all pairs of elements that generate D_8 (there are 12 pairs).
5. Use the given lattice to find all elements $x \in D_{16}$ such that $D_{16} = \langle x, s \rangle$ (there are 16 such elements x).
6. Use the given lattices to help find the centralizers of every element in the following groups:
 - (a) D_8
 - (b) Q_8
 - (c) S_3
 - (d) D_{16} .
7. Find the center of D_{16} .
8. In each of the following groups find the normalizer of each subgroup:
 - (a) S_3
 - (b) Q_8 .
9. Draw the lattices of subgroups of the following groups:
 - (a) $\mathbb{Z}/16\mathbb{Z}$
 - (b) $\mathbb{Z}/24\mathbb{Z}$
 - (c) $\mathbb{Z}/48\mathbb{Z}$. [See Exercise 6 in Section 3.]
10. Classify groups of order 4 by proving that if $|G| = 4$ then $G \cong Z_4$ or $G \cong V_4$. [See Exercise 36, Section 1.1.]
11. Consider the group of order 16 with the following presentation:

$$QD_{16} = \langle \sigma, \tau \mid \sigma^8 = \tau^2 = 1, \sigma\tau = \tau\sigma^3 \rangle$$

(called the *quasidihedral* or *semidihedral* group of order 16). This group has three subgroups of order 8: $\langle \tau, \sigma^2 \rangle \cong D_8$, $\langle \sigma \rangle \cong Z_8$ and $\langle \sigma^2, \sigma\tau \rangle \cong Q_8$ and every proper subgroup is contained in one of these three subgroups. Fill in the missing subgroups in the lattice of all subgroups of the quasidihedral group on the following page, exhibiting each subgroup with at most two generators. (This is another example of a nonplanar lattice.)

The next three examples lead to two nonisomorphic groups that have the same lattice of subgroups.

12. The group $A = Z_2 \times Z_4 = \langle a, b \mid a^2 = b^4 = 1, ab = ba \rangle$ has order 8 and has three subgroups of order 4: $\langle a, b^2 \rangle \cong V_4$, $\langle b \rangle \cong Z_4$ and $\langle ab \rangle \cong Z_4$ and every proper



subgroup is contained in one of these three. Draw the lattice of all subgroups of A , giving each subgroup in terms of at most two generators.

13. The group $G = Z_2 \times Z_8 = \langle x, y \mid x^2 = y^8 = 1, xy = yx \rangle$ has order 16 and has three subgroups of order 8: $\langle x, y^2 \rangle \cong Z_2 \times Z_4$, $\langle y \rangle \cong Z_8$ and $\langle xy \rangle \cong Z_8$ and every proper subgroup is contained in one of these three. Draw the lattice of all subgroups of G , giving each subgroup in terms of at most two generators (cf. Exercise 12).

14. Let M be the group of order 16 with the following presentation:

$$\langle u, v \mid u^2 = v^8 = 1, vu = uv^5 \rangle$$

(sometimes called the *modular* group of order 16). It has three subgroups of order 8: $\langle u, v^2 \rangle$, $\langle v \rangle$ and $\langle uv \rangle$ and every proper subgroup is contained in one of these three. Prove that $\langle u, v^2 \rangle \cong Z_2 \times Z_4$, $\langle v \rangle \cong Z_8$ and $\langle uv \rangle \cong Z_8$. Show that the lattice of subgroups of M is the same as the lattice of subgroups of $Z_2 \times Z_8$ (cf. Exercise 13) but that these two groups are not isomorphic.

15. Describe the isomorphism type of each of the three subgroups of D_{16} of order 8.
 16. Use the lattice of subgroups of the quasidihedral group of order 16 to show that every element of order 2 is contained in the proper subgroup $\langle \tau, \sigma^2 \rangle$ (cf. Exercise 11).
 17. Use the lattice of subgroups of the modular group M of order 16 to show that the set $\{x \in M \mid x^2 = 1\}$ is a subgroup of M isomorphic to the Klein 4-group (cf. Exercise 14).
 18. Use the lattice to help find the centralizer of every element of QD_{16} (cf. Exercise 11).
 19. Use the lattice to help find $N_{D_{16}}(\langle s, r^4 \rangle)$.
 20. Use the lattice of subgroups of QD_{16} (cf. Exercise 11) to help find the normalizers
 (a) $N_{QD_{16}}(\langle \tau\sigma \rangle)$ (b) $N_{QD_{16}}(\langle \tau, \sigma^4 \rangle)$.

CHAPTER 3

Quotient Groups and Homomorphisms

3.1 DEFINITIONS AND EXAMPLES

In this chapter we introduce the notion of a *quotient* group of a group G , which is another way of obtaining a “smaller” group from the group G and, as we did with subgroups, we shall use quotient groups to study the structure of G . The structure of the group G is reflected in the structure of the quotient groups and the subgroups of G . For example, we shall see that the lattice of subgroups for a *quotient* of G is reflected at the “top” (in a precise sense) of the lattice for G whereas the lattice for a *subgroup* of G occurs naturally at the “bottom.” One can therefore obtain information about the group G by combining this information and we shall indicate how some classification theorems arise in this way.

The study of the quotient groups of G is essentially equivalent to the study of the homomorphisms of G , i.e., the maps of the group G to another group which respect the group structures. If φ is a homomorphism from G to a group H recall that the *fibers* of φ are the sets of elements of G projecting to single elements of H , which we can represent pictorially in Figure 1, where the vertical line in the box above a point a represents the fiber of φ over a .

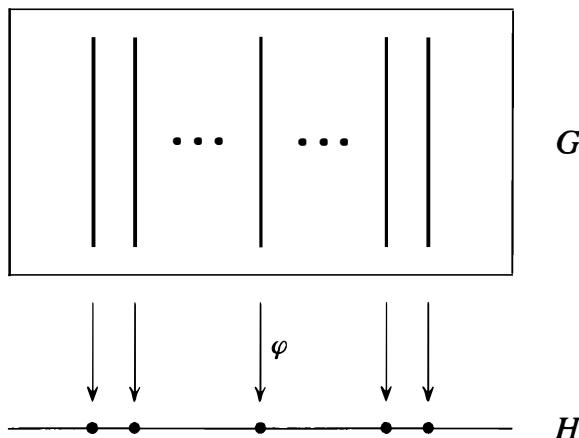


Fig. 1

The group operation in H provides a way to multiply two elements in the image of φ (i.e., two elements on the horizontal line in Figure 1). This suggests a natural multiplication of the *fibers* lying above these two points making *the set of fibers into a group*: if X_a is the fiber above a and X_b is the fiber above b then the product of X_a with X_b is defined to be the fiber X_{ab} above the product ab , i.e., $X_a X_b = X_{ab}$. This multiplication is associative since multiplication is associative in H , the identity is the fiber over the identity of H , and the inverse of the fiber over a is the fiber over a^{-1} , as is easily checked from the definition. For example, the associativity is proved as follows: $(X_a X_b) X_c = (X_{ab}) X_c = X_{(ab)c}$ and $X_a (X_b X_c) = X_a (X_{bc}) = X_{a(bc)}$. Since $(ab)c = a(bc)$ in H , $(X_a X_b) X_c = X_a (X_b X_c)$. Roughly speaking, the group G is partitioned into pieces (the fibers) and these pieces themselves have the structure of a group, called a *quotient group* of G (a formal definition follows the example below).

Since the multiplication of fibers is defined from the multiplication in H , by construction the quotient group with this multiplication is naturally isomorphic to the image of G under the homomorphism φ (fiber X_a is identified with its image a in H).

Example

Let $G = \mathbb{Z}$, let $H = \mathbb{Z}_n = \langle x \rangle$ be the cyclic group of order n and define $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}_n$ by $\varphi(a) = x^a$. Since

$$\varphi(a+b) = x^{a+b} = x^a x^b = \varphi(a)\varphi(b)$$

it follows that φ is a homomorphism (note that the operation in \mathbb{Z} is addition and the operation in \mathbb{Z}_n is multiplication). Note also that φ is surjective. The fiber of φ over x^a is then

$$\begin{aligned}\varphi^{-1}(x^a) &= \{m \in \mathbb{Z} \mid x^m = x^a\} = \{m \in \mathbb{Z} \mid x^{m-a} = 1\} \\ &= \{m \in \mathbb{Z} \mid n \text{ divides } m-a\} \quad (\text{by Proposition 2.3}) \\ &= \{m \in \mathbb{Z} \mid m \equiv a \pmod{n}\} = \bar{a},\end{aligned}$$

i.e., the fibers of φ are precisely the residue classes modulo n . Figure 1 here becomes:

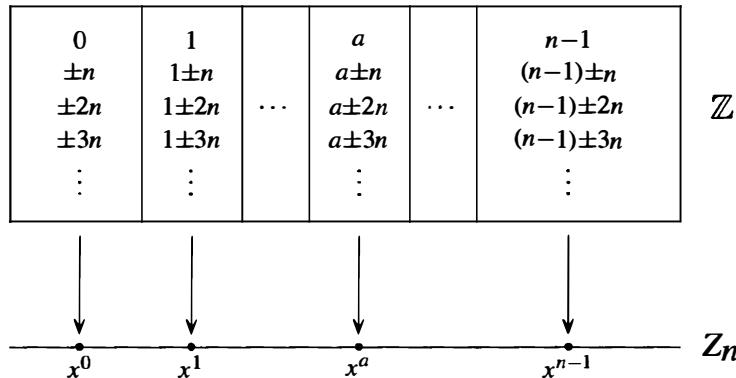


Fig. 2

The multiplication in Z_n is just $x^a x^b = x^{a+b}$. The corresponding fibers are \bar{a} , \bar{b} , and $\overline{a+b}$, so the corresponding group operation for the fibers is $\bar{a} \cdot \bar{b} = \overline{a+b}$. This is just the group $\mathbb{Z}/n\mathbb{Z}$ under addition, a group isomorphic to the image of φ (all of Z_n).

The identity of this group (the fiber above the identity in Z_n) consists of all the multiples of n in \mathbb{Z} , namely $n\mathbb{Z}$, a subgroup of \mathbb{Z} , and the remaining fibers are just translates, $a + n\mathbb{Z}$, of this subgroup. The group operation can also be defined directly by taking *representatives* from these fibers, adding these representatives in \mathbb{Z} and taking the fiber containing this sum (this was the original definition of the group $\mathbb{Z}/n\mathbb{Z}$). From a computational point of view computing the product of \bar{a} and \bar{b} by simply adding representatives a and b is much easier than first computing the image of these fibers under φ (namely, x^a and x^b), multiplying these in H (obtaining x^{a+b}) and then taking the fiber over this product.

We first consider some basic properties of homomorphisms and their fibers. The fiber of a homomorphism $\varphi : G \rightarrow H$ lying above the identity of H is given a name:

Definition. If φ is a homomorphism $\varphi : G \rightarrow H$, the *kernel* of φ is the set

$$\{g \in G \mid \varphi(g) = 1\}$$

and will be denoted by $\ker \varphi$ (here 1 is the identity of H).

Proposition 1. Let G and H be groups and let $\varphi : G \rightarrow H$ be a homomorphism.

- (1) $\varphi(1_G) = 1_H$, where 1_G and 1_H are the identities of G and H , respectively.
- (2) $\varphi(g^{-1}) = \varphi(g)^{-1}$ for all $g \in G$.
- (3) $\varphi(g^n) = \varphi(g)^n$ for all $n \in \mathbb{Z}$.
- (4) $\ker \varphi$ is a subgroup of G .
- (5) $\text{im } (\varphi)$, the image of G under φ , is a subgroup of H .

Proof: (1) Since $\varphi(1_G) = \varphi(1_G 1_G) = \varphi(1_G)\varphi(1_G)$, the cancellation laws show that (1) holds.

(2) $\varphi(1_G) = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1})$ and, by part (1), $\varphi(1_G) = 1_H$, hence

$$1_H = \varphi(g)\varphi(g^{-1}).$$

Multiplying both sides on the left by $\varphi(g)^{-1}$ and simplifying gives (2).

(3) This is an easy exercise in induction for $n \in \mathbb{Z}^+$. By part (2), conclusion (3) holds for negative values of n as well.

(4) Since $1_G \in \ker \varphi$, the kernel of φ is not empty. Let $x, y \in \ker \varphi$, that is $\varphi(x) = \varphi(y) = 1_H$. Then

$$\varphi(xy^{-1}) = \varphi(x)\varphi(y^{-1}) = \varphi(x)\varphi(y)^{-1} = 1_H 1_H^{-1} = 1_H$$

that is, $xy^{-1} \in \ker \varphi$. By the subgroup criterion, $\ker \varphi \leq G$.

(5) Since $\varphi(1_G) = 1_H$, the identity of H lies in the image of φ , so $\text{im } (\varphi)$ is nonempty. If x and y are in $\text{im } (\varphi)$, say $x = \varphi(a)$, $y = \varphi(b)$, then $y^{-1} = \varphi(b^{-1})$ by (2) so that $xy^{-1} = \varphi(a)\varphi(b^{-1}) = \varphi(ab^{-1})$ since φ is a homomorphism. Hence also xy^{-1} is in the image of φ , so $\text{im } (\varphi)$ is a subgroup of H by the subgroup criterion.

We can now define some terminology associated with quotient groups.

Definition. Let $\varphi : G \rightarrow H$ be a homomorphism with kernel K . The *quotient group* or *factor group*, G/K (read G modulo K or simply G mod K), is the group whose elements are the fibers of φ with group operation defined above: namely if X is the fiber above a and Y is the fiber above b then the product of X with Y is defined to be the fiber above the product ab .

The notation emphasizes the fact that the kernel K is a *single element* in the group G/K and we shall see below (Proposition 2) that, as in the case of $\mathbb{Z}/n\mathbb{Z}$ above, the other elements of G/K are just the “translates” of the kernel K . Hence we may think of G/K as being obtained by collapsing or “dividing out” by K (or more precisely, by equivalence modulo K). This explains why G/K is referred to as a “quotient” group.

The definition of the quotient group G/K above requires the map φ explicitly, since the multiplication of the fibers is performed by first projecting the fibers to H via φ , multiplying in H and then determining the fiber over this product. Just as for $\mathbb{Z}/n\mathbb{Z}$ above, it is also possible to define the multiplication of fibers directly in terms of *representatives* from the fibers. This is computationally simpler and the map φ does not enter explicitly. We first show that the fibers of a homomorphism can be expressed in terms of the kernel of the homomorphism just as in the example above (where the kernel was $n\mathbb{Z}$ and the fibers were translates of the form $a + n\mathbb{Z}$).

Proposition 2. Let $\varphi : G \rightarrow H$ be a homomorphism of groups with kernel K . Let $X \in G/K$ be the fiber above a , i.e., $X = \varphi^{-1}(a)$. Then

- (1) For any $u \in X$, $X = \{uk \mid k \in K\}$
- (2) For any $u \in X$, $X = \{ku \mid k \in K\}$.

Proof: We prove (1) and leave the proof of (2) as an exercise. Let $u \in X$ so, by definition of X , $\varphi(u) = a$. Let

$$uK = \{uk \mid k \in K\}.$$

We first prove $uK \subseteq X$. For any $k \in K$,

$$\begin{aligned}\varphi(uk) &= \varphi(u)\varphi(k) && (\text{since } \varphi \text{ is a homomorphism}) \\ &= \varphi(u)1 && (\text{since } k \in \ker \varphi) \\ &= a,\end{aligned}$$

that is, $uk \in X$. This proves $uK \subseteq X$. To establish the reverse inclusion suppose $g \in X$ and let $k = u^{-1}g$. Then

$$\begin{aligned}\varphi(k) &= \varphi(u^{-1})\varphi(g) = \varphi(u)^{-1}\varphi(g) && (\text{by Proposition 1}) \\ &= a^{-1}a = 1.\end{aligned}$$

Thus $k \in \ker \varphi$. Since $k = u^{-1}g$, $g = uk \in uK$, establishing the inclusion $X \subseteq uK$. This proves (1).

The sets arising in Proposition 2 to describe the fibers of a homomorphism φ are defined for *any* subgroup K of G , not necessarily the kernel of some homomorphism (we shall determine necessary and sufficient conditions for a subgroup to be such a kernel shortly) and are given a name:

Definition. For any $N \leq G$ and any $g \in G$ let

$$gN = \{gn \mid n \in N\} \quad \text{and} \quad Ng = \{ng \mid n \in N\}$$

called respectively a *left coset* and a *right coset* of N in G . Any element of a coset is called a *representative* for the coset.

We have already seen in Proposition 2 that if N is the kernel of a homomorphism and g_1 is any representative for the coset gN then $g_1N = gN$ (and if $g_1 \in Ng$ then $Ng_1 = Ng$). We shall see that this fact is valid for arbitrary subgroups N in Proposition 4 below, which explains the terminology of a *representative*.

If G is an additive group we shall write $g + N$ and $N + g$ for the left and right cosets of N in G with representative g , respectively. In general we can think of the left coset, gN , of N in G as the left translate of N by g . (The reader may wish to review Exercise 18 of Section 1.7 which proves that the right cosets of N in G are precisely the orbits of N acting on G by left multiplication.)

In terms of this definition, Proposition 2 shows that the fibers of a homomorphism are the left cosets of the kernel (and also the right cosets of the kernel), i.e., the elements of the quotient G/K are the left cosets gK , $g \in G$. In the example of $\mathbb{Z}/n\mathbb{Z}$ the multiplication in the quotient group could also be defined in terms of representatives for the cosets. The following result shows the same result is true for G/K in general (provided we know that K is the kernel of some homomorphism), namely that the product of two left cosets X and Y in G/K is computed by choosing any representative u of X , any representative v of Y , multiplying u and v in G and forming the coset $(uv)K$.

Theorem 3. Let G be a group and let K be the kernel of some homomorphism from G to another group. Then the set whose elements are the left cosets of K in G with operation defined by

$$uK \circ vK = (uv)K$$

forms a group, G/K . In particular, this operation is well defined in the sense that if u_1 is any element in uK and v_1 is any element in vK , then $u_1v_1 \in uvK$, i.e., $u_1v_1K = uvK$ so that the multiplication does not depend on the choice of representatives for the cosets. The same statement is true with “right coset” in place of “left coset.”

Proof: Let $X, Y \in G/K$ and let $Z = XY$ in G/K , so that by Proposition 2(1) X , Y and Z are (left) cosets of K . By assumption, K is the kernel of some homomorphism $\varphi : G \rightarrow H$ so $X = \varphi^{-1}(a)$ and $Y = \varphi^{-1}(b)$ for some $a, b \in H$. By definition of the operation in G/K , $Z = \varphi^{-1}(ab)$. Let u and v be arbitrary representatives of X , Y , respectively, so that $\varphi(u) = a$, $\varphi(v) = b$ and $X = uK$, $Y = vK$. We must show $uv \in Z$. Now

$$\begin{aligned} uv \in Z &\Leftrightarrow uv \in \varphi^{-1}(ab) \\ &\Leftrightarrow \varphi(uv) = ab \\ &\Leftrightarrow \varphi(u)\varphi(v) = ab. \end{aligned}$$

Since the latter equality does hold, $uv \in Z$ hence Z is the (left) coset uvK . (Exercise 2 below shows conversely that every $z \in Z$ can be written as uv , for some $u \in X$ and $v \in Y$.) This proves that the product of X with Y is the coset uvK for any choice of representatives $u \in X$, $v \in Y$ completing the proof of the first statements of the theorem. The last statement in the theorem follows immediately since, by Proposition 2, $uK = Ku$ and $vK = Kv$ for all u and v in G .

In terms of Figure 1, the multiplication in G/K via representatives can be pictured as in the following Figure 3.

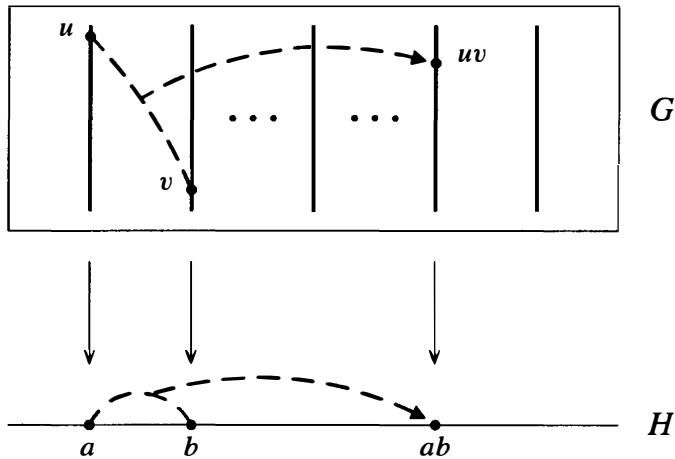


Fig. 3

We emphasize the fact that *the multiplication is independent of the particular representatives chosen*. Namely, the product (or sum, if the group is written additively) of two cosets X and Y is the coset uvK containing the product uv where u and v are *any* representatives for the cosets X and Y , respectively. This process of considering only the coset containing an element, or “reducing mod K ” is the same as what we have been doing, in particular, in $\mathbb{Z}/n\mathbb{Z}$. A useful notation for denoting the coset uK containing a representative u is \bar{u} . With this notation (which we introduced in the Preliminaries in dealing with $\mathbb{Z}/n\mathbb{Z}$), the quotient group G/K is denoted \overline{G} and the product of elements \bar{u} and \bar{v} is simply the coset containing uv , i.e., \overline{uv} . This notation also reinforces the fact that the cosets uK in G/K are *elements* \bar{u} in G/K .

Examples

- (1) The first example in this chapter of the homomorphism φ from \mathbb{Z} to \mathbb{Z}_n has fibers the left (and also the right) cosets $a + n\mathbb{Z}$ of the kernel $n\mathbb{Z}$. Theorem 3 proves that these cosets form a group under addition of representatives, namely $\mathbb{Z}/n\mathbb{Z}$, which explains the notation for this group. The group is naturally isomorphic to its image under φ , so we recover the isomorphism $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ of Chapter 2.
- (2) If $\varphi : G \rightarrow H$ is an *isomorphism*, then $K = 1$, the fibers of φ are the singleton subsets of G and so $G/1 \cong G$.

- (3) Let G be any group, let $H = 1$ be the group of order 1 and define $\varphi : G \rightarrow H$ by $\varphi(g) = 1$, for all $g \in G$. It is immediate that φ is a homomorphism. This map is called the *trivial homomorphism*. Note that in this case $\ker \varphi = G$ and G/G is a group with the single element, G , i.e., $G/G \cong Z_1 = \{1\}$.
- (4) Let $G = \mathbb{R}^2$ (operation vector addition), let $H = \mathbb{R}$ (operation addition) and define $\varphi : \mathbb{R}^2 \rightarrow \mathbb{R}$ by $\varphi((x, y)) = x$. Thus φ is projection onto the x -axis. We show φ is a homomorphism:

$$\begin{aligned}\varphi((x_1, y_1) + (x_2, y_2)) &= \varphi((x_1 + x_2, y_1 + y_2)) \\ &= x_1 + x_2 = \varphi((x_1, y_1)) + \varphi((x_2, y_2)).\end{aligned}$$

Now

$$\begin{aligned}\ker \varphi &= \{(x, y) \mid \varphi((x, y)) = 0\} \\ &= \{(x, y) \mid x = 0\} = \text{the } y\text{-axis}.\end{aligned}$$

Note that $\ker \varphi$ is indeed a subgroup of \mathbb{R}^2 and that the fiber of φ over $a \in \mathbb{R}$ is the translate of the y -axis by a , i.e., the line $x = a$. This is also the left (and the right) coset of the kernel with representative $(a, 0)$ (or any other representative point projecting to a):

$$\overline{(a, 0)} = (a, 0) + \text{y-axis}.$$

Hence Figure 1 in this example becomes

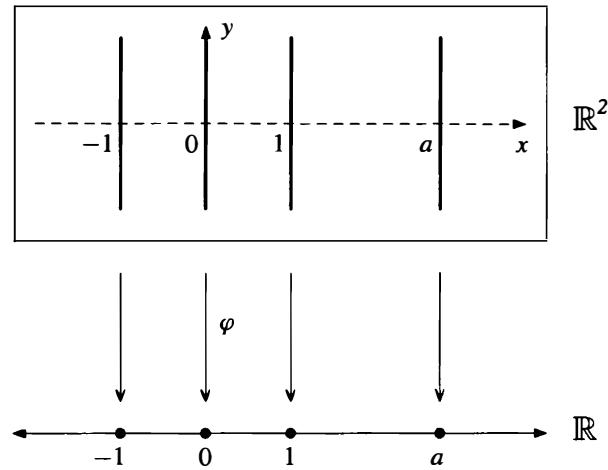


Fig. 4

The group operation (written additively here) can be described either by using the map φ : the sum of the line $(x = a)$ and the line $(x = b)$ is the line $(x = a + b)$; or directly in terms of coset representatives: the sum of the vertical line containing the point (a, y_1) and the vertical line containing the point (b, y_2) is the vertical line containing the point $(a + b, y_1 + y_2)$. Note in particular that the choice of representatives of these vertical lines is not important (i.e., the y -coordinates are not important).

- (5) (An example where the group G is non-abelian.) Let $G = Q_8$ and let $H = V_4$ be the Klein 4-group (Section 2.5, Example 2). Define $\varphi : Q_8 \rightarrow V_4$ by

$$\varphi(\pm 1) = 1, \quad \varphi(\pm i) = a, \quad \varphi(\pm j) = b, \quad \varphi(\pm k) = c.$$

The check that φ is a homomorphism is left as an exercise — relying on symmetry minimizes the work in showing $\varphi(xy) = \varphi(x)\varphi(y)$ for all x and y in Q_8 . It is clear that φ is surjective and that $\ker \varphi = \{\pm 1\}$. One might think of φ as an “absolute value” function on Q_8 so the fibers of φ are the sets $E = \{\pm 1\}$, $A = \{\pm i\}$, $B = \{\pm j\}$ and $C = \{\pm k\}$, which are collapsed to 1, a , b , and c respectively in $Q_8/(\pm 1)$ and these are the left (and also the right) cosets of $\ker \varphi$ (for example, $A = i \cdot \ker \varphi = \{i, -i\} = \ker \varphi \cdot i$).

By Theorem 3, if we are given a subgroup K of a group G which we know is the kernel of some homomorphism, we may define the quotient G/K without recourse to the homomorphism by the multiplication $uKvK = uvK$. This raises the question of whether it is possible to define the quotient group G/N similarly for *any* subgroup N of G . The answer is no in general since this multiplication is not in general well defined (cf. Proposition 5 later). In fact we shall see that it is possible to define the structure of a group on the cosets of N if and only if N is the kernel of some homomorphism (Proposition 7). We shall also give a criterion to determine when a subgroup N is such a kernel — this is the notion of a *normal* subgroup and we shall consider non-normal subgroups in subsequent sections.

We first show that the cosets of an arbitrary subgroup of G partition G (i.e., their union is all of G and distinct cosets have trivial intersection).

Proposition 4. Let N be any subgroup of the group G . The set of left cosets of N in G form a partition of G . Furthermore, for all $u, v \in G$, $uN = vN$ if and only if $v^{-1}u \in N$ and in particular, $uN = vN$ if and only if u and v are representatives of the same coset.

Proof: First of all note that since N is a subgroup of G , $1 \in N$. Thus $g = g \cdot 1 \in gN$ for all $g \in G$, i.e.,

$$G = \bigcup_{g \in G} gN.$$

To show that distinct left cosets have empty intersection, suppose $uN \cap vN \neq \emptyset$. We show $uN = vN$. Let $x \in uN \cap vN$. Write

$$x = un = vm, \quad \text{for some } n, m \in N.$$

In the latter equality multiply both sides on the right by n^{-1} to get

$$u = vmn^{-1} = vm_1, \quad \text{where } m_1 = mn^{-1} \in N.$$

Now for any element ut of uN ($t \in N$),

$$ut = (vm_1)t = v(m_1t) \in vN.$$

This proves $uN \subseteq vN$. By interchanging the roles of u and v one obtains similarly that $vN \subseteq uN$. Thus two cosets with nonempty intersection coincide.

By the first part of the proposition, $uN = vN$ if and only if $u \in vN$ if and only if $u = vn$, for some $n \in N$ if and only if $v^{-1}u \in N$, as claimed. Finally, $v \in uN$ is equivalent to saying v is a representative for uN , hence $uN = vN$ if and only if u and v are representatives for the same coset (namely the coset $uN = vN$).

Proposition 5. Let G be a group and let N be a subgroup of G .

(1) The operation on the set of left cosets of N in G described by

$$uN \cdot vN = (uv)N$$

is well defined if and only if $gng^{-1} \in N$ for all $g \in G$ and all $n \in N$.

(2) If the above operation is well defined, then it makes the set of left cosets of N in G into a group. In particular the identity of this group is the coset $1N$ and the inverse of gN is the coset $g^{-1}N$ i.e., $(gN)^{-1} = g^{-1}N$.

Proof: (1) Assume first that this operation is well defined, that is, for all $u, v \in G$,

$$\text{if } u, u_1 \in uN \text{ and } v, v_1 \in vN \quad \text{then} \quad uvN = u_1v_1N.$$

Let g be an arbitrary element of G and let n be an arbitrary element of N . Letting $u = 1, u_1 = n$ and $v = v_1 = g^{-1}$ and applying the assumption above we deduce that

$$1g^{-1}N = ng^{-1}N \quad \text{i.e.,} \quad g^{-1}N = ng^{-1}N.$$

Since $1 \in N, ng^{-1} \cdot 1 \in ng^{-1}N$. Thus $ng^{-1} \in g^{-1}N$, hence $ng^{-1} = g^{-1}n_1$, for some $n_1 \in N$. Multiplying both sides on the left by g gives $gng^{-1} = n_1 \in N$, as claimed.

Conversely, assume $gng^{-1} \in N$ for all $g \in G$ and all $n \in N$. To prove the operation stated above is well defined let $u, u_1 \in uN$ and $v, v_1 \in vN$. We may write

$$u_1 = un \text{ and } v_1 = vm, \quad \text{for some } n, m \in N.$$

We must prove that $u_1v_1 \in uvN$:

$$\begin{aligned} u_1v_1 &= (un)(vm) = u(vv^{-1})num \\ &= (uv)(v^{-1}nv)m = (uv)(n_1m), \end{aligned}$$

where $n_1 = v^{-1}nv = (v^{-1})n(v^{-1})^{-1}$ is an element of N by assumption. Now N is closed under products, so $n_1m \in N$. Thus

$$u_1v_1 = (uv)n_2, \quad \text{for some } n_2 \in N.$$

Thus the left cosets uvN and u_1v_1N contain the common element u_1v_1 . By the preceding proposition they are equal. This proves that the operation is well defined.

(2) If the operation on cosets is well defined the group axioms are easy to check and are induced by their validity in G . For example, the associative law holds because for all $u, v, w \in G$,

$$\begin{aligned} (uN)(vNwN) &= uN(vwN) \\ &= u(vw)N \\ &= (uv)wN = (uNvN)(wN), \end{aligned}$$

since $u(vw) = (uv)w$ in G . The identity in G/N is the coset $1N$ and the inverse of gN is $g^{-1}N$ as is immediate from the definition of the multiplication.

As indicated before, the subgroups N satisfying the condition in Proposition 5 for which there is a natural group structure on the quotient G/N are given a name:

Definition. The element gng^{-1} is called the *conjugate* of $n \in N$ by g . The set $gNg^{-1} = \{gng^{-1} \mid n \in N\}$ is called the *conjugate* of N by g . The element g is said to *normalize* N if $gNg^{-1} = N$. A subgroup N of a group G is called *normal* if every element of G normalizes N , i.e., if $gNg^{-1} = N$ for all $g \in G$. If N is a normal subgroup of G we shall write $N \trianglelefteq G$.

Note that the structure of G is reflected in the structure of the quotient G/N when N is a normal subgroup (for example, the associativity of the multiplication in G/N is induced from the associativity in G and inverses in G/N are induced from inverses in G). We shall see more of the relationship of G to its quotient G/N when we consider the Isomorphism Theorems later in Section 3.

We summarize our results above as Theorem 6.

Theorem 6. Let N be a subgroup of the group G . The following are equivalent:

- (1) $N \trianglelefteq G$
- (2) $N_G(N) = G$ (recall $N_G(N)$ is the normalizer in G of N)
- (3) $gN = Ng$ for all $g \in G$
- (4) the operation on left cosets of N in G described in Proposition 5 makes the set of left cosets into a group
- (5) $gNg^{-1} \subseteq N$ for all $g \in G$.

Proof: We have already done the hard equivalences; the others are left as exercises.

As a practical matter, one tries to minimize the computations necessary to determine whether a given subgroup N is normal in a group G . In particular, one tries to avoid as much as possible the computation of all the conjugates gng^{-1} for $n \in N$ and $g \in G$. For example, the elements of N itself normalize N since N is a subgroup. Also, if one has a set of *generators* for N , it suffices to check that all conjugates of these generators lie in N to prove that N is a normal subgroup (this is because the conjugate of a product is the product of the conjugates and the conjugate of the inverse is the inverse of the conjugate) — this is Exercise 26 later. Similarly, if generators for G are also known, then it suffices to check that these generators for G normalize N . In particular, if generators for *both* N and G are known, this reduces the calculations to a small number of conjugations to check. If N is a *finite* group then it suffices to check that the conjugates of a set of generators for N by a set of generators for G are again elements of N (Exercise 29). Finally, it is often possible to prove directly that $N_G(N) = G$ without excessive computations (some examples appear in the next section), again proving that N is a normal subgroup of G without mindlessly computing all possible conjugates gng^{-1} .

We now prove that the normal subgroups are precisely the same as the kernels of homomorphisms considered earlier.

Proposition 7. A subgroup N of the group G is normal if and only if it is the kernel of some homomorphism.

Proof: If N is the kernel of the homomorphism φ , then Proposition 2 shows that the left cosets of N are the same as the right cosets of N (and both are the fibers of the

map φ). By (3) of Theorem 6, N is then a normal subgroup. (Another direct proof of this from the definition of normality for N is given in the exercises).

Conversely, if $N \trianglelefteq G$, let $H = G/N$ and define $\pi : G \rightarrow H$ by

$$\pi(g) = gN \quad \text{for all } g \in G.$$

By definition of the operation in G/N ,

$$\pi(g_1g_2) = (g_1g_2)N = g_1Ng_2N = \pi(g_1)\pi(g_2).$$

This proves π is a homomorphism. Now

$$\begin{aligned} \ker \pi &= \{g \in G \mid \pi(g) = 1N\} \\ &= \{g \in G \mid gN = 1N\} \\ &= \{g \in G \mid g \in N\} = N. \end{aligned}$$

Thus N is the kernel of the homomorphism π .

The homomorphism π constructed above demonstrating the normal subgroup N as the kernel of a homomorphism is given a name:

Definition. Let $N \trianglelefteq G$. The homomorphism $\pi : G \rightarrow H$ defined by $\pi(g) = gN$ is called the *natural projection (homomorphism)*¹ of G onto H . If $\bar{H} \leq G/N$ is a subgroup of G/N , the *complete preimage* of \bar{H} in G is the preimage of \bar{H} under the natural projection homomorphism.

The complete preimage of a subgroup of G/N is a subgroup of G (cf. Exercise 1) which contains the subgroup N since these are the elements which map to the identity $\bar{1} \in \bar{H}$. We shall see in the Isomorphism Theorems in Section 3 that there is a natural correspondence between the subgroups of G that contain N and the subgroups of the quotient G/N .

We now have an “internal” criterion which determines precisely when a subgroup N of a given group G is the kernel of some homomorphism, namely,

$$N_G(N) = N.$$

We may thus think of the normalizer of a subgroup N of G as being a measure of “how close” N is to being a normal subgroup (this explains the choice of name for this subgroup). Keep in mind that the property of being normal is an *embedding* property, that is, it depends on the relation of N to G , not on the internal structure of N itself (the same group N may be a normal subgroup of G but not be normal in a larger group containing G).

We began the discussion of quotient groups with the existence of a homomorphism φ of G to H and showed the kernel of this homomorphism is a normal subgroup N of G and the quotient G/N (defined in terms of fibers originally) is naturally isomorphic

¹The word “natural” has a precise mathematical meaning in the theory of categories; for our purposes we use the term to indicate that the definition of this homomorphism is a “coordinate free” projection i.e., is described only in terms of the elements themselves, not in terms of generators for G or N (cf. Appendix II).

to the image of G under φ in H . Conversely, if $N \trianglelefteq G$, we can find a group H (namely, G/N) and a homomorphism $\pi : G \rightarrow H$ such that $\ker \pi = N$ (namely, the natural projection). The study of homomorphic images of G (i.e., the images of homomorphisms from G into other groups) is thus equivalent to the study of quotient groups of G and we shall use homomorphisms to produce normal subgroups and vice versa.

We developed the theory of quotient groups by way of homomorphisms rather than simply defining the notion of a normal subgroup and its associated quotient group to emphasize the fact that the *elements* of the quotient are *subsets* (the fibers or cosets of the kernel N) of the original group G . The visualization in Figure 1 also emphasizes that N (and its cosets) are projected (or collapsed) onto single elements in the quotient G/N . Computations in the quotient group G/N are performed by taking *representatives* from the various cosets involved.

Some examples of normal subgroups and their associated quotients follow.

Examples

Let G be a group.

- (1) The subgroups 1 and G are always normal in G ; $G/1 \cong G$ and $G/G \cong 1$.
- (2) If G is an *abelian* group, *any* subgroup N of G is normal because for all $g \in G$ and all $n \in N$,

$$gng^{-1} = gg^{-1}n = n \in N.$$

Note that it is important that G be abelian, not just that N be abelian. The structure of G/N may vary as we take different subgroups N of G . For instance, if $G = \mathbb{Z}$, then every subgroup N of G is cyclic:

$$N = \langle n \rangle = \langle -n \rangle = n\mathbb{Z}, \quad \text{for some } n \in \mathbb{Z}$$

and $G/N = \mathbb{Z}/n\mathbb{Z}$ is a cyclic group with generator $\bar{1} = 1 + n\mathbb{Z}$ (note that 1 is a generator for G).

Suppose now that $G = Z_k$ is the cyclic group of order k . Let x be a generator of G and let $N \leq G$. By Proposition 2.6 $N = \langle x^d \rangle$, where d is the smallest power of x which lies in N . Now

$$G/N = \{gN \mid g \in G\} = \{x^\alpha N \mid \alpha \in \mathbb{Z}\}$$

and since $x^\alpha N = (xN)^\alpha$ (see Exercise 4 below), it follows that

$$G/N = \langle xN \rangle \quad \text{i.e., } G/N \text{ is cyclic with } xN \text{ as a generator.}$$

By Exercise 5 below, the order of xN in G/N equals d . By Proposition 2.5, $d = \frac{|G|}{|N|}$.

In summary,

quotient groups of a cyclic group are cyclic

and the image of a generator g for G is a generator \bar{g} for the quotient. If in addition G is a *finite* cyclic group and $N \leq G$, then $|G/N| = \frac{|G|}{|N|}$ gives a formula for the order of the quotient group.

- (3) If $N \leq Z(G)$, then $N \trianglelefteq G$ because for all $g \in G$ and all $n \in N$, $gng^{-1} = n \in N$, generalizing the previous example (where the center $Z(G)$ is all of G). Thus, in particular, $Z(G) \trianglelefteq G$. The subgroup $\langle -1 \rangle$ of Q_8 was previously seen to be the kernel of a homomorphism but since $\langle -1 \rangle = Z(Q_8)$ we obtain normality of this subgroup

now in another fashion. We already saw that $Q_8/\langle -1 \rangle \cong V_4$. The discussion for D_8 in the next paragraph could be applied equally well to Q_8 to give an independent identification of the isomorphism type of the quotient.

Let $G = D_8$ and let $Z = \langle r^2 \rangle = Z(D_8)$. Since $Z = \{1, r^2\}$, each coset, gZ , consists of the two element set $\{g, gr^2\}$. Since these cosets partition the 8 elements of D_8 into pairs, there must be 4 (disjoint) left cosets of Z in D_8 :

$$\bar{1} = 1Z, \quad \bar{r} = rZ, \quad \bar{s} = sZ, \quad \text{and} \quad \bar{rs} = rsZ.$$

Now by the classification of groups of order 4 (Exercise 10, Section 2.5) we know that $D_8/Z(D_8) \cong Z_4$ or V_4 . To determine which of these two is correct (i.e., determine the isomorphism type of the quotient) simply observe that

$$(\bar{r})^2 = r^2Z = 1Z = \bar{1}$$

$$(\bar{s})^2 = s^2Z = 1Z = \bar{1}$$

$$(\bar{rs})^2 = (rs)^2Z = 1Z = \bar{1}$$

so every nonidentity element in D_8/Z has order 2. In particular there is no element of order 4 in the quotient, hence D_8/Z is not cyclic so $D_8/Z(D_8) \cong V_4$.

EXERCISES

Let G and H be groups.

1. Let $\varphi : G \rightarrow H$ be a homomorphism and let E be a subgroup of H . Prove that $\varphi^{-1}(E) \leq G$ (i.e., the preimage or pullback of a subgroup under a homomorphism is a subgroup). If $E \trianglelefteq H$ prove that $\varphi^{-1}(E) \trianglelefteq G$. Deduce that $\ker \varphi \trianglelefteq G$.
2. Let $\varphi : G \rightarrow H$ be a homomorphism of groups with kernel K and let $a, b \in \varphi(G)$. Let $X \in G/K$ be the fiber above a and let Y be the fiber above b , i.e., $X = \varphi^{-1}(a)$, $Y = \varphi^{-1}(b)$. Fix an element u of X (so $\varphi(u) = a$). Prove that if $XY = Z$ in the quotient group G/K and w is any member of Z , then there is some $v \in Y$ such that $uv = w$. [Show $u^{-1}w \in Y$.]
3. Let A be an abelian group and let B be a subgroup of A . Prove that A/B is abelian. Give an example of a non-abelian group G containing a proper normal subgroup N such that G/N is abelian.
4. Prove that in the quotient group G/N , $(gN)^\alpha = g^\alpha N$ for all $\alpha \in \mathbb{Z}$.
5. Use the preceding exercise to prove that the order of the element gN in G/N is n , where n is the smallest positive integer such that $g^n \in N$ (and gN has infinite order if no such positive integer exists). Give an example to show that the order of gN in G/N may be strictly smaller than the order of g in G .
6. Define $\varphi : \mathbb{R}^\times \rightarrow \{\pm 1\}$ by letting $\varphi(x)$ be x divided by the absolute value of x . Describe the fibers of φ and prove that φ is a homomorphism.
7. Define $\pi : \mathbb{R}^2 \rightarrow \mathbb{R}$ by $\pi((x, y)) = x + y$. Prove that π is a surjective homomorphism and describe the kernel and fibers of π geometrically.
8. Let $\varphi : \mathbb{R}^\times \rightarrow \mathbb{R}^\times$ be the map sending x to the absolute value of x . Prove that φ is a homomorphism and find the image of φ . Describe the kernel and the fibers of φ .
9. Define $\varphi : \mathbb{C}^\times \rightarrow \mathbb{R}^\times$ by $\varphi(a + bi) = a^2 + b^2$. Prove that φ is a homomorphism and find the image of φ . Describe the kernel and the fibers of φ geometrically (as subsets of the plane).

10. Let $\varphi : \mathbb{Z}/8\mathbb{Z} \rightarrow \mathbb{Z}/4\mathbb{Z}$ by $\varphi(\bar{a}) = \bar{a}$. Show that this is a well defined, surjective homomorphism and describe its fibers and kernel explicitly (showing that φ is well defined involves the fact that \bar{a} has a different meaning in the domain and range of φ).

11. Let F be a field and let $G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in F, ac \neq 0 \right\} \leq GL_2(F)$.

- (a) Prove that the map $\varphi : \left(\begin{matrix} a & b \\ 0 & c \end{matrix} \right) \mapsto a$ is a surjective homomorphism from G onto F^\times (recall that F^\times is the multiplicative group of nonzero elements in F). Describe the fibers and kernel of φ .
- (b) Prove that the map $\psi : \left(\begin{matrix} a & b \\ 0 & c \end{matrix} \right) \mapsto (a, c)$ is a surjective homomorphism from G onto $F^\times \times F^\times$. Describe the fibers and kernel of ψ .
- (c) Let $H = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in F \right\}$. Prove that H is isomorphic to the additive group F .

12. Let G be the additive group of real numbers, let H be the multiplicative group of complex numbers of absolute value 1 (the unit circle S^1 in the complex plane) and let $\varphi : G \rightarrow H$ be the homomorphism $\varphi : r \mapsto e^{2\pi i r}$. Draw the points on a real line which lie in the kernel of φ . Describe similarly the elements in the fibers of φ above the points -1 , i , and $e^{4\pi i/3}$ of H . (Figure 1 of the text for this homomorphism φ is usually depicted using the following diagram.)

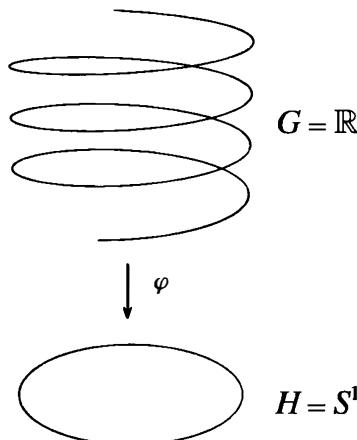


Fig. 5

13. Repeat the preceding exercise with the map φ replaced by the map $\varphi : r \mapsto e^{4\pi i r}$.

14. Consider the additive quotient group \mathbb{Q}/\mathbb{Z} .

- (a) Show that every coset of \mathbb{Z} in \mathbb{Q} contains exactly one representative $q \in \mathbb{Q}$ in the range $0 \leq q < 1$.
- (b) Show that every element of \mathbb{Q}/\mathbb{Z} has finite order but that there are elements of arbitrarily large order.
- (c) Show that \mathbb{Q}/\mathbb{Z} is the torsion subgroup of \mathbb{R}/\mathbb{Z} (cf. Exercise 6, Section 2.1).
- (d) Prove that \mathbb{Q}/\mathbb{Z} is isomorphic to the multiplicative group of root of unity in \mathbb{C}^\times .

15. Prove that a quotient of a divisible abelian group by any proper subgroup is also divisible. Deduce that \mathbb{Q}/\mathbb{Z} is divisible (cf. Exercise 19, Section 2.4).

16. Let G be a group, let N be a normal subgroup of G and let $\overline{G} = G/N$. Prove that if

$G = \langle x, y \rangle$ then $\overline{G} = \langle \bar{x}, \bar{y} \rangle$. Prove more generally that if $G = \langle S \rangle$ for any subset S of G , then $\overline{G} = \langle \bar{S} \rangle$.

17. Let G be the dihedral group of order 16 (whose lattice appears in Section 2.5):

$$G = \langle r, s \mid r^8 = s^2 = 1, rs = sr^{-1} \rangle$$

and let $\overline{G} = G/\langle r^4 \rangle$ be the quotient of G by the subgroup generated by r^4 (this subgroup is the center of G , hence is normal).

- (a) Show that the order of \overline{G} is 8.
- (b) Exhibit each element of \overline{G} in the form $\bar{s}^a \bar{r}^b$, for some integers a and b .
- (c) Find the order of each of the elements of \overline{G} exhibited in (b).
- (d) Write each of the following elements of \overline{G} in the form $\bar{s}^a \bar{r}^b$, for some integers a and b as in (b): \overline{rs} , $\overline{sr^{-2}s}$, $\overline{s^{-1}r^{-1}sr}$.
- (e) Prove that $\overline{H} = \langle \bar{s}, \bar{r}^2 \rangle$ is a normal subgroup of \overline{G} and \overline{H} is isomorphic to the Klein 4-group. Describe the isomorphism type of the complete preimage of \overline{H} in G .
- (f) Find the center of \overline{G} and describe the isomorphism type of $\overline{G}/Z(\overline{G})$.

18. Let G be the quasidihedral group of order 16 (whose lattice was computed in Exercise 11 of Section 2.5):

$$G = \langle \sigma, \tau \mid \sigma^8 = \tau^2 = 1, \sigma\tau = \tau\sigma^3 \rangle$$

and let $\overline{G} = G/\langle \sigma^4 \rangle$ be the quotient of G by the subgroup generated by σ^4 (this subgroup is the center of G , hence is normal).

- (a) Show that the order of \overline{G} is 8.
- (b) Exhibit each element of \overline{G} in the form $\bar{\tau}^a \bar{\sigma}^b$, for some integers a and b .
- (c) Find the order of each of the elements of \overline{G} exhibited in (b).
- (d) Write each of the following elements of \overline{G} in the form $\bar{\tau}^a \bar{\sigma}^b$, for some integers a and b as in (b): $\overline{\sigma\tau}$, $\overline{\tau\sigma^{-2}\tau}$, $\overline{\tau^{-1}\sigma^{-1}\tau\sigma}$.
- (e) Prove that $\overline{G} \cong D_8$.

19. Let G be the modular group of order 16 (whose lattice was computed in Exercise 14 of Section 2.5):

$$G = \langle u, v \mid u^2 = v^8 = 1, vu = uv^5 \rangle$$

and let $\overline{G} = G/\langle v^4 \rangle$ be the quotient of G by the subgroup generated by v^4 (this subgroup is contained in the center of G , hence is normal).

- (a) Show that the order of \overline{G} is 8.
- (b) Exhibit each element of \overline{G} in the form $\bar{u}^a \bar{v}^b$, for some integers a and b .
- (c) Find the order of each of the elements of \overline{G} exhibited in (b).
- (d) Write each of the following elements of \overline{G} in the form $\bar{u}^a \bar{v}^b$, for some integers a and b as in (b): \overline{vu} , $\overline{uv^{-2}u}$, $\overline{u^{-1}v^{-1}uv}$.
- (e) Prove that \overline{G} is abelian and is isomorphic to $Z_2 \times Z_4$.

20. Let $G = \mathbb{Z}/24\mathbb{Z}$ and let $\tilde{G} = G/\langle \overline{12} \rangle$, where for each integer a we simplify notation by writing $\tilde{\tilde{a}}$ as \tilde{a} .

- (a) Show that $\tilde{G} = \{\tilde{0}, \tilde{1}, \dots, \tilde{11}\}$.
- (b) Find the order of each element of \tilde{G} .
- (c) Prove that $\tilde{G} \cong \mathbb{Z}/12\mathbb{Z}$. (Thus $(\mathbb{Z}/24\mathbb{Z})/\langle 12\mathbb{Z}/24\mathbb{Z} \rangle \cong \mathbb{Z}/12\mathbb{Z}$, just as if we inverted and cancelled the $24\mathbb{Z}$'s.)

21. Let $G = Z_4 \times Z_4$ be given in terms of the following generators and relations:

$$G = \langle x, y \mid x^4 = y^4 = 1, xy = yx \rangle.$$

Let $\bar{G} = G/\langle x^2y^2 \rangle$ (note that every subgroup of the abelian group G is normal).

- (a) Show that the order of \bar{G} is 8.
- (b) Exhibit each element of \bar{G} in the form $\bar{x}^a\bar{y}^b$, for some integers a and b .
- (c) Find the order of each of the elements of \bar{G} exhibited in (b).
- (d) Prove that $\bar{G} \cong \mathbb{Z}_4 \times \mathbb{Z}_2$.

22. (a) Prove that if H and K are normal subgroups of a group G then their intersection $H \cap K$ is also a normal subgroup of G .
- (b) Prove that the intersection of an arbitrary nonempty collection of normal subgroups of a group is a normal subgroup (do not assume the collection is countable).
23. Prove that the join (cf. Section 2.5) of any nonempty collection of normal subgroups of a group is a normal subgroup.
24. Prove that if $N \trianglelefteq G$ and H is any subgroup of G then $N \cap H \trianglelefteq H$.
25. (a) Prove that a subgroup N of G is normal if and only if $gNg^{-1} \subseteq N$ for all $g \in G$.
- (b) Let $G = GL_2(\mathbb{Q})$, let N be the subgroup of upper triangular matrices with integer entries and 1's on the diagonal, and let g be the diagonal matrix with entries 2,1. Show that $gNg^{-1} \subseteq N$ but g does *not* normalize N .
26. Let $a, b \in G$.
- (a) Prove that the conjugate of the product of a and b is the product of the conjugate of a and the conjugate of b . Prove that the order of a and the order of any conjugate of a are the same.
 - (b) Prove that the conjugate of a^{-1} is the inverse of the conjugate of a .
 - (c) Let $N = \langle S \rangle$ for some subset S of G . Prove that $N \trianglelefteq G$ if $gSg^{-1} \subseteq N$ for all $g \in G$.
 - (d) Deduce that if N is the cyclic group $\langle x \rangle$, then N is normal in G if and only if for each $g \in G$, $gxg^{-1} = x^k$ for some $k \in \mathbb{Z}$.
 - (e) Let n be a positive integer. Prove that the subgroup N of G generated by all the elements of G of order n is a normal subgroup of G .
27. Let N be a *finite* subgroup of a group G . Show that $gNg^{-1} \subseteq N$ if and only if $gNg^{-1} = N$. Deduce that $N_G(N) = \{g \in G \mid gNg^{-1} \subseteq N\}$.
28. Let N be a *finite* subgroup of a group G and assume $N = \langle S \rangle$ for some subset S of G . Prove that an element $g \in G$ normalizes N if and only if $gSg^{-1} \subseteq N$.
29. Let N be a *finite* subgroup of G and suppose $G = \langle T \rangle$ and $N = \langle S \rangle$ for some subsets S and T of G . Prove that N is normal in G if and only if $tSt^{-1} \subseteq N$ for all $t \in T$.
30. Let $N \trianglelefteq G$ and let $g \in G$. Prove that $gN = Ng$ if and only if $g \in N_G(N)$.
31. Prove that if $H \trianglelefteq G$ and N is a normal subgroup of H then $H \trianglelefteq N_G(N)$. Deduce that $N_G(N)$ is the largest subgroup of G in which N is normal (i.e., is the join of all subgroups H for which $N \trianglelefteq H$).
32. Prove that every subgroup of Q_8 is normal. For each subgroup find the isomorphism type of its corresponding quotient. [You may use the lattice of subgroups for Q_8 in Section 2.5.]
33. Find all normal subgroups of D_8 and for each of these find the isomorphism type of its corresponding quotient. [You may use the lattice of subgroups for D_8 in Section 2.5.]
34. Let $D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$ be the usual presentation of the dihedral group of order $2n$ and let k be a positive integer dividing n .
- (a) Prove that $\langle r^k \rangle$ is a normal subgroup of D_{2n} .
 - (b) Prove that $D_{2n}/\langle r^k \rangle \cong D_{2k}$.

35. Prove that $SL_n(F) \trianglelefteq GL_n(F)$ and describe the isomorphism type of the quotient group (cf. Exercise 9, Section 2.1).
36. Prove that if $G/Z(G)$ is cyclic then G is abelian. [If $G/Z(G)$ is cyclic with generator $xZ(G)$, show that every element of G can be written in the form $x^a z$ for some integer $a \in \mathbb{Z}$ and some element $z \in Z(G)$.]
37. Let A and B be groups. Show that $\{(a, 1) \mid a \in A\}$ is a normal subgroup of $A \times B$ and the quotient of $A \times B$ by this subgroup is isomorphic to B .
38. Let A be an abelian group and let D be the (diagonal) subgroup $\{(a, a) \mid a \in A\}$ of $A \times A$. Prove that D is a normal subgroup of $A \times A$ and $(A \times A)/D \cong A$.
39. Suppose A is the non-abelian group S_3 and D is the diagonal subgroup $\{(a, a) \mid a \in A\}$ of $A \times A$. Prove that D is not normal in $A \times A$.
40. Let G be a group, let N be a normal subgroup of G and let $\bar{G} = G/N$. Prove that \bar{x} and \bar{y} commute in \bar{G} if and only if $x^{-1}y^{-1}xy \in N$. (The element $x^{-1}y^{-1}xy$ is called the *commutator* of x and y and is denoted by $[x, y]$.)
41. Let G be a group. Prove that $N = \langle x^{-1}y^{-1}xy \mid x, y \in G \rangle$ is a normal subgroup of G and G/N is abelian (N is called the *commutator subgroup* of G).
42. Assume both H and K are normal subgroups of G with $H \cap K = 1$. Prove that $xy = yx$ for all $x \in H$ and $y \in K$. [Show $x^{-1}y^{-1}xy \in H \cap K$.]
43. Assume $\mathcal{P} = \{A_i \mid i \in I\}$ is any partition of G with the property that \mathcal{P} is a group under the “quotient operation” defined as follows: to compute the product of A_i with A_j take any element a_i of A_i and any element a_j of A_j and let $A_i A_j$ be the element of \mathcal{P} containing $a_i a_j$ (this operation is assumed to be well defined). Prove that the element of \mathcal{P} that contains the identity of G is a normal subgroup of G and the elements of \mathcal{P} are the cosets of this subgroup (so \mathcal{P} is just a quotient group of G in the usual sense).

3.2 MORE ON COSETS AND LAGRANGE’S THEOREM

In this section we continue the study of quotient groups. Since for finite groups one of the most important invariants of a group is its order we first prove that the order of a quotient group of a finite group can be readily computed: $|G/N| = \frac{|G|}{|N|}$. In fact we derive this as a consequence of a more general result, Lagrange’s Theorem (see Exercise 19, Section 1.7). This theorem is one of the most important combinatorial results in finite group theory and will be used repeatedly. After indicating some easy consequences of Lagrange’s Theorem we study more subtle questions concerning cosets of non-normal subgroups.

The proof of Lagrange’s Theorem is straightforward and important. It is the same line of reasoning we used in Example 3 of the preceding section to compute $|D_8/Z(D_8)|$.

Theorem 8. (Lagrange’s Theorem) If G is a finite group and H is a subgroup of G , then the order of H divides the order of G (i.e., $|H| \mid |G|$) and the number of left cosets of H in G equals $\frac{|G|}{|H|}$.

Proof: Let $|H| = n$ and let the number of left cosets of H in G equal k . By

Proposition 4 the set of left cosets of H in G partition G . By definition of a left coset the map:

$$H \rightarrow gH \quad \text{defined by} \quad h \mapsto gh$$

is a surjection from H to the left coset gH . The left cancellation law implies this map is injective since $gh_1 = gh_2$ implies $h_1 = h_2$. This proves that H and gH have the same order:

$$|gH| = |H| = n.$$

Since G is partitioned into k disjoint subsets each of which has cardinality n , $|G| = kn$. Thus $k = \frac{|G|}{n} = \frac{|G|}{|H|}$, completing the proof.

Definition. If G is a group (possibly infinite) and $H \leq G$, the number of left cosets of H in G is called the *index* of H in G and is denoted by $|G : H|$.

In the case of finite groups the index of H in G is $\frac{|G|}{|H|}$. For G an infinite group the quotient $\frac{|G|}{|H|}$ does not make sense. Infinite groups may have subgroups of finite or infinite index (e.g., $\{0\}$ is of infinite index in \mathbb{Z} and $\langle n \rangle$ is of index n in \mathbb{Z} for every $n > 0$).

We now derive some easy consequences of Lagrange's Theorem.

Corollary 9. If G is a finite group and $x \in G$, then the order of x divides the order of G . In particular $x^{|G|} = 1$ for all x in G .

Proof: By Proposition 2.2, $|x| = |\langle x \rangle|$. The first part of the corollary follows from Lagrange's Theorem applied to $H = \langle x \rangle$. The second statement is clear since now $|G|$ is a multiple of the order of x .

Corollary 10. If G is a group of prime order p , then G is cyclic, hence $G \cong \mathbb{Z}_p$.

Proof: Let $x \in G$, $x \neq 1$. Thus $|\langle x \rangle| > 1$ and $|\langle x \rangle|$ divides $|G|$. Since $|G|$ is prime we must have $|\langle x \rangle| = |G|$, hence $G = \langle x \rangle$ is cyclic (with any nonidentity element x as generator). Theorem 2.4 completes the proof.

With Lagrange's Theorem in hand we examine some additional examples of normal subgroups.

Examples

(1) Let $H = \langle (1 2 3) \rangle \leq S_3$ and let $G = S_3$. We show $H \trianglelefteq S_3$. As noted in Section 2.2,

$$H \leq N_G(H) \leq G.$$

By Lagrange's Theorem, the order of H divides the order of $N_G(H)$ and the order of $N_G(H)$ divides the order of G . Since G has order 6 and H has order 3, the only possibilities for $N_G(H)$ are H or G . A direct computation gives

$$(1 2)(1 2 3)(1 2) = (1 3 2) = (1 2 3)^{-1}.$$

Since $(1\ 2) = (1\ 2)^{-1}$, this calculation shows that $(1\ 2)$ conjugates a generator of H to another generator of H . By Exercise 24 of Section 2.3 this is sufficient to prove that $(1\ 2) \in N_G(H)$. Thus $N_G(H) \neq H$ so $N_G(H) = G$, i.e., $H \trianglelefteq S_3$, as claimed. This argument illustrates that checking normality of a subgroup can often be reduced to a small number of calculations. A generalization of this example is given in the next example.

- (2) Let G be any group containing a subgroup H of index 2. We prove $H \trianglelefteq G$. Let $g \in G - H$ so, by hypothesis, the two left cosets of H in G are $1H$ and gH . Since $1H = H$ and the cosets partition G , we must have $gH = G - H$. Now the two right cosets of H in G are $H1$ and Hg . Since $H1 = H$, we again must have $Hg = G - H$. Combining these gives $gH = Hg$, so every left coset of H in G is a right coset. By Theorem 6, $H \trianglelefteq G$. By definition of index, $|G/H| = 2$, so that $G/H \cong Z_2$. One must be careful to appreciate that the reason H is normal in this case is not because we can choose the same coset representatives 1 and g for both the left and right cosets of H but that there is a type of pigeon-hole principle at work: since $1H = H = H1$ for any subgroup H of any group G , the index assumption forces the remaining elements to comprise the remaining coset (either left or right). We shall see that this result is itself a special case of a result we shall prove in the next chapter.

Note that this result proves that $\langle i \rangle$, $\langle j \rangle$ and $\langle k \rangle$ are normal subgroups of Q_8 and that $\langle s, r^2 \rangle$, $\langle r \rangle$ and $\langle sr, r^2 \rangle$ are normal subgroups of D_8 .

- (3) The property “is a normal subgroup of” is not transitive. For example,

$$\langle s \rangle \trianglelefteq \langle s, r^2 \rangle \trianglelefteq D_8$$

(each subgroup is of index 2 in the next), however, $\langle s \rangle$ is not normal in D_8 because $rsr^{-1} = sr^2 \notin \langle s \rangle$.

We now examine some examples of non-normal subgroups. Although in abelian groups every subgroup is normal, this is not the case in non-abelian groups (in some sense Q_8 is the unique exception to this). In fact, there are groups G in which the only normal subgroups are the trivial ones: 1 and G . Such groups are called *simple groups* (simple does not mean easy, however). Simple groups play an important role in the study of general groups and this role will be described in Section 4. For now we emphasize that not every subgroup of a group G is normal in G ; indeed, normal subgroups may be quite rare in G . The search for normal subgroups of a given group is in general a highly nontrivial problem.

Examples

- (1) Let $H = \langle (1\ 2) \rangle \leq S_3$. Since H is of prime index 3 in S_3 , by Lagrange’s Theorem the only possibilities for $N_{S_3}(H)$ are H or S_3 . Direct computation shows

$$(1\ 3)(1\ 2)(1\ 3)^{-1} = (1\ 3)(1\ 2)(1\ 3) = (2\ 3) \notin H$$

so $N_{S_3}(H) \neq S_3$, that is, H is not a normal subgroup of S_3 . One can also see this by considering the left and right cosets of H ; for instance

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

Since the left coset $(1\ 3)H$ is the unique left coset of H containing $(1\ 3)$, the right coset $H(1\ 3)$ cannot be a left coset (see also Exercise 6). Note also that the “group operation” on the left cosets of H in S_3 defined by multiplying representatives is not

even well defined. For example, consider the product of the two left cosets $1H$ and $(1\ 3)H$. The elements 1 and $(1\ 2)$ are both representatives for the coset $1H$, yet $1 \cdot (1\ 3) = (1\ 3)$ and $(1\ 2) \cdot (1\ 3) = (1\ 3\ 2)$ are not both elements of the same left coset as they should be if the product of these cosets were independent of the particular representatives chosen. This is an example of Theorem 6 which states that the cosets of a subgroup form a group *only* when the subgroup is a normal subgroup.

(2) Let $G = S_n$ for some $n \in \mathbb{Z}^+$ and fix some $i \in \{1, 2, \dots, n\}$. As in Section 2.2 let

$$G_i = \{\sigma \in G \mid \sigma(i) = i\}$$

be the stabilizer of the point i . Suppose $\tau \in G$ and $\tau(i) = j$. It follows directly from the definition of G_i that for all $\sigma \in G_i$, $\tau\sigma(i) = j$. Furthermore, if $\mu \in G$ and $\mu(i) = j$, then $\tau^{-1}\mu(i) = i$, that is, $\tau^{-1}\mu \in G_i$, so $\mu \in \tau G_i$. This proves that

$$\tau G_i = \{\mu \in G \mid \mu(i) = j\},$$

i.e., the left coset τG_i consists of the permutations in S_n which take i to j . We can clearly see that distinct left cosets have empty intersection and that the number of distinct left cosets equals the number of distinct images of the integer i under the action of G , namely there are n distinct left cosets. Thus $|G : G_i| = n$. Using the same notation let $k = \tau^{-1}(i)$, so that $\tau(k) = i$. By similar reasoning we see that

$$G_i \tau = \{\lambda \in G \mid \lambda(k) = i\},$$

i.e., the right coset $G_i \tau$ consists of the permutations in S_n which take k to i . If $n > 2$, for some nonidentity element τ we have $\tau G_i \neq G_i \tau$ since there are certainly permutations which take i to j but do not take k to i . Thus G_i is not a normal subgroup. In fact $N_G(G_i) = G_i$ by Exercise 30 of Section 1, so G_i is in some sense far from being normal in S_n . This example generalizes the preceding one.

(3) In D_8 the only subgroup of order 2 which is normal is the center $\langle r^2 \rangle$.

We shall see many more examples of non-normal subgroups as we develop the theory.

The *full converse* to Lagrange's Theorem is *not* true: namely, if G is a finite group and n divides $|G|$, then G need not have a subgroup of order n . For example, let A be the group of symmetries of a regular tetrahedron. By Exercise 9 of Section 1.2, $|A| = 12$.

Suppose A had a subgroup H of order 6. Since $\frac{|A|}{|H|} = 2$, H would be of index 2 in A , hence $H \trianglelefteq A$ and $A/H \cong \mathbb{Z}_2$. Since the quotient group has order 2, the square of every element in the quotient is the identity, so for all $g \in A$, $(gH)^2 = 1H$, that is, for all $g \in A$, $g^2 \in H$. If g is an element of A of order 3, we obtain $g = (g^2)^2 \in H$, that is, H must contain all elements of A of order 3. This is a contradiction since $|H| = 6$ but one can easily exhibit 8 rotations of a tetrahedron of order 3.

There are some partial converses to Lagrange's Theorem. For finite *abelian* groups the full converse of Lagrange is true, namely an abelian group has a subgroup of order n for each divisor n of $|G|$ (in fact, this holds under weaker assumptions than "abelian"; we shall see this in Chapter 6). A partial converse which holds for arbitrary finite groups is the following result:

Theorem 11. (*Cauchy's Theorem*) If G is a finite group and p is a prime dividing $|G|$, then G has an element of order p .

Proof: We shall give a proof of this in the next chapter and another elegant proof is outlined in Exercise 9.

The strongest converse to Lagrange's Theorem which applies to *arbitrary* finite groups is the following:

Theorem 12. (*Sylow*) If G is a finite group of order $p^\alpha m$, where p is a prime and p does not divide m , then G has a subgroup of order p^α .

We shall prove this theorem in the next chapter and derive more information on the number of subgroups of order p^α .

We conclude this section with some useful results involving cosets.

Definition. Let H and K be subgroups of a group and define

$$HK = \{hk \mid h \in H, k \in K\}.$$

Proposition 13. If H and K are finite subgroups of a group then

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Proof: Notice that HK is a union of left cosets of K , namely,

$$HK = \bigcup_{h \in H} hK.$$

Since each coset of K has $|K|$ elements it suffices to find the number of *distinct* left cosets of the form hK , $h \in H$. But $h_1K = h_2K$ for $h_1, h_2 \in H$ if and only if $h_2^{-1}h_1 \in K$. Thus

$$h_1K = h_2K \Leftrightarrow h_2^{-1}h_1 \in H \cap K \Leftrightarrow h_1(H \cap K) = h_2(H \cap K).$$

Thus the number of distinct cosets of the form hK , for $h \in H$ is the number of distinct cosets $h(H \cap K)$, for $h \in H$. The latter number, by Lagrange's Theorem, equals $\frac{|H|}{|H \cap K|}$. Thus HK consists of $\frac{|H|}{|H \cap K|}$ distinct cosets of K (each of which has $|K|$ elements) which gives the formula above.

Notice that there was no assumption that HK be a subgroup in Proposition 13. For example, if $G = S_3$, $H = \langle (12) \rangle$ and $K = \langle (23) \rangle$, then $|H| = |K| = 2$ and $|H \cap K| = 1$, so $|HK| = 4$. By Lagrange's Theorem HK cannot be a subgroup. As a consequence, we must have $S_3 = \langle (12), (23) \rangle$.

Proposition 14. If H and K are subgroups of a group, HK is a subgroup if and only if $HK = KH$.

Proof: Assume first that $HK = KH$ and let $a, b \in HK$. We prove $ab^{-1} \in HK$ so HK is a subgroup by the subgroup criterion. Let

$$a = h_1 k_1 \quad \text{and} \quad b = h_2 k_2,$$

for some $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Thus $b^{-1} = k_2^{-1} h_2^{-1}$, so $ab^{-1} = h_1 k_1 k_2^{-1} h_2^{-1}$. Let $k_3 = k_1 k_2^{-1} \in K$ and $h_3 = h_2^{-1}$. Thus $ab^{-1} = h_1 k_3 h_3$. Since $HK = KH$,

$$k_3 h_3 = h_4 k_4, \quad \text{for some } h_4 \in H, \quad k_4 \in K.$$

Thus $ab^{-1} = h_1 h_4 k_4$, and since $h_1 h_4 \in H, k_4 \in K$, we obtain $ab^{-1} \in HK$, as desired.

Conversely, assume that HK is a subgroup of G . Since $K \leq HK$ and $H \leq HK$, by the closure property of subgroups, $KH \subseteq HK$. To show the reverse containment let $hk \in HK$. Since HK is assumed to be a subgroup, write $hk = a^{-1}$, for some $a \in HK$. If $a = h_1 k_1$, then

$$hk = (h_1 k_1)^{-1} = k_1^{-1} h_1^{-1} \in KH,$$

completing the proof.

Note that $HK = KH$ does *not* imply that the elements of H commute with those of K (contrary to what the notation may suggest) but rather that every product hk is of the form $k'h'$ (h need not be h' nor k be k') and conversely. For example, if $G = D_{2n}$, $H = \langle r \rangle$ and $K = \langle s \rangle$, then $G = HK = KH$ so that HK is a subgroup and $rs = sr^{-1}$ so the elements of H do not commute with the elements of K . This is an example of the following sufficient condition for HK to be a subgroup:

Corollary 15. If H and K are subgroups of G and $H \leq N_G(K)$, then HK is a subgroup of G . In particular, if $K \trianglelefteq G$ then $HK \leq G$ for any $H \leq G$.

Proof: We prove $HK = KH$. Let $h \in H, k \in K$. By assumption, $hkh^{-1} \in K$, hence

$$hk = (hkh^{-1})h \in KH.$$

This proves $HK \subseteq KH$. Similarly, $kh = h(h^{-1}kh) \in HK$, proving the reverse containment. The corollary follows now from the preceding proposition.

Definition. If A is any subset of $N_G(K)$ (or $C_G(K)$), we shall say A normalizes K (centralizes K , respectively).

With this terminology, Corollary 15 states that HK is a subgroup if H normalizes K (similarly, HK is a subgroup if K normalizes H).

In some instances one can prove that a finite group is a product of two of its subgroups by simply using the order formula in Proposition 13. For example, let $G = S_4$, $H = D_8$ and let $K = \langle (1\ 2\ 3) \rangle$, where we consider D_8 as a subgroup of S_4 by identifying each symmetry with its permutation on the 4 vertices of a square

(under some fixed labelling). By Lagrange's Theorem, $H \cap K = 1$ (see Exercise 8). Proposition 13 then shows $|HK| = 24$ hence we must have $HK = S_4$. Since HK is a group, $HK = KH$. We leave as an exercise the verification that neither H nor K normalizes the other (so Corollary 15 could not have been used to give $HK = KH$).

Finally, throughout this chapter we have worked with left cosets of a subgroup. The same combinatorial results could equally well have been proved using right cosets. For normal subgroups this is trivial since left and right cosets are the same, but for non-normal subgroups some left cosets are not right cosets (for any choice of representative) so some (simple) verifications are necessary. For example, Lagrange's Theorem gives that in a finite group G

$$\text{the number of right cosets of the subgroup } H \text{ is } \frac{|G|}{|H|}.$$

Thus in a finite group the *number* of left cosets of H in G equals the *number* of right cosets even though the left cosets are not right cosets in general. This is also true for infinite groups as Exercise 12 below shows. Thus for purely combinatorial purposes one may use either left or right cosets (but not a mixture when a partition of G is needed). Our consistent use of left cosets is somewhat arbitrary although it will have some benefits when we discuss actions on cosets in the next chapter. Readers may encounter in some works the notation $H \setminus G$ to denote the set of right cosets of H in G .

In some papers one may also see the notation G/H used to denote the set of left cosets of H in G even when H is not normal in G (in which case G/H is called the *coset space* of left cosets of H in G). We shall not use this notation.

EXERCISES

Let G be a group.

- Which of the following are permissible orders for subgroups of a group of order 120: 1, 2, 5, 7, 9, 15, 60, 240? For each permissible order give the corresponding index.
- Prove that the lattice of subgroups of S_3 in Section 2.5 is correct (i.e., prove that it contains all subgroups of S_3 and that their pairwise joins and intersections are correctly drawn).
- Prove that the lattice of subgroups of Q_8 in Section 2.5 is correct.
- Show that if $|G| = pq$ for some primes p and q (not necessarily distinct) then either G is abelian or $Z(G) = 1$. [See Exercise 36 in Section 1.]
- Let H be a subgroup of G and fix some element $g \in G$.
 - Prove that gHg^{-1} is a subgroup of G of the same order as H .
 - Deduce that if $n \in \mathbb{Z}^+$ and H is the unique subgroup of G of order n then $H \trianglelefteq G$.
- Let $H \leq G$ and let $g \in G$. Prove that if the right coset Hg equals *some* left coset of H in G then it equals the left coset gH and g must be in $N_G(H)$.
- Let $H \leq G$ and define a relation \sim on G by $a \sim b$ if and only if $b^{-1}a \in H$. Prove that \sim is an equivalence relation and describe the equivalence class of each $a \in G$. Use this to prove Proposition 4.
- Prove that if H and K are finite subgroups of G whose orders are relatively prime then $H \cap K = 1$.

9. This exercise outlines a proof of Cauchy's Theorem due to James McKay (*Another proof of Cauchy's group theorem*, Amer. Math. Monthly, 66(1959), p. 119). Let G be a finite group and let p be a prime dividing $|G|$. Let \mathcal{S} denote the set of p -tuples of elements of G the product of whose coordinates is 1:

$$\mathcal{S} = \{(x_1, x_2, \dots, x_p) \mid x_i \in G \text{ and } x_1 x_2 \cdots x_p = 1\}.$$

- (a) Show that \mathcal{S} has $|G|^{p-1}$ elements, hence has order divisible by p .

Define the relation \sim on \mathcal{S} by letting $\alpha \sim \beta$ if β is a cyclic permutation of α .

- (b) Show that a cyclic permutation of an element of \mathcal{S} is again an element of \mathcal{S} .
(c) Prove that \sim is an equivalence relation on \mathcal{S} .
(d) Prove that an equivalence class contains a single element if and only if it is of the form (x, x, \dots, x) with $x^p = 1$.
(e) Prove that every equivalence class has order 1 or p (this uses the fact that p is a prime). Deduce that $|G|^{p-1} = k + pd$, where k is the number of classes of size 1 and d is the number of classes of size p .
(f) Since $\{(1, 1, \dots, 1)\}$ is an equivalence class of size 1, conclude from (e) that there must be a nonidentity element x in G with $x^p = 1$, i.e., G contains an element of order p . [Show $p \mid k$ and so $k > 1$.]

10. Suppose H and K are subgroups of finite index in the (possibly infinite) group G with $|G : H| = m$ and $|G : K| = n$. Prove that $\text{l.c.m.}(m, n) \leq |G : H \cap K| \leq mn$. Deduce that if m and n are relatively prime then $|G : H \cap K| = |G : H| \cdot |G : K|$.
11. Let $H \leq K \leq G$. Prove that $|G : H| = |G : K| \cdot |K : H|$ (do not assume G is finite).
12. Let $H \leq G$. Prove that the map $x \mapsto x^{-1}$ sends each left coset of H in G onto a right coset of H and gives a bijection between the set of left cosets and the set of right cosets of H in G (hence the number of left cosets of H in G equals the number of right cosets).
13. Fix any labelling of the vertices of a square and use this to identify D_8 as a subgroup of S_4 . Prove that the elements of D_8 and $\langle (1\ 2\ 3) \rangle$ do not commute in S_4 .
14. Prove that S_4 does not have a normal subgroup of order 8 or a normal subgroup of order 3.
15. Let $G = S_n$ and for fixed $i \in \{1, 2, \dots, n\}$ let G_i be the stabilizer of i . Prove that $G_i \cong S_{n-1}$.
16. Use Lagrange's Theorem in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ to prove *Fermat's Little Theorem*: if p is a prime then $a^p \equiv a \pmod{p}$ for all $a \in \mathbb{Z}$.
17. Let p be a prime and let n be a positive integer. Find the order of \bar{p} in $(\mathbb{Z}/(p^n-1)\mathbb{Z})^\times$ and deduce that $n \mid \varphi(p^n - 1)$ (here φ is Euler's function).
18. Let G be a finite group, let H be a subgroup of G and let $N \trianglelefteq G$. Prove that if $|H|$ and $|G : N|$ are relatively prime then $H \leq N$.
19. Prove that if N is a normal subgroup of the finite group G and $(|N|, |G : N|) = 1$ then N is the unique subgroup of G of order $|N|$.
20. If A is an abelian group with $A \trianglelefteq G$ and B is any subgroup of G prove that $A \cap B \trianglelefteq AB$.
21. Prove that \mathbb{Q} has no proper subgroups of finite index. Deduce that \mathbb{Q}/\mathbb{Z} has no proper subgroups of finite index. [Recall Exercise 21, Section 1.6 and Exercise 15, Section 1.]
22. Use Lagrange's Theorem in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ to prove *Euler's Theorem*: $a^{\varphi(n)} \equiv 1 \pmod{n}$ for every integer a relatively prime to n , where φ denotes Euler's φ -function.
23. Determine the last two digits of $3^{3^{100}}$. [Determine $3^{100} \pmod{\varphi(100)}$ and use the previous exercise.]

3.3 THE ISOMORPHISM THEOREMS

In this section we derive some straightforward consequences of the relations between quotient groups and homomorphisms which were discussed in Section 1. In particular we consider the relation between the lattice of subgroups of a quotient group, G/N , and the lattice of subgroups of the group G . The first result restates our observations in Section 1 on the relation of the image of a homomorphism to the quotient by the kernel (sometimes called the Fundamental Theorem of Homomorphisms):

Theorem 16. (*The First Isomorphism Theorem*) If $\varphi : G \rightarrow H$ is a homomorphism of groups, then $\ker \varphi \trianglelefteq G$ and $G/\ker \varphi \cong \varphi(G)$.

Corollary 17. Let $\varphi : G \rightarrow H$ be a homomorphism of groups.

- (1) φ is injective if and only if $\ker \varphi = 1$.
- (2) $|G : \ker \varphi| = |\varphi(G)|$.

Proof: Exercise.

When we consider abstract vector spaces we shall see that Corollary 17(2) gives a formula possibly already familiar from the theory of linear transformations: if $\varphi : V \rightarrow W$ is a linear transformation of vector spaces, then $\dim V = \text{rank } \varphi + \text{nullity } \varphi$.

Theorem 18. (*The Second or Diamond Isomorphism Theorem*) Let G be a group, let A and B be subgroups of G and assume $A \leq N_G(B)$. Then AB is a subgroup of G , $B \trianglelefteq AB$, $A \cap B \trianglelefteq A$ and $AB/B \cong A/A \cap B$.

Proof: By Corollary 15, AB is a subgroup of G . Since $A \leq N_G(B)$ by assumption and $B \leq N_G(B)$ trivially, it follows that $AB \leq N_G(B)$, i.e., B is a normal subgroup of the subgroup AB .

Since B is normal in AB , the quotient group AB/B is well defined. Define the map $\varphi : A \rightarrow AB/B$ by $\varphi(a) = aB$. Since the group operation in AB/B is well defined it is easy to see that φ is a homomorphism:

$$\varphi(a_1 a_2) = (a_1 a_2)B = a_1 B \cdot a_2 B = \varphi(a_1)\varphi(a_2).$$

Alternatively, the map φ is just the restriction to the subgroup A of the natural projection homomorphism $\pi : AB \rightarrow AB/B$, so is also a homomorphism. It is clear from the definition of AB that φ is surjective. The identity in AB/B is the coset $1B$, so the kernel of φ consists of the elements $a \in A$ with $aB = 1B$, which by Proposition 4 are the elements $a \in B$, i.e., $\ker \varphi = A \cap B$. By the First Isomorphism Theorem, $A \cap B \trianglelefteq A$ and $A/A \cap B \cong AB/B$, completing the proof.

Note that this gives a new proof of the order formula in Proposition 13 in the special case that $A \leq N_G(B)$. The reason this theorem is called the Diamond Isomorphism is because of the portion of the lattice of subgroups of G involved (see Figure 6). The markings in the lattice lines indicate which quotients are isomorphic. The “quotient”

AB/A need not be a group (i.e., A need not be normal in AB), however we still have $|AB : A| = |B : A \cap B|$.

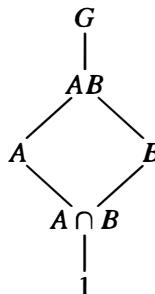


Fig. 6

The third Isomorphism Theorem considers the question of taking quotient groups of quotient groups.

Theorem 19. (The Third Isomorphism Theorem) Let G be a group and let H and K be normal subgroups of G with $H \leq K$. Then $K/H \trianglelefteq G/H$ and

$$(G/H)/(K/H) \cong G/K.$$

If we denote the quotient by H with a bar, this can be written

$$\overline{G/K} \cong G/K.$$

Proof: We leave as an easy exercise the verification that $K/H \trianglelefteq G/H$. Define

$$\varphi : G/H \rightarrow G/K$$

$$(gH) \mapsto gK.$$

To show φ is well defined suppose $g_1H = g_2H$. Then $g_1 = g_2h$, for some $h \in H$. Because $H \leq K$, the element h is also an element of K , hence $g_1K = g_2K$ i.e., $\varphi(g_1H) = \varphi(g_2H)$, which shows φ is well defined. Since g may be chosen arbitrarily in G , φ is a surjective homomorphism. Finally,

$$\begin{aligned} \ker \varphi &= \{gH \in G/H \mid \varphi(gH) = 1K\} \\ &= \{gH \in G/H \mid gK = 1K\} \\ &= \{gH \in G/H \mid g \in K\} = K/H. \end{aligned}$$

By the First Isomorphism Theorem, $(G/H)/(K/H) \cong G/K$.

An easy aid for remembering the Third Isomorphism Theorem is: “invert and cancel” (as one would for fractions). This theorem shows that we gain no new structural information from taking quotients of a quotient group.

The final isomorphism theorem describes the relation between the lattice of subgroups of the quotient group G/N and the lattice of subgroups of G . The lattice for G/N can be read immediately from the lattice for G by collapsing the group N to the identity. More precisely, there is a one-to-one correspondence between the subgroups of G containing N and the subgroups of G/N , so that the lattice for G/N (or rather, an isomorphic copy) appears in the lattice for G as the collection of subgroups of G between N and G . In particular, the lattice for G/N appears at the “top” of the lattice for G , a result we mentioned at the beginning of the chapter.

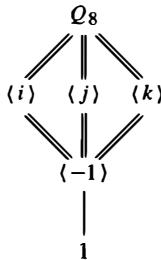
Theorem 20. (The Fourth or Lattice Isomorphism Theorem) Let G be a group and let N be a normal subgroup of G . Then there is a bijection from the set of subgroups A of G which contain N onto the set of subgroups $\bar{A} = A/N$ of G/N . In particular, every subgroup of \bar{G} is of the form A/N for some subgroup A of G containing N (namely, its preimage in G under the natural projection homomorphism from G to G/N). This bijection has the following properties: for all $A, B \leq G$ with $N \leq A$ and $N \leq B$,

- (1) $A \leq B$ if and only if $\bar{A} \leq \bar{B}$,
- (2) if $A \leq B$, then $|B : A| = |\bar{B} : \bar{A}|$,
- (3) $\langle A, B \rangle = \langle \bar{A}, \bar{B} \rangle$,
- (4) $\bar{A} \cap \bar{B} = \bar{A} \cap \bar{B}$, and
- (5) $A \trianglelefteq G$ if and only if $\bar{A} \trianglelefteq \bar{G}$.

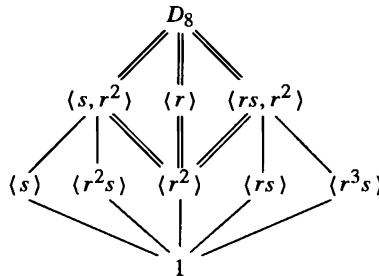
Proof: The complete preimage of a subgroup in G/N is a subgroup of G by Exercise 1 of Section 1. The numerous details of the theorem to check are all completely straightforward. We therefore leave the proof of this theorem to the exercises.

Examples

- (1) Let $G = Q_8$ and let N be the normal subgroup $\langle -1 \rangle$. The (isomorphic copy of the) lattice of G/N consists of the double lines in the lattice of G below. Note that we previously proved that $Q_8/\langle -1 \rangle \cong V_4$ and the two lattices do indeed coincide (see Section 2.5 for the lattices of Q_8 and V_4).



- (2) The same process gives us the lattice of $D_8/\langle r^2 \rangle$ (the double lines) in the lattice of D_8 :



Note that in the second example above there are subgroups of G which do not directly correspond to subgroups in the quotient group G/N , namely the subgroups of G which do not contain the normal subgroup N . This is because the subgroup N projects to a point in G/N and so several subgroups of G can project to the same

subgroup in the quotient. The image of the subgroup H of G under the natural projection homomorphism from G to G/N is the same as the image of the subgroup HN of G , and the subgroup HN of G contains N . Conversely, the preimage of a subgroup \bar{H} of G/N contains N and is the unique subgroup of G containing N whose image in G/N is \bar{H} . It is the subgroups of G containing N which appear explicitly in the lattice for G/N .

The two lattices of groups of order 8 above emphasize the fact that the isomorphism type of a group cannot in general be determined from the knowledge of the isomorphism types of G/N and N , since $Q_8/\langle -1 \rangle \cong D_8/\langle r^2 \rangle$ and $\langle -1 \rangle \cong \langle r^2 \rangle$ yet Q_8 and D_8 are not isomorphic. We shall discuss this question further in the next section.

We shall often indicate the index of one subgroup in another in the lattice of subgroups, as follows:

$$\begin{array}{c} A \\ | n \\ B \end{array}$$

where the integer n equals $|A : B|$. For example, all the unbroken edges in the lattices of Q_8 and D_8 would be labelled with 2. Thus the order of any subgroup, A , is the product of all integers which label any path upward from the identity to A . Also, by Theorem 20(2) these indices remain unchanged in quotients of G by normal subgroups of G contained in B , i.e., the portion of the lattice for G corresponding to the lattice of the quotient group has the correct indices for the quotient as well.

Finally we include a remark concerning the definition of homomorphisms on quotient groups. We have, in the course of the proof of the isomorphism theorems, encountered situations where a homomorphism φ on the quotient group G/N is specified by giving the value of φ on the coset gN in terms of the representative g alone. In each instance we then had to prove φ was well defined, i.e., was independent of the choice of g . In effect we are defining a homomorphism, Φ , on G itself by specifying the value of φ at g . Then independence of g is equivalent to requiring that Φ be trivial on N , so that

$$\varphi \text{ is well defined on } G/N \text{ if and only if } N \leq \ker \Phi.$$

This gives a simple criterion for defining homomorphisms on quotients (namely, define a homomorphism on G and check that N is contained in its kernel). In this situation we shall say the homomorphism Φ factors through N and φ is the *induced* homomorphism on G/N . This can be denoted pictorially as in Figure 7, where the diagram indicates that $\Phi = \varphi \circ \pi$, i.e., the image in H of an element in G does not depend on which path one takes in the diagram. If this is the case, then the diagram is said to *commute*.

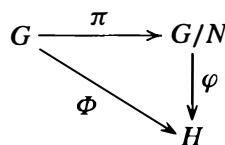


Fig. 7

At this point we have developed all the background material so that Section 6.3 on free groups and presentations may now be read.

EXERCISES

Let G be a group.

1. Let F be a finite field of order q and let $n \in \mathbb{Z}^+$. Prove that $|GL_n(F) : SL_n(F)| = q - 1$. [See Exercise 35, Section 1.]
2. Prove all parts of the Lattice Isomorphism Theorem.
3. Prove that if H is a normal subgroup of G of prime index p then for all $K \leq G$ either
 - (i) $K \leq H$ or
 - (ii) $G = HK$ and $|K : K \cap H| = p$.
4. Let C be a normal subgroup of the group A and let D be a normal subgroup of the group B . Prove that $(C \times D) \trianglelefteq (A \times B)$ and $(A \times B)/(C \times D) \cong (A/C) \times (B/D)$.
5. Let $QD_{16} = \langle \sigma, \tau \rangle$ be the quasidihedral group described in Exercise 11 of Section 2.5. Prove that $\langle \sigma^4 \rangle$ is normal in QD_{16} and use the Lattice Isomorphism Theorem to draw the lattice of subgroups of $QD_{16}/\langle \sigma^4 \rangle$. Which group of order 8 has the same lattice as this quotient? Use generators and relations for $QD_{16}/\langle \sigma^4 \rangle$ to decide the isomorphism type of this group.
6. Let $M = \langle v, u \rangle$ be the modular group of order 16 described in Exercise 14 of Section 2.5. Prove that $\langle v^4 \rangle$ is normal in M and use the Lattice Isomorphism Theorem to draw the lattice of subgroups of $M/\langle v^4 \rangle$. Which group of order 8 has the same lattice as this quotient? Use generators and relations for $M/\langle v^4 \rangle$ to decide the isomorphism type of this group.
7. Let M and N be normal subgroups of G such that $G = MN$. Prove that $G/(M \cap N) \cong (G/M) \times (G/N)$. [Draw the lattice.]
8. Let p be a prime and let G be the group of p -power roots of 1 in \mathbb{C} (cf. Exercise 18, Section 2.4). Prove that the map $z \mapsto z^p$ is a surjective homomorphism. Deduce that G is isomorphic to a proper quotient of itself.
9. Let p be a prime and let G be a group of order $p^a m$, where p does not divide m . Assume P is a subgroup of G of order p^a and N is a normal subgroup of G of order $p^b n$, where p does not divide n . Prove that $|P \cap N| = p^b$ and $|PN/N| = p^{a-b}$. (The subgroup P of G is called a *Sylow p-subgroup* of G . This exercise shows that the intersection of any Sylow p -subgroup of G with a normal subgroup N is a Sylow p -subgroup of N .)
10. Generalize the preceding exercise as follows. A subgroup H of a finite group G is called a *Hall subgroup* of G if its index in G is relatively prime to its order: $(|G : H|, |H|) = 1$. Prove that if H is a Hall subgroup of G and $N \trianglelefteq G$, then $H \cap N$ is a Hall subgroup of N and HN/N is a Hall subgroup of G/N .

3.4 COMPOSITION SERIES AND THE HÖLDER PROGRAM

The remarks in the preceding section on lattices leave us with the intuitive picture that a quotient group G/N is the group whose structure (e.g., lattice) describes the structure of G “above” the normal subgroup N . Although this is somewhat vague, it gives at least some notion of the driving force behind one of the most powerful techniques in finite group theory (and even some branches of infinite group theory): the use of induction. In many instances the application of an inductive procedure follows a pattern similar to the following proof of a special case of Cauchy’s Theorem. Although Cauchy’s Theorem is valid for arbitrary groups (cf. Exercise 9 of Section 2), the following is a good example

of the use of information on a normal subgroup N and on the quotient G/N to determine information about G , and we shall need this particular result in Chapter 4.

Proposition 21. If G is a finite abelian group and p is a prime dividing $|G|$, then G contains an element of order p .

Proof: The proof proceeds by induction on $|G|$, namely, we assume the result is valid for every group whose order is strictly smaller than the order of G and then prove the result valid for G (this is sometimes referred to as *complete* induction). Since $|G| > 1$, there is an element $x \in G$ with $x \neq 1$. If $|G| = p$ then x has order p by Lagrange's Theorem and we are done. We may therefore assume $|G| > p$.

Suppose p divides $|x|$ and write $|x| = pn$. By Proposition 2.5(3), $|x^n| = p$, and again we have an element of order p . We may therefore assume p does not divide $|x|$.

Let $N = \langle x \rangle$. Since G is abelian, $N \trianglelefteq G$. By Lagrange's Theorem, $|G/N| = \frac{|G|}{|N|}$

and since $N \neq 1$, $|G/N| < |G|$. Since p does not divide $|N|$, we must have $p \mid |G/N|$. We can now apply the induction assumption to the smaller group G/N to conclude it contains an element, $\bar{y} = yN$, of order p . Since $y \notin N$ ($\bar{y} \neq \bar{1}$) but $y^p \in N$ ($\bar{y}^p = \bar{1}$), we must have $(\bar{y}^p) \neq (\bar{y})$, that is, $|\bar{y}^p| < |\bar{y}|$. Proposition 2.5(2) implies $p \mid |\bar{y}|$. We are now in the situation described in the preceding paragraph, so that argument again produces an element of order p . The induction is complete.

The philosophy behind this method of proof is that if we have a sufficient amount of information about some normal subgroup, N , of a group G and sufficient information on G/N , then somehow we can piece this information together to force G itself to have some desired property. The induction comes into play because both N and G/N have smaller order than G . In general, just how much data are required is a delicate matter since, as we have already seen, the full isomorphism type of G cannot be determined from the isomorphism types of N and G/N alone.

Clearly a basic obstruction to this approach is the necessity of producing a normal subgroup, N , of G with $N \neq 1$ or G . In the preceding argument this was easy since G was abelian. Groups with no nontrivial proper normal subgroups are fundamental obstructions to this method of proof.

Definition. A (finite or infinite) group G is called *simple* if $|G| > 1$ and the only normal subgroups of G are 1 and G .

By Lagrange's Theorem if $|G|$ is a prime, its only subgroups (let alone normal ones) are 1 and G , so G is simple. In fact, every abelian simple group is isomorphic to Z_p , for some prime p (cf. Exercise 1). There are non-abelian simple groups (of both finite and infinite order), the smallest of which has order 60 (we shall introduce this group as a member of an infinite family of simple groups in the next section).

Simple groups, by definition, cannot be “factored” into pieces like N and G/N and as a result they play a role analogous to that of the primes in the arithmetic of \mathbb{Z} . This analogy is supported by a “unique factorization theorem” (for finite groups) which we now describe.

Definition. In a group G a sequence of subgroups

$$1 = N_0 \leq N_1 \leq N_2 \leq \cdots \leq N_{k-1} \leq N_k = G$$

is called a *composition series* if $N_i \trianglelefteq N_{i+1}$ and N_{i+1}/N_i a simple group, $0 \leq i \leq k-1$. If the above sequence is a composition series, the quotient groups N_{i+1}/N_i are called *composition factors* of G .

Keep in mind that it is not assumed that each $N_i \trianglelefteq G$, only that $N_i \trianglelefteq N_{i+1}$. Thus

$$1 \trianglelefteq (s) \trianglelefteq (s, r^2) \trianglelefteq D_8 \quad \text{and} \quad 1 \trianglelefteq (r^2) \trianglelefteq (r) \trianglelefteq D_8$$

are two composition series for D_8 and in each series there are 3 composition factors, each of which is isomorphic to (the simple group) Z_2 .

Theorem 22. (Jordan–Hölder) Let G be a finite group with $G \neq 1$. Then

(1) G has a composition series and

(2) The composition factors in a composition series are unique, namely, if $1 = N_0 \leq N_1 \leq \cdots \leq N_r = G$ and $1 = M_0 \leq M_1 \leq \cdots \leq M_s = G$ are two composition series for G , then $r = s$ and there is some permutation, π , of $\{1, 2, \dots, r\}$ such that

$$M_{\pi(i)}/M_{\pi(i)-1} \cong N_i/N_{i-1}, \quad 1 \leq i \leq r.$$

Proof: This is fairly straightforward. Since we shall not explicitly use this theorem to prove others in the text we outline the proof in a series of exercises at the end of this section.

Thus every finite group has a “factorization” (i.e., composition series) and although the series itself need not be unique (as D_8 shows) the number of composition factors and their isomorphism types are uniquely determined. Furthermore, nonisomorphic groups may have the same (up to isomorphism) list of composition factors (see Exercise 2). This motivates a two-part program for classifying all finite groups up to isomorphism:

The Hölder Program

(1) Classify all finite simple groups.

(2) Find all ways of “putting simple groups together” to form other groups.

These two problems form part of an underlying motivation for much of the development of group theory. Analogues of these problems may also be found as recurring themes throughout mathematics. We include a few more comments on the current status of progress on these problems.

The classification of finite simple groups (part (1) of the Hölder Program) was completed in 1980, about 100 years after the formulation of the Hölder Program. Efforts by over 100 mathematicians covering between 5,000 and 10,000 journal pages (spread over some 300 to 500 individual papers) have resulted in the proof of the following result:

Theorem. There is a list consisting of 18 (infinite) families of simple groups and 26 simple groups not belonging to these families (the *sporadic* simple groups) such that every finite simple group is isomorphic to one of the groups in this list.

One example of a family of simple groups is $\{Z_p \mid p \text{ a prime}\}$. A second infinite family in the list of finite simple groups is:

$$\{SL_n(\mathbb{F})/Z(SL_n(\mathbb{F})) \mid n \in \mathbb{Z}^+, n \geq 2 \text{ and } \mathbb{F} \text{ a finite field}\}.$$

These groups are all simple except for $SL_2(\mathbb{F}_2)$ and $SL_2(\mathbb{F}_3)$ where \mathbb{F}_2 is the finite field with 2 elements and \mathbb{F}_3 is the finite field with 3 elements. This is a 2-parameter family (n and \mathbb{F} being independent parameters). We shall not prove these groups are simple (although it is not technically beyond the scope of the text) but rather refer the reader to the book *Finite Group Theory* (by M. Aschbacher, Cambridge University Press, 1986) for proofs and an extensive discussion of the simple group problem. A third family of finite simple groups, the alternating groups, is discussed in the next section; we shall prove these groups are simple in the next chapter.

To gain some idea of the complexity of the classification of finite simple groups the reader may wish to peruse the proof of one of the cornerstones of the entire classification:

Theorem. (Feit–Thompson) If G is a simple group of odd order, then $G \cong Z_p$ for some prime p .

This proof takes 255 pages of hard mathematics.²

Part (2) of the Hölder Program, sometimes called the *extension problem*, was rather vaguely formulated. A more precise description of “putting two groups together” is: given groups A and B , describe how to obtain all groups G containing a normal subgroup N such that $N \cong B$ and $G/N \cong A$. For instance, if $A = B = Z_2$, there are precisely two possibilities for G , namely, Z_4 and V_4 (see Exercise 10 of Section 2.5) and the Hölder program seeks to describe how the two groups of order 4 could have been built from two Z_2 ’s without a priori knowledge of the existence of the groups of order 4. This part of the Hölder Program is extremely difficult, even when the subgroups involved are of small order. For example, all composition factors of a group G have order 2 if and only if $|G| = 2^n$, for some n (one implication is easy and we shall prove both implications in Chapter 6). It is known, however, that the number of nonisomorphic groups of order 2^n grows (exponentially) as a function of 2^n , so the number of ways of putting groups of 2-power order together is not bounded. Nonetheless, there are a wealth of interesting and powerful techniques in this subtle area which serve to unravel the structure of large classes of groups. We shall discuss only a couple of ways of building larger groups from smaller ones (in the sense above) but even from this limited excursion into the area of group extensions we shall construct numerous new examples of groups and prove some classification theorems.

One class of groups which figures prominently in the theory of polynomial equations is the class of *solvable* groups:

²Solvability of groups of odd order, Pacific Journal of Mathematics, 13(1963), pp. 775–1029.

Definition. A group G is *solvable* if there is a chain of subgroups

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \dots \trianglelefteq G_s = G$$

such that G_{i+1}/G_i is abelian for $i = 0, 1, \dots, s - 1$.

The terminology comes from the correspondence in Galois Theory between these groups and polynomials which can be solved by radicals (which essentially means there is an algebraic formula for the roots). Exercise 8 shows that finite solvable groups are precisely those groups whose composition factors are all of prime order.

One remarkable property of finite solvable groups is the following generalization of Sylow's Theorem due to Philip Hall (cf. Theorem 6.11 and Theorem 19.8).

Theorem. The finite group G is solvable if and only if for every divisor n of $|G|$ such that $(n, \frac{|G|}{n}) = 1$, G has a subgroup of order n .

As another illustration of how properties of a group G can be deduced from combined information from a normal subgroup N and the quotient group G/N we prove

if N and G/N are solvable, then G is solvable.

To see this let $\overline{G} = G/N$, let $1 = N_0 \trianglelefteq N_1 \trianglelefteq \dots \trianglelefteq N_n = N$ be a chain of subgroups of N such that N_{i+1}/N_i is abelian, $0 \leq i < n$ and let $\overline{1} = \overline{G}_0 \trianglelefteq \overline{G}_1 \trianglelefteq \dots \trianglelefteq \overline{G}_m = \overline{G}$ be a chain of subgroups of \overline{G} such that $\overline{G}_{i+1}/\overline{G}_i$ is abelian, $0 \leq i < m$. By the Lattice Isomorphism Theorem there are subgroups G_i of G with $N \leq G_i$ such that $G_i/N = \overline{G}_i$ and $G_i \trianglelefteq G_{i+1}$, $0 \leq i < m$. By the Third Isomorphism Theorem

$$\overline{G_{i+1}/G_i} = (G_{i+1}/N)/(G_i/N) \cong G_{i+1}/G_i.$$

Thus

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \dots \trianglelefteq N_n = N = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_m = G$$

is a chain of subgroups of G all of whose successive quotient groups are abelian. This proves G is solvable.

It is inaccurate to say that finite group theory is concerned *only* with the Hölder Program. It is accurate to say that the Hölder Program suggests a large number of problems and motivates a number of algebraic techniques. For example, in the study of the extension problem where we are given groups A and B and wish to find G and $N \trianglelefteq G$ with $N \cong B$ and $G/N \cong A$, we shall see that (under certain conditions) we are led to an *action* of the group A on the set B . Such actions form the crux of the next chapter (and will result in information both about simple and non-simple groups) and this notion is a powerful one in mathematics not restricted to the theory of groups.

The final section of this chapter introduces another family of groups and although in line with our interest in simple groups, it will be of independent importance throughout the text, particularly in our study later of determinants and the solvability of polynomial equations.

EXERCISES

1. Prove that if G is an abelian simple group then $G \cong \mathbb{Z}_p$ for some prime p (do not assume G is a finite group).
2. Exhibit all 3 composition series for Q_8 and all 7 composition series for D_8 . List the composition factors in each case.
3. Find a composition series for the quasidihedral group of order 16 (cf. Exercise 11, Section 2.5). Deduce that QD_{16} is solvable.
4. Use Cauchy's Theorem and induction to show that a finite abelian group has a subgroup of order n for each positive divisor n of its order.
5. Prove that subgroups and quotient groups of a solvable group are solvable.
6. Prove part (1) of the Jordan–Hölder Theorem by induction on $|G|$.
7. If G is a finite group and $H \trianglelefteq G$ prove that there is a composition series of G , one of whose terms is H .
8. Let G be a *finite* group. Prove that the following are equivalent:
 - (i) G is solvable
 - (ii) G has a chain of subgroups: $1 = H_0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \dots \trianglelefteq H_s = G$ such that H_{i+1}/H_i is cyclic, $0 \leq i \leq s - 1$
 - (iii) all composition factors of G are of prime order
 - (iv) G has a chain of subgroups: $1 = N_0 \trianglelefteq N_1 \trianglelefteq N_2 \trianglelefteq \dots \trianglelefteq N_t = G$ such that each N_i is a normal subgroup of G and N_{i+1}/N_i is abelian, $0 \leq i \leq t - 1$.

[For (iv), prove that a minimal nontrivial normal subgroup M of G is necessarily abelian and then use induction. To see that M is abelian, let $N \trianglelefteq M$ be of prime index (by (iii)) and show that $x^{-1}y^{-1}xy \in N$ for all $x, y \in M$ (cf. Exercise 40, Section 1). Apply the same argument to gNg^{-1} to show that $x^{-1}y^{-1}xy$ lies in the intersection of all G -conjugates of N , and use the minimality of M to conclude that $x^{-1}y^{-1}xy = 1$.]

9. Prove the following special case of part (2) of the Jordan–Hölder Theorem: assume the finite group G has two composition series

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \dots \trianglelefteq N_r = G \quad \text{and} \quad 1 = M_0 \trianglelefteq M_1 \trianglelefteq M_2 = G.$$

Show that $r = 2$ and that the list of composition factors is the same. [Use the Second Isomorphism Theorem.]

10. Prove part (2) of the Jordan–Hölder Theorem by induction on $\min\{r, s\}$. [Apply the inductive hypothesis to $H = N_{r-1} \cap M_{s-1}$ and use the preceding exercises.]
11. Prove that if H is a nontrivial normal subgroup of the solvable group G then there is a nontrivial subgroup A of H with $A \trianglelefteq G$ and A abelian.
12. Prove (without using the Feit–Thompson Theorem) that the following are equivalent:
 - (i) every group of odd order is solvable
 - (ii) the only simple groups of odd order are those of prime order.

3.5 TRANSPOSITIONS AND THE ALTERNATING GROUP

Transpositions and Generation of S_n

As we saw in Section 1.3 (and will prove in the next chapter) every element of S_n can be written as a product of disjoint cycles in an essentially unique fashion. In contrast,

every element of S_n can be written in many different ways as a (nondisjoint) product of cycles. For example, even in S_3 the element $\sigma = (1\ 2\ 3)$ may be written

$$\sigma = (1\ 2\ 3) = (1\ 3)(1\ 2) = (1\ 2)(1\ 3)(1\ 2)(1\ 3) = (1\ 2)(2\ 3)$$

and, in fact, there are an infinite number of different ways to write σ . Not requiring the cycles to be disjoint totally destroys the uniqueness of a representation of a permutation as a product of cycles. We can, however, obtain a sort of “parity check” from writing permutations (nonuniquely) as products of 2-cycles.

Definition. A 2-cycle is called a *transposition*.

Intuitively, every permutation of $\{1, 2, \dots, n\}$ can be realized by a succession of transpositions or simple interchanges of pairs of elements (try this on a small deck of cards sometime!). We illustrate how this may be done. First observe that

$$(a_1 a_2 \dots a_m) = (a_1 a_m)(a_1 a_{m-1})(a_1 a_{m-2}) \dots (a_1 a_2)$$

for any m -cycle. Now any permutation in S_n may be written as a product of cycles (for instance, its cycle decomposition). Writing each of these cycles in turn as a product of transpositions by the above procedure we see that

every element of S_n may be written as a product of transpositions

or, equivalently,

$$S_n = \langle T \rangle \quad \text{where} \quad T = \{(i\ j) \mid 1 \leq i < j \leq n\}.$$

For example, the permutation σ in Section 1.3 may be written

$$\begin{aligned} \sigma &= (1\ 1\ 2\ 8\ 10\ 4)(2\ 1\ 3)(5\ 1\ 1\ 7)(6\ 9) \\ &= (1\ 4)(1\ 10)(1\ 8)(1\ 12)(2\ 13)(5\ 7)(5\ 11)(6\ 9). \end{aligned}$$

The Alternating Group

Again we emphasize that for any $\sigma \in S_n$ there may be many ways of writing σ as a product of transpositions. For fixed σ we now show that the parity (i.e., an odd or even number of terms) is the same for any product of transpositions equaling σ .

Let x_1, \dots, x_n be independent variables and let Δ be the polynomial

$$\Delta = \prod_{1 \leq i < j \leq n} (x_i - x_j),$$

i.e., the product of all the terms $x_i - x_j$ for $i < j$. For example, when $n = 4$,

$$\Delta = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4).$$

For each $\sigma \in S_n$ let σ act on Δ by permuting the variables in the same way it permutes their indices:

$$\sigma(\Delta) = \prod_{1 \leq i < j \leq n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

For example, if $n = 4$ and $\sigma = (1\ 2\ 3\ 4)$ then

$$\sigma(\Delta) = (x_2 - x_3)(x_2 - x_4)(x_2 - x_1)(x_3 - x_4)(x_3 - x_1)(x_4 - x_1)$$

(we have written the factors in the same order as above and applied σ to each factor to get $\sigma(\Delta)$). Note (in general) that Δ contains one factor $x_i - x_j$ for all $i < j$, and since σ is a bijection of the indices, $\sigma(\Delta)$ must contain either $x_i - x_j$ or $x_j - x_i$, but not both (and certainly no $x_i - x_i$ terms), for all $i < j$. If $\sigma(\Delta)$ has a factor $x_j - x_i$ where $j > i$, write this term as $-(x_i - x_j)$. Collecting all the changes in sign together we see that Δ and $\sigma(\Delta)$ have the same factors up to a product of -1 's, i.e.,

$$\sigma(\Delta) = \pm \Delta, \quad \text{for all } \sigma \in S_n.$$

For each $\sigma \in S_n$ let

$$\epsilon(\sigma) = \begin{cases} +1, & \text{if } \sigma(\Delta) = \Delta \\ -1, & \text{if } \sigma(\Delta) = -\Delta. \end{cases}$$

In the example above with $n = 4$ and $\sigma = (1\ 2\ 3\ 4)$, there are exactly 3 factors of the form $x_j - x_i$ where $j > i$ in $\sigma(\Delta)$, each of which contributes a factor of -1 . Hence

$$(1\ 2\ 3\ 4)(\Delta) = (-1)^3(\Delta) = -\Delta,$$

so

$$\epsilon((1\ 2\ 3\ 4)) = -1.$$

Definition.

- (1) $\epsilon(\sigma)$ is called the *sign* of σ .
- (2) σ is called an *even permutation* if $\epsilon(\sigma) = 1$ and an *odd permutation* if $\epsilon(\sigma) = -1$

The next result shows that the sign of a permutation defines a homomorphism.

Proposition 23. The map $\epsilon : S_n \rightarrow \{\pm 1\}$ is a homomorphism (where $\{\pm 1\}$ is a multiplicative version of the cyclic group of order 2).

Proof: By definition,

$$(\tau\sigma)(\Delta) = \prod_{1 \leq i < j \leq n} (x_{\tau\sigma(i)} - x_{\tau\sigma(j)}).$$

Suppose that $\sigma(\Delta)$ has exactly k factors of the form $x_j - x_i$ with $j > i$, that is $\epsilon(\sigma) = (-1)^k$. When calculating $(\tau\sigma)(\Delta)$, after first applying σ to the indices we see that $(\tau\sigma)(\Delta)$ has exactly k factors of the form $x_{\tau(j)} - x_{\tau(i)}$ with $j > i$. Interchanging the order of the terms in these k factors introduces the sign change $(-1)^k = \epsilon(\sigma)$, and now all factors of $(\tau\sigma)(\Delta)$ are of the form $x_{\tau(p)} - x_{\tau(q)}$, with $p < q$. Thus

$$(\tau\sigma)(\Delta) = \epsilon(\sigma) \prod_{1 \leq p < q \leq n} (x_{\tau(p)} - x_{\tau(q)}).$$

Since by definition of ϵ

$$\prod_{1 \leq p < q \leq n} (x_{\tau(p)} - x_{\tau(q)}) = \epsilon(\tau)\Delta$$

we have $(\tau\sigma)(\Delta) = \epsilon(\sigma)\epsilon(\tau)\Delta$. Thus $\epsilon(\tau\sigma) = \epsilon(\sigma)\epsilon(\tau) = \epsilon(\tau)\epsilon(\sigma)$, as claimed.

To see the proof in action, let $n = 4$, $\sigma = (1\ 2\ 3\ 4)$, $\tau = (4\ 2\ 3)$ so $\tau\sigma = (1\ 3\ 2\ 4)$. By definition (using the explicit Δ in this case),

$$\begin{aligned} (\tau\sigma)(\Delta) &= (1\ 3\ 2\ 4)(\Delta) \\ &= (x_3 - x_4)(x_3 - x_2)(x_3 - x_1)(x_4 - x_2)(x_4 - x_1)(x_2 - x_1) \\ &= (-1)^5 \Delta \end{aligned}$$

where all factors except the first one are flipped to recover Δ . This shows $\epsilon(\tau\sigma) = -1$. On the other hand, since we already computed $\sigma(\Delta)$

$$\begin{aligned} (\tau\sigma)(\Delta) &= \tau(\sigma(\Delta)) \\ &= (x_{\tau(2)} - x_{\tau(3)})(x_{\tau(2)} - x_{\tau(4)})(x_{\tau(2)} - x_{\tau(1)})(x_{\tau(3)} - x_{\tau(4)}) \times \\ &\quad \times (x_{\tau(3)} - x_{\tau(1)})(x_{\tau(4)} - x_{\tau(1)}) \\ &= (-1)^3 \prod_{1 \leq p < q \leq 4} (x_{\tau(p)} - x_{\tau(q)}) = (-1)^3 \tau(\Delta) \end{aligned}$$

where here the third, fifth, and sixth factors need to have their terms interchanged in order to put all factors in the form $x_{\tau(p)} - x_{\tau(q)}$ with $p < q$. We already calculated that $\epsilon(\sigma) = (-1)^3 = -1$ and, by the same method, it is easy to see that $\epsilon(\tau) = (-1)^2 = 1$ so $\epsilon(\tau\sigma) = -1 = \epsilon(\tau)\epsilon(\sigma)$.

The next step is to compute $\epsilon((i\ j))$, for any transposition $(i\ j)$. Rather than compute this directly for arbitrary i and j we do it first for $i = 1$ and $j = 2$ and reduce the general case to this. It is clear that applying $(1\ 2)$ to Δ (regardless of what n is) will flip exactly one factor, namely $x_1 - x_2$; thus $\epsilon((1\ 2)) = -1$. Now for any transposition $(i\ j)$ let λ be the permutation which interchanges 1 and i , interchanges 2 and j , and leaves all other numbers fixed (if $i = 1$ or $j = 2$, λ fixes i or j , respectively). Then it is easy to see that $(i\ j) = \lambda(1\ 2)\lambda$ (compute what the right hand side does to any $k \in \{1, 2, \dots, n\}$). Since ϵ is a homomorphism we obtain

$$\begin{aligned} \epsilon((i\ j)) &= \epsilon(\lambda(1\ 2)\lambda) \\ &= \epsilon(\lambda)\epsilon((1\ 2))\epsilon(\lambda) \\ &= (-1)\epsilon(\lambda)^2 \\ &= -1. \end{aligned}$$

This proves

Proposition 24. Transpositions are all odd permutations and ϵ is a surjective homomorphism.

Definition. The *alternating group of degree n* , denoted by A_n , is the kernel of the homomorphism ϵ (i.e., the set of even permutations).

Note that by the First Isomorphism Theorem $S_n/A_n \cong \epsilon(S_n) = \{\pm 1\}$, so that the order of A_n is easily determined: $|A_n| = \frac{1}{2}|S_n| = \frac{1}{2}(n!)$. Also, $S_n - A_n$ is the coset of

A_n which is not the identity coset and this is the set of all odd permutations. The signs of permutations obey the usual $\mathbb{Z}/2\mathbb{Z}$ laws:

$$\begin{aligned}(even)(even) &= (odd)(odd) = even \\ (even)(odd) &= (odd)(even) = odd.\end{aligned}$$

Moreover, since ϵ is a homomorphism and every $\sigma \in S_n$ is a product of transpositions, say $\sigma = \tau_1 \tau_2 \cdots \tau_k$, then $\epsilon(\sigma) = \epsilon(\tau_1) \cdots \epsilon(\tau_k)$; since $\epsilon(\tau_i) = -1$, for $i = 1, 2, \dots, k$, $\epsilon(\sigma) = (-1)^k$. Thus the class of $k \pmod{2}$, i.e., the parity of the number of transpositions in the product, is the same no matter how we write σ as a product of transpositions:

$$\epsilon(\sigma) = \begin{cases} +1, & \text{if } \sigma \text{ is a product of an even number of transpositions} \\ -1, & \text{if } \sigma \text{ is a product of an odd number of transpositions.}\end{cases}$$

Finally we give a quick way of computing $\epsilon(\sigma)$ from the cycle decomposition of σ . Recall that an m -cycle may be written as a product of $m - 1$ transpositions. Thus

an m -cycle is an odd permutation if and only if m is even.

For any permutation σ let $\alpha_1 \alpha_2 \cdots \alpha_k$ be its cycle decomposition. Then $\epsilon(\sigma)$ is given by $\epsilon(\alpha_1) \cdots \epsilon(\alpha_k)$ and $\epsilon(\alpha_i) = -1$ if and only if the length of α_i is even. It follows that for $\epsilon(\sigma)$ to be -1 the product of the $\epsilon(\alpha_i)$'s must contain an odd number of factors of (-1) . We summarize this in the following proposition:

Proposition 25. The permutation σ is odd if and only if the number of cycles of even length in its cycle decomposition is odd.

For example, $\sigma = (1\ 2\ 3\ 4\ 5\ 6)(7\ 8\ 9)(10\ 11)(12\ 13\ 14\ 15)(16\ 17\ 18)$ has 3 cycles of even length, so $\epsilon(\sigma) = -1$. On the other hand, $\tau = (1\ 12\ 8\ 10\ 4)(2\ 13)(5\ 11\ 7)(6\ 9)$ has exactly 2 cycles of even length, hence $\epsilon(\tau) = 1$.

Be careful not to confuse the terms “odd” and “even” for a permutation σ with the parity of the order of σ . In fact, if σ is of odd order, all cycles in the cycle decomposition of σ have odd length so σ has an even (in this case 0) number of cycles of even length and hence is an even permutation. If $|\sigma|$ is even, σ may be either an even or an odd permutation; e.g., $(1\ 2)$ is odd, $(1\ 2)(3\ 4)$ is even but both have order 2.

As we mentioned in the preceding section, the alternating groups A_n will be important in the study of solvability of polynomials. In the next chapter we shall prove:

A_n is a non-abelian simple group for all $n \geq 5$.

For small values of n , A_n is already familiar to us: A_1 and A_2 are both the trivial group and $|A_3| = 3$ (so $A_3 = \langle (1\ 2\ 3) \rangle \cong \mathbb{Z}_3$). The group A_4 has order 12. Exercise 7 shows A_4 is isomorphic to the group of symmetries of a regular tetrahedron. The lattice of subgroups of A_4 appears in Figure 8 (Exercise 8 asserts that this is its complete lattice of subgroups). One of the nicer aspects of this lattice is that (unlike “virtually all groups”) it is a planar graph (there are no crossing lines except at the vertices; see the lattice of D_{16} for a nonplanar lattice).

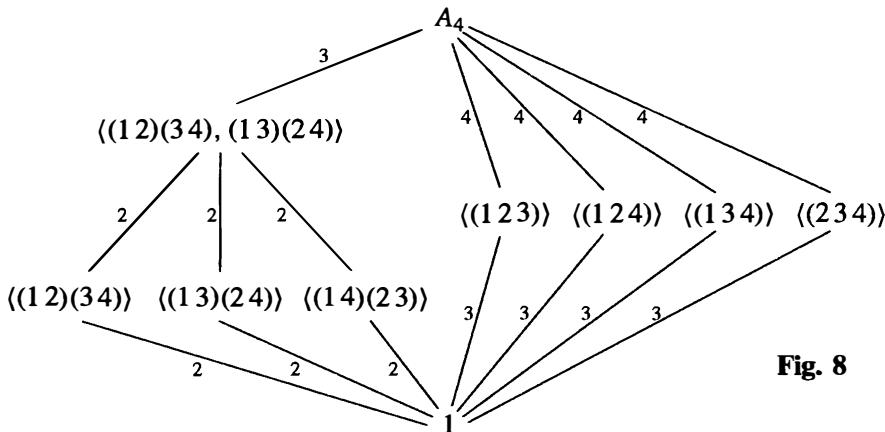


Fig. 8

EXERCISES

1. In Exercises 1 and 2 of Section 1.3 you were asked to find the cycle decomposition of some permutations. Write each of these permutations as a product of transpositions. Determine which of these is an even permutation and which is an odd permutation.
2. Prove that σ^2 is an even permutation for every permutation σ .
3. Prove that S_n is generated by $\{(i \ i+1) \mid 1 \leq i \leq n-1\}$. [Consider conjugates, viz. $(2 \ 3)(1 \ 2)(2 \ 3)^{-1}$.]
4. Show that $S_n = \langle (1 \ 2), (1 \ 2 \ 3 \dots \ n) \rangle$ for all $n \geq 2$.
5. Show that if p is prime, $S_p = \langle \sigma, \tau \rangle$ where σ is any transposition and τ is any p -cycle.
6. Show that $\langle (1 \ 3), (1 \ 2 \ 3 \ 4) \rangle$ is a proper subgroup of S_4 . What is the isomorphism type of this subgroup?
7. Prove that the group of rigid motions of a tetrahedron is isomorphic to A_4 . [Recall Exercise 20 in Section 1.7.]
8. Prove the lattice of subgroups of A_4 given in the text is correct. [By the preceding exercise and the comments following Lagrange's Theorem, A_4 has no subgroup of order 6.]
9. Prove that the (unique) subgroup of order 4 in A_4 is normal and is isomorphic to V_4 .
10. Find a composition series for A_4 . Deduce that A_4 is solvable.
11. Prove that S_4 has no subgroup isomorphic to Q_8 .
12. Prove that A_n contains a subgroup isomorphic to S_{n-2} for each $n \geq 3$.
13. Prove that every element of order 2 in A_n is the square of an element of order 4 in S_n . [An element of order 2 in A_n is a product of $2k$ commuting transpositions.]
14. Prove that the subgroup of A_4 generated by any element of order 2 and any element of order 3 is all of A_4 .
15. Prove that if x and y are distinct 3-cycles in S_4 with $x \neq y^{-1}$, then the subgroup of S_4 generated by x and y is A_4 .
16. Let x and y be distinct 3-cycles in S_5 with $x \neq y^{-1}$.
 - (a) Prove that if x and y fix a common element of $\{1, \dots, 5\}$, then $\langle x, y \rangle \cong A_4$.
 - (b) Prove that if x and y do not fix a common element of $\{1, \dots, 5\}$, then $\langle x, y \rangle = A_5$.
17. If x and y are 3-cycles in S_n , prove that $\langle x, y \rangle$ is isomorphic to Z_3 , A_4 , A_5 or $Z_3 \times Z_3$.

CHAPTER 4

Group Actions

In this chapter we consider some of the consequences of a group acting on a set. It is an important and recurring idea in mathematics that when one object acts on another then much information can be obtained on both. As more structure is added to the set on which the group acts (for example, groups acting on groups or groups acting on vector spaces (considered in Chapter 18)), more information on the structure of the group becomes available. This study of group actions culminates here in the proof of Sylow's Theorem and the examples and classifications which accrue from it.

The concept of an action will recur as we study modules, vector spaces, canonical forms for matrices and Galois Theory, and is one of the fundamental unifying themes in the text.

4.1 GROUP ACTIONS AND PERMUTATION REPRESENTATIONS

In this section we give the basic theory of group actions and then apply this theory to subgroups of S_n acting on $\{1, 2, \dots, n\}$ to prove that every element of S_n has a unique cycle decomposition. In Sections 2 and 3 we apply the general theory to two other specific group actions to derive some important results.

Let G be a group acting on a nonempty set A . Recall from Section 1.7 that for each $g \in G$ the map

$$\sigma_g : A \rightarrow A \quad \text{defined by} \quad \sigma_g : a \mapsto g \cdot a$$

is a permutation of A . We also saw in Section 1.7 that there is a homomorphism associated to an action of G on A :

$$\varphi : G \rightarrow S_A \quad \text{defined by} \quad \varphi(g) = \sigma_g,$$

called the *permutation representation* associated to the given action. Recall some additional terminology associated to group actions introduced in Sections 1.7 and 2.2.

Definition.

- (1) The *kernel* of the action is the set of elements of G that act trivially on every element of A : $\{g \in G \mid g \cdot a = a \text{ for all } a \in A\}$.
- (2) For each $a \in A$ the *stabilizer* of a in G is the set of elements of G that fix the element a : $\{g \in G \mid g \cdot a = a\}$ and is denoted by G_a .
- (3) An action is *faithful* if its kernel is the identity.

Note that the kernel of an action is precisely the same as the kernel of the associated permutation representation; in particular, the kernel is a normal subgroup of G . Two group elements induce the same permutation on A if and only if they are in the same coset of the kernel (if and only if they are in the same fiber of the permutation representation φ). In particular an action of G on A may also be viewed as a faithful action of the quotient group $G/\ker\varphi$ on A . Recall from Section 2.2 that the stabilizer in G of an element a of A is a subgroup of G . If a is a fixed element of A , then the kernel of the action is contained in the stabilizer G_a since the kernel of the action is the set of elements of G that stabilize every point, namely $\cap_{a \in A} G_a$.

Examples

- (1) Let n be a positive integer. The group $G = S_n$ acts on the set $A = \{1, 2, \dots, n\}$ by $\sigma \cdot i = \sigma(i)$ for all $i \in \{1, \dots, n\}$. The permutation representation associated to this action is the identity map $\varphi : S_n \rightarrow S_n$. This action is faithful and for each $i \in \{1, \dots, n\}$ the stabilizer G_i (the subgroup of all permutations fixing i) is isomorphic to S_{n-1} (cf. Exercise 15, Section 3.2).
- (2) Let $G = D_8$ act on the set A consisting of the four vertices of a square. Label these vertices 1, 2, 3, 4 in a clockwise fashion as in Figure 2 of Section 1.2. Let r be the rotation of the square clockwise by $\pi/2$ radians and let s be the reflection in the line which passes through vertices 1 and 3. Then the permutations of the vertices given by r and s are

$$\sigma_r = (1 \ 2 \ 3 \ 4) \quad \text{and} \quad \sigma_s = (2 \ 4).$$

Note that since the permutation representation is a homomorphism, the permutation of the four vertices corresponding to sr is $\sigma_{sr} = \sigma_s \sigma_r = (1 \ 4)(2 \ 3)$. The action of D_8 on the four vertices of a square is faithful since only the identity symmetry fixes all four vertices. The stabilizer of any vertex a is the subgroup of D_8 of order 2 generated by the reflection about the line passing through a and the center of the square (so, for example, the stabilizer of vertex 1 is $\langle s \rangle$).

- (3) Label the four vertices of a square as in the preceding example and now let A be the set whose elements consist of unordered pairs of opposite vertices: $A = \{ \{1, 3\}, \{2, 4\} \}$. Then D_8 also acts on this set A since each symmetry of the square sends a pair of opposite vertices to a pair of opposite vertices. The rotation r interchanges the pairs $\{1, 3\}$ and $\{2, 4\}$; the reflection s fixes both unordered pairs of opposite vertices. Thus if we label the pairs $\{1, 3\}$ and $\{2, 4\}$ as **1** and **2**, respectively, then the permutations of A given by r and s are

$$\sigma_r = (\mathbf{1} \ \mathbf{2}) \quad \text{and} \quad \sigma_s = \text{the identity permutation.}$$

This action of D_8 is not faithful: its kernel is $\langle s, r^2 \rangle$. Moreover, for each $a \in A$ the stabilizer in D_8 of a is the same as the kernel of the action.

- (4) Label the four vertices of a square as in Example 2 and now let A be the following set of unordered pairs of vertices: $\{ \{1, 2\}, \{3, 4\} \}$. The group D_8 does *not* act on this set A because $\{1, 2\} \in A$ but $r \cdot \{1, 2\} = \{2, 3\} \notin A$.

The relation between actions and homomorphisms into symmetric groups may be reversed. Namely, given any nonempty set A and any homomorphism φ of the group G into S_A we obtain an action of G on A by defining

$$g \cdot a = \varphi(g)(a)$$

for all $g \in G$ and all $a \in A$. The kernel of this action is the same as $\ker \varphi$. The permutation representation associated to this action is precisely the given homomorphism φ . This proves the following result.

Proposition 1. For any group G and any nonempty set A there is a bijection between the actions of G on A and the homomorphisms of G into S_A .

In view of Proposition 1 the definition of a permutation representation may be rephrased.

Definition. If G is a group, a *permutation representation* of G is any homomorphism of G into the symmetric group S_A for some nonempty set A . We shall say a given action of G on A *affords* or *induces* the associated permutation representation of G .

We can think of a permutation representation as an analogue of the matrix representation of a linear transformation. In the case where A is a finite set of n elements we have $S_A \cong S_n$ (cf. Section 1.6), so by fixing a labelling of the elements of A we may consider our permutations as elements of the group S_n (which is exactly what we did in Examples 2 and 3 above), in the same way that fixing a basis for a vector space allows us to view a linear transformation as a matrix.

We now prove a combinatorial result about group actions which will have important consequences when we apply it to specific actions in subsequent sections.

Proposition 2. Let G be a group acting on the nonempty set A . The relation on A defined by

$$a \sim b \quad \text{if and only if} \quad a = g \cdot b \text{ for some } g \in G$$

is an equivalence relation. For each $a \in A$, the number of elements in the equivalence class containing a is $|G : G_a|$, the index of the stabilizer of a .

Proof: We first prove \sim is an equivalence relation. By axiom 2 of an action, $a = 1 \cdot a$ for all $a \in A$, i.e., $a \sim a$ and the relation is reflexive. If $a \sim b$, then $a = g \cdot b$ for some $b \in G$ so that

$$g^{-1} \cdot a = g^{-1} \cdot (g \cdot b) = (g^{-1}g) \cdot b = 1 \cdot b = b$$

that is, $b \sim a$ and the relation is symmetric. Finally, if $a \sim b$ and $b \sim c$, then $a = g \cdot b$ and $b = h \cdot c$, for some $g, h \in G$ so

$$a = g \cdot b = g \cdot (h \cdot c) = (gh) \cdot c$$

hence $a \sim c$, and the relation is transitive.

To prove the last statement of the proposition we exhibit a bijection between the left cosets of G_a in G and the elements of the equivalence class of a . Let \mathcal{C}_a be the class of a , so

$$\mathcal{C}_a = \{g \cdot a \mid g \in G\}.$$

Suppose $b = g \cdot a \in \mathcal{C}_a$. Then gG_a is a left coset of G_a in G . The map

$$b = g \cdot a \mapsto gG_a$$

is a map from \mathcal{C}_a to the set of left cosets of G_a in G . This map is surjective since for any $g \in G$ the element $g \cdot a$ is an element of \mathcal{C}_a . Since $g \cdot a = h \cdot a$ if and only if $h^{-1}g \in G_a$ if and only if $gG_a = hG_a$, the map is also injective, hence is a bijection. This completes the proof.

By Proposition 2 a group G acting on the set A partitions A into disjoint equivalence classes under the action of G . These classes are given a name:

Definition. Let G be a group acting on the nonempty set A .

- (1) The equivalence class $\{g \cdot a \mid g \in G\}$ is called the *orbit* of G containing a .
- (2) The action of G on A is called *transitive* if there is only one orbit, i.e., given any two elements $a, b \in A$ there is some $g \in G$ such that $a = g \cdot b$.

Examples

Let G be a group acting on the set A .

- (1) If G acts trivially on A then $G_a = G$ for all $a \in A$ and the orbits are the elements of A . This action is transitive if and only if $|A| = 1$.
- (2) The symmetric group $G = S_n$ acts transitively in its usual action as permutations on $A = \{1, 2, \dots, n\}$. Note that the stabilizer in G of any point i has index $n = |A|$ in S_n .
- (3) When the group G acts on the set A , any subgroup of G also acts on A . If G is transitive on A a subgroup of G need not be transitive on A . For example, if $G = \langle (1 2), (3 4) \rangle \leq S_4$ then the orbits of G on $\{1, 2, 3, 4\}$ are $\{1, 2\}$ and $\{3, 4\}$ and there is no element of G that sends 2 to 3. The discussion below on cycle decompositions shows that when $\langle \sigma \rangle$ is any cyclic subgroup of S_n then the orbits of $\langle \sigma \rangle$ consist of the sets of numbers that appear in the individual cycles in the cycle decomposition of σ (for example, the orbits of $\langle (1 2)(3 4 5) \rangle$ are $\{1, 2\}$ and $\{3, 4, 5\}$).
- (4) The group D_8 acts transitively on the four vertices of the square and the stabilizer of any vertex is the subgroup of order 2 (and index 4) generated by the reflection about the line of symmetry passing through that point.
- (5) The group D_8 also acts transitively on the set of two pairs of opposite vertices. In this action the stabilizer of any point is $\langle s, r^2 \rangle$ (which is of index 2).

Cycle Decompositions

We now prove that every element of the symmetric group S_n has the unique cycle decomposition described in Section 1.3. Let $A = \{1, 2, \dots, n\}$, let σ be an element of S_n and let $G = \langle \sigma \rangle$. Then $\langle \sigma \rangle$ acts on A and so, by Proposition 2, it partitions $\{1, 2, \dots, n\}$ into a unique set of (disjoint) orbits. Let \mathcal{O} be one of these orbits and let $x \in \mathcal{O}$. By (the proof of) Proposition 2 applied to $A = \mathcal{O}$ we see that there is a bijection between the left cosets of G_x in G and the elements of \mathcal{O} , given explicitly by

$$\sigma^i x \mapsto \sigma^i G_x.$$

Since G is a cyclic group, $G_x \trianglelefteq G$ and G/G_x is cyclic of order d , where d is the smallest positive integer for which $\sigma^d \in G_x$ (cf. Example 2 following Proposition 7 in Section 3.1). Also, $d = |G : G_x| = |\mathcal{O}|$. Thus the distinct cosets of G_x in G are

$$1G_x, \sigma G_x, \sigma^2 G_x, \dots, \sigma^{d-1} G_x.$$

This shows that the distinct elements of \mathcal{O} are

$$x, \sigma(x), \sigma^2(x), \dots, \sigma^{d-1}(x).$$

Ordering the elements of \mathcal{O} in this manner shows that σ cycles the elements of \mathcal{O} , that is, on an orbit of size d , σ acts as a d -cycle. This proves the existence of a cycle decomposition for each $\sigma \in S_n$.

The orbits of $\langle \sigma \rangle$ are uniquely determined by σ . The only latitude is in which order the orbits are listed. Within each orbit, \mathcal{O} , we may begin with any element as a representative. Choosing $\sigma^i(x)$ instead of x as the initial representative simply produces the elements of \mathcal{O} in the order

$$\sigma^i(x), \sigma^{i+1}(x), \dots, \sigma^{d-1}(x), x, \sigma(x), \dots, \sigma^{i-1}(x),$$

which is a cyclic permutation (forward $i - 1$ terms) of the original list. It follows that the cycle decomposition above is unique up to a rearrangement of the cycles and up to a cyclic permutation of the integers within each cycle.

Subgroups of symmetric groups are called *permutation groups*. For any subgroup G of S_n the orbits of G will refer to its orbits on $\{1, 2, \dots, n\}$. The orbits of an element σ in S_n will mean the orbits of the group $\langle \sigma \rangle$ (namely the sets of integers comprising the cycles in its cycle decomposition).

The exercises below further illustrate how group theoretic information can be obtained from permutation representations.

EXERCISES

Let G be a group and let A be a nonempty set.

1. Let G act on the set A . Prove that if $a, b \in A$ and $b = g \cdot a$ for some $g \in G$, then $G_b = gG_ag^{-1}$ (G_a is the stabilizer of a). Deduce that if G acts transitively on A then the kernel of the action is $\bigcap_{g \in G} gG_ag^{-1}$.
2. Let G be a *permutation group* on the set A (i.e., $G \leq S_A$), let $\sigma \in G$ and let $a \in A$. Prove that $\sigma G_a \sigma^{-1} = G_{\sigma(a)}$. Deduce that if G acts transitively on A then

$$\bigcap_{\sigma \in G} \sigma G_a \sigma^{-1} = 1.$$

3. Assume that G is an abelian, transitive subgroup of S_A . Show that $\sigma(a) \neq a$ for all $\sigma \in G - \{1\}$ and all $a \in A$. Deduce that $|G| = |A|$. [Use the preceding exercise.]
4. Let S_3 act on the set Ω of ordered pairs: $\{(i, j) \mid 1 \leq i, j \leq 3\}$ by $\sigma((i, j)) = (\sigma(i), \sigma(j))$. Find the orbits of S_3 on Ω . For each $\sigma \in S_3$ find the cycle decomposition of σ under this action (i.e., find its cycle decomposition when σ is considered as an element of S_9 — first fix a labelling of these nine ordered pairs). For each orbit \mathcal{O} of S_3 acting on these nine points pick some $a \in \mathcal{O}$ and find the stabilizer of a in S_3 .
5. For each of parts (a) and (b) repeat the preceding exercise but with S_3 acting on the specified set:
 - (a) the set of 27 triples $\{(i, j, k) \mid 1 \leq i, j, k \leq 3\}$
 - (b) the set $\mathcal{P}(\{1, 2, 3\}) - \{\emptyset\}$ of all 7 nonempty subsets of $\{1, 2, 3\}$.
6. As in Exercise 12 of Section 2.2 let R be the set of all polynomials with integer coefficients in the independent variables x_1, x_2, x_3, x_4 and let S_4 act on R by permuting the indices of

the four variables:

$$\sigma \cdot p(x_1, x_2, x_3, x_4) = p(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}, x_{\sigma(4)})$$

for all $\sigma \in S_4$.

- (a) Find the polynomials in the orbit of S_4 on R containing $x_1 + x_2$ (recall from Exercise 12 in Section 2.2 that the stabilizer of this polynomial has order 4).
 - (b) Find the polynomials in the orbit of S_4 on R containing $x_1x_2 + x_3x_4$ (recall from Exercise 12 in Section 2.2 that the stabilizer of this polynomial has order 8).
 - (c) Find the polynomials in the orbit of S_4 on R containing $(x_1 + x_2)(x_3 + x_4)$.
7. Let G be a transitive permutation group on the finite set A . A *block* is a nonempty subset B of A such that for all $\sigma \in G$ either $\sigma(B) = B$ or $\sigma(B) \cap B = \emptyset$ (here $\sigma(B)$ is the set $\{\sigma(b) \mid b \in B\}$).
- (a) Prove that if B is a block containing the element a of A , then the set G_B defined by $G_B = \{\sigma \in G \mid \sigma(B) = B\}$ is a subgroup of G containing G_a .
 - (b) Show that if B is a block and $\sigma_1(B), \sigma_2(B), \dots, \sigma_n(B)$ are all the distinct images of B under the elements of G , then these form a partition of A .
 - (c) A (transitive) group G on a set A is said to be *primitive* if the only blocks in A are the trivial ones: the sets of size 1 and A itself. Show that S_4 is primitive on $A = \{1, 2, 3, 4\}$. Show that D_8 is not primitive as a permutation group on the four vertices of a square.
 - (d) Prove that the transitive group G is primitive on A if and only if for each $a \in A$, the only subgroups of G containing G_a are G_a and G (i.e., G_a is a *maximal* subgroup of G , cf. Exercise 16, Section 2.4). [Use part (a).]
8. A transitive permutation group G on a set A is called *doubly transitive* if for any (hence all) $a \in A$ the subgroup G_a is transitive on the set $A - \{a\}$.
- (a) Prove that S_n is doubly transitive on $\{1, 2, \dots, n\}$ for all $n \geq 2$.
 - (b) Prove that a doubly transitive group is primitive. Deduce that D_8 is not doubly transitive in its action on the 4 vertices of a square.
9. Assume G acts transitively on the finite set A and let H be a normal subgroup of G . Let $\mathcal{O}_1, \mathcal{O}_2, \dots, \mathcal{O}_r$ be the distinct orbits of H on A .
- (a) Prove that G permutes the sets $\mathcal{O}_1, \mathcal{O}_2, \dots, \mathcal{O}_r$ in the sense that for each $g \in G$ and each $i \in \{1, \dots, r\}$ there is a j such that $g\mathcal{O}_i = \mathcal{O}_j$, where $g\mathcal{O} = \{g \cdot a \mid a \in \mathcal{O}\}$ (i.e., in the notation of Exercise 7 the sets $\mathcal{O}_1, \dots, \mathcal{O}_r$ are blocks). Prove that G is transitive on $\{\mathcal{O}_1, \dots, \mathcal{O}_r\}$. Deduce that all orbits of H on A have the same cardinality.
 - (b) Prove that if $a \in \mathcal{O}_1$ then $|\mathcal{O}_1| = |H : H \cap G_a|$ and prove that $r = |G : HG_a|$. [Draw the sublattice describing the Second Isomorphism Theorem for the subgroups H and G_a of G . Note that $H \cap G_a = H_a$.]
10. Let H and K be subgroups of the group G . For each $x \in G$ define the *HK double coset* of x in G to be the set
- $$HxK = \{hxk \mid h \in H, k \in K\}.$$
- (a) Prove that HxK is the union of the left cosets x_1K, \dots, x_nK where $\{x_1K, \dots, x_nK\}$ is the orbit containing xK of H acting by left multiplication on the set of left cosets of K .
 - (b) Prove that HxK is a union of right cosets of H .
 - (c) Show that HxK and HyK are either the same set or are disjoint for all $x, y \in G$. Show that the set of HK double cosets partitions G .
 - (d) Prove that $|HxK| = |K| \cdot |H : H \cap xKx^{-1}|$.
 - (e) Prove that $|HxK| = |H| \cdot |K : K \cap x^{-1}Hx|$.

4.2 GROUPS ACTING ON THEMSELVES BY LEFT MULTIPLICATION — CAYLEY'S THEOREM

In this section G is any group and we first consider G *acting on itself* (i.e., $A = G$) by *left multiplication*:

$$g \cdot a = ga \quad \text{for all } g \in G, a \in G$$

where ga denotes the product of the two group elements g and a in G (if G is written additively, the action will be written $g \cdot a = g + a$ and called left translation). We saw in Section 1.7 that this satisfies the two axioms of a group action.

When G is a finite group of order n it is convenient to label the elements of G with the integers $1, 2, \dots, n$ in order to describe the permutation representation afforded by this action. In this way the elements of G are listed as g_1, g_2, \dots, g_n and for each $g \in G$ the permutation σ_g may be described as a permutation of the indices $1, 2, \dots, n$ as follows:

$$\sigma_g(i) = j \quad \text{if and only if} \quad gg_i = g_j.$$

A different labelling of the group elements will give a different description of σ_g as a permutation of $\{1, 2, \dots, n\}$ (cf. the exercises).

Example

Let $G = \{1, a, b, c\}$ be the Klein 4-group whose group table is written out in Section 2.5. Label the group elements $1, a, b, c$ with the integers $1, 2, 3, 4$, respectively. Under this labelling we compute the permutation σ_a induced by the action of left multiplication by the group element a :

$$\begin{aligned} a \cdot 1 &= a1 = a \text{ and so } \sigma_a(1) = 2 \\ a \cdot a &= aa = 1 \text{ and so } \sigma_a(2) = 1 \\ a \cdot b &= ab = c \text{ and so } \sigma_a(3) = 4 \text{ and} \\ a \cdot c &= ac = b \text{ and so } \sigma_a(4) = 3. \end{aligned}$$

With this labelling of the elements of G we see that $\sigma_a = (1 \ 2)(3 \ 4)$. In the permutation representation associated to the action of the Klein 4-group on itself by left multiplication one similarly computes that

$$a \mapsto \sigma_a = (1 \ 2)(3 \ 4) \quad b \mapsto \sigma_b = (1 \ 3)(2 \ 4) \quad c \mapsto \sigma_c = (1 \ 4)(2 \ 3),$$

which explicitly gives the permutation representation $G \rightarrow S_4$ associated to this action under this labelling.

It is easy to see (and we shall prove this shortly in a more general setting) that the action of a group on itself by left multiplication is always transitive and faithful, and that the stabilizer of any point is the identity subgroup (these facts can be checked by inspection for the above example).

We now consider a generalization of the action of a group by left multiplication on the set of its elements. Let H be any subgroup of G and let A be the set of all left cosets of H in G . Define an action of G on A by

$$g \cdot aH = gaH \quad \text{for all } g \in G, aH \in A$$

where gaH is the left coset with representative ga . One easily checks that this satisfies the two axioms for a group action, i.e., that G does act on the set of left cosets of H .

by left multiplication. In the special case when H is the identity subgroup of G the coset aH is just $\{a\}$ and if we identify the element a with the set $\{a\}$, this action by left multiplication on left cosets of the identity subgroup is the same as the action of G on itself by left multiplication.

When H is of finite index m in G it is convenient to label the left cosets of H with the integers $1, 2, \dots, m$ in order to describe the permutation representation afforded by this action. In this way the distinct left cosets of H in G are listed as a_1H, a_2H, \dots, a_mH and for each $g \in G$ the permutation σ_g may be described as a permutation of the indices $1, 2, \dots, m$ as follows:

$$\sigma_g(i) = j \quad \text{if and only if} \quad ga_iH = a_jH.$$

A different labelling of the group elements will give a different description of σ_g as a permutation of $\{1, 2, \dots, m\}$ (cf. the exercises).

Example

Let $G = D_8$ and let $H = \langle s \rangle$. Label the distinct left cosets $1H, rH, r^2H, r^3H$ with the integers $1, 2, 3, 4$ respectively. Under this labelling we compute the permutation σ_s induced by the action of left multiplication by the group element s on the left cosets of H :

$$\begin{aligned}s \cdot 1H &= sH = 1H \text{ and so } \sigma_s(1) = 1 \\ s \cdot rH &= srH = r^3H \text{ and so } \sigma_s(2) = 4 \\ s \cdot r^2H &= sr^2H = r^2H \text{ and so } \sigma_s(3) = 3 \\ s \cdot r^3H &= sr^3H = rH \text{ and so } \sigma_s(4) = 2.\end{aligned}$$

With this labelling of the left cosets of H we obtain $\sigma_s = (2 \ 4)$. In the permutation representation associated to the action of D_8 on the left cosets of $\langle s \rangle$ by left multiplication one similarly computes that $\sigma_r = (1 \ 2 \ 3 \ 4)$. Note that the permutation representation is a homomorphism, so once its value has been determined on generators for D_8 its value on any other element can be determined (e.g., $\sigma_{sr^2} = \sigma_s\sigma_r^2$).

Theorem 3. Let G be a group, let H be a subgroup of G and let G act by left multiplication on the set A of left cosets of H in G . Let π_H be the associated permutation representation afforded by this action. Then

- (1) G acts transitively on A
- (2) the stabilizer in G of the point $1H \in A$ is the subgroup H
- (3) the kernel of the action (i.e., the kernel of π_H) is $\bigcap_{x \in G} xHx^{-1}$, and $\ker \pi_H$ is the largest normal subgroup of G contained in H .

Proof: To see that G acts transitively on A , let aH and bH be any two elements of A , and let $g = ba^{-1}$. Then $g \cdot aH = (ba^{-1})aH = bH$, and so the two arbitrary elements aH and bH of A lie in the same orbit, which proves (1). For (2), the stabilizer of the point $1H$ is, by definition, $\{g \in G \mid g \cdot 1H = 1H\}$, i.e., $\{g \in G \mid gH = H\} = H$.

By definition of π_H we have

$$\begin{aligned}\ker \pi_H &= \{g \in G \mid gxH = xH \text{ for all } x \in G\} \\ &= \{g \in G \mid (x^{-1}gx)H = H \text{ for all } x \in G\} \\ &= \{g \in G \mid x^{-1}gx \in H \text{ for all } x \in G\} \\ &= \{g \in G \mid g \in xHx^{-1} \text{ for all } x \in G\} = \bigcap_{x \in G} xHx^{-1},\end{aligned}$$

which proves the first assertion of (3). The second assertion of (3) comes from observing first that $\ker \pi_H \trianglelefteq G$ and $\ker \pi_H \leq H$. If now N is any normal subgroup of G contained in H then we have $N = xN x^{-1} \leq xHx^{-1}$ for all $x \in G$ so that

$$N \leq \bigcap_{x \in G} xHx^{-1} = \ker \pi_H.$$

This shows that $\ker \pi_H$ is the largest normal subgroup of G contained in H .

Corollary 4. (*Cayley's Theorem*) Every group is isomorphic to a subgroup of some symmetric group. If G is a group of order n , then G is isomorphic to a subgroup of S_n .

Proof: Let $H = 1$ and apply the preceding theorem to obtain a homomorphism of G into S_G (here we are identifying the cosets of the identity subgroup with the elements of G). Since the kernel of this homomorphism is contained in $H = 1$, G is isomorphic to its image in S_G .

Note that G is isomorphic to a *subgroup* of a symmetric group, not to the full symmetric group itself. For example, we exhibited an isomorphism of the Klein 4-group with the subgroup $\langle (1\ 2)(3\ 4), (1\ 3)(2\ 4) \rangle$ of S_4 . Recall that subgroups of symmetric groups are called *permutation groups* so Cayley's Theorem states that every group is isomorphic to a permutation group. The permutation representation afforded by left multiplication on the elements of G (cosets of $H = 1$) is called the *left regular representation* of G . One might think that we could study all groups more effectively by simply studying subgroups of symmetric groups (and all finite groups by studying subgroups of S_n , for all n). This approach alone is neither computationally nor theoretically practical, since to study groups of order n we would have to work in the much larger group S_n (cf. Exercise 7, for example).

Historically, finite groups were first studied not in an axiomatic setting as we have developed but as subgroups of S_n . Thus Cayley's Theorem proves that the historical notion of a group and the modern (axiomatic) one are equivalent. One advantage of the modern approach is that we are not, in our study of a given group, restricted to considering that group as a subgroup of some *particular* symmetric group (so in some sense our groups are “coordinate free”).

The next result generalizes our result on the normality of subgroups of index 2.

Corollary 5. If G is a finite group of order n and p is the smallest prime dividing $|G|$, then any subgroup of index p is normal.

Remark: In general, a group of order n need not have a subgroup of index p (for example, A_4 has no subgroup of index 2).

Proof: Suppose $H \leq G$ and $|G : H| = p$. Let π_H be the permutation representation afforded by multiplication on the set of left cosets of H in G , let $K = \ker \pi_H$ and let $|H : K| = k$. Then $|G : K| = |G : H||H : K| = pk$. Since H has p left cosets, G/K is isomorphic to a subgroup of S_p (namely, the image of G under π_H) by the First Isomorphism Theorem. By Lagrange's Theorem, $pk = |G/K|$ divides $p!$.

Thus $k \mid \frac{p!}{p} = (p - 1)!$. But all prime divisors of $(p - 1)!$ are less than p and by the minimality of p , every prime divisor of k is greater than or equal to p . This forces $k = 1$, so $H = K \trianglelefteq G$, completing the proof.

EXERCISES

Let G be a group and let H be a subgroup of G .

1. Let $G = \{1, a, b, c\}$ be the Klein 4-group whose group table is written out in Section 2.5.

- (a) Label $1, a, b, c$ with the integers 1,2,4,3, respectively, and prove that under the left regular representation of G into S_4 the nonidentity elements are mapped as follows:

$$a \mapsto (1 \ 2)(3 \ 4) \quad b \mapsto (1 \ 4)(2 \ 3) \quad c \mapsto (1 \ 3)(2 \ 4).$$

- (b) Relabel $1, a, b, c$ as 1,4,2,3, respectively, and compute the image of each element of G under the left regular representation of G into S_4 . Show that the image of G in S_4 under this labelling is the same *subgroup* as the image of G in part (a) (even though the nonidentity elements individually map to different permutations under the two different labellings).

2. List the elements of S_3 as 1, $(1 \ 2)$, $(2 \ 3)$, $(1 \ 3)$, $(1 \ 2 \ 3)$, $(1 \ 3 \ 2)$ and label these with the integers 1,2,3,4,5,6 respectively. Exhibit the image of each element of S_3 under the left regular representation of S_3 into S_6 .

3. Let r and s be the usual generators for the dihedral group of order 8.

- (a) List the elements of D_8 as $1, r, r^2, r^3, s, sr, sr^2, sr^3$ and label these with the integers 1, 2, ..., 8 respectively. Exhibit the image of each element of D_8 under the left regular representation of D_8 into S_8 .

- (b) Relabel this same list of elements of D_8 with the integers 1, 3, 5, 7, 2, 4, 6, 8 respectively and recompute the image of each element of D_8 under the left regular representation with respect to this new labelling. Show that the two subgroups of S_8 obtained in parts (a) and (b) are different.

4. Use the left regular representation of Q_8 to produce two elements of S_8 which generate a subgroup of S_8 isomorphic to the quaternion group Q_8 .

5. Let r and s be the usual generators for the dihedral group of order 8 and let $H = \langle s \rangle$. List the left cosets of H in D_8 as $1H, rH, r^2H$ and r^3H .

- (a) Label these cosets with the integers 1,2,3,4, respectively. Exhibit the image of each element of D_8 under the representation π_H of D_8 into S_4 obtained from the action of D_8 by left multiplication on the set of 4 left cosets of H in D_8 . Deduce that this representation is faithful (i.e., the elements of S_4 obtained form a subgroup isomorphic to D_8).

- (b) Repeat part (a) with the list of cosets relabelled by the integers 1,3,2,4, respectively. Show that the permutations obtained from this labelling form a subgroup of S_4 that is different from the subgroup obtained in part (a).

- (c) Let $K = \langle sr \rangle$, list the cosets of K in D_8 as $1K, rK, r^2K$ and r^3K , and label these with the integers 1,2,3,4. Prove that, with respect to this labelling, the image of D_8 under the representation π_K obtained from left multiplication on the cosets of K is the same *subgroup* of S_4 as in part (a) (even though the subgroups H and K are different and some of the elements of D_8 map to different permutations under the two homomorphisms).

6. Let r and s be the usual generators for the dihedral group of order 8 and let $N = \langle r^2 \rangle$. List the left cosets of N in D_8 as $1N, rN, sN$ and srN . Label these cosets with the integers 1,2,3,4 respectively. Exhibit the image of each element of D_8 under the representation π_N of D_8 into S_4 obtained from the action of D_8 by left multiplication on the set of 4 left cosets of N in D_8 . Deduce that this representation is not faithful and prove that $\pi_N(D_8)$ is isomorphic to the Klein 4-group.
7. Let Q_8 be the quaternion group of order 8.
 - (a) Prove that Q_8 is isomorphic to a subgroup of S_8 .
 - (b) Prove that Q_8 is not isomorphic to a subgroup of S_n for any $n \leq 7$. [If Q_8 acts on any set A of order ≤ 7 show that the stabilizer of any point $a \in A$ must contain the subgroup $\{-1\}$.]
8. Prove that if H has finite index n then there is a normal subgroup K of G with $K \leq H$ and $|G : K| \leq n!$.
9. Prove that if p is a prime and G is a group of order p^α for some $\alpha \in \mathbb{Z}^+$, then every subgroup of index p is normal in G . Deduce that every group of order p^2 has a normal subgroup of order p .
10. Prove that every non-abelian group of order 6 has a nonnormal subgroup of order 2. Use this to classify groups of order 6. [Produce an injective homomorphism into S_3 .]
11. Let G be a finite group and let $\pi : G \rightarrow S_G$ be the left regular representation. Prove that if x is an element of G of order n and $|G| = mn$, then $\pi(x)$ is a product of m n -cycles. Deduce that $\pi(x)$ is an odd permutation if and only if $|x|$ is even and $\frac{|G|}{|x|}$ is odd.
12. Let G and π be as in the preceding exercise. Prove that if $\pi(G)$ contains an odd permutation then G has a subgroup of index 2. [Use Exercise 3 in Section 3.3.]
13. Prove that if $|G| = 2k$ where k is odd then G has a subgroup of index 2. [Use Cauchy's Theorem to produce an element of order 2 and then use the preceding two exercises.]
14. Let G be a finite group of composite order n with the property that G has a subgroup of order k for each positive integer k dividing n . Prove that G is not simple.

4.3 GROUPS ACTING ON THEMSELVES BY CONJUGATION —THE CLASS EQUATION

In this section G is any group and we first consider G acting on itself (i.e., $A = G$) by conjugation:

$$g \cdot a = gag^{-1} \quad \text{for all } g \in G, a \in G$$

where gag^{-1} is computed in the group G as usual. This definition satisfies the two axioms for a group action because

$$g_1 \cdot (g_2 \cdot a) = g_1 \cdot (g_2 a g_2^{-1}) = g_1(g_2 a g_2^{-1})g_1^{-1} = (g_1 g_2)a(g_1 g_2)^{-1} = (g_1 g_2) \cdot a$$

and

$$1 \cdot a = 1a1^{-1} = a$$

for all $g_1, g_2 \in G$ and all $a \in G$.

Definition. Two elements a and b of G are said to be *conjugate in G* if there is some $g \in G$ such that $b = gag^{-1}$ (i.e., if and only if they are in the same orbit of G acting on itself by conjugation). The orbits of G acting on itself by conjugation are called the *conjugacy classes of G* .

Examples

- (1) If G is an abelian group then the action of G on itself by conjugation is the trivial action: $g \cdot a = a$, for all $g, a \in G$, and for each $a \in G$ the conjugacy class of a is $\{a\}$.
- (2) If $|G| > 1$ then, unlike the action by left multiplication, G does *not* act transitively on itself by conjugation because $\{1\}$ is always a conjugacy class (i.e., an orbit for this action). More generally, the one element subset $\{a\}$ is a conjugacy class if and only if $gag^{-1} = a$ for all $g \in G$ if and only if a is in the center of G .
- (3) In S_3 one can compute directly that the conjugacy classes are $\{1\}$, $\{(1 2), (1 3), (2 3)\}$ and $\{(1 2 3), (1 3 2)\}$. We shall shortly develop techniques for computing conjugacy classes more easily, particularly in symmetric groups.

As in the case of a group acting on itself by left multiplication, the action by conjugation can be generalized. If S is any subset of G , define

$$gSg^{-1} = \{gsg^{-1} \mid s \in S\}.$$

A group G acts on the set $\mathcal{P}(G)$ of all subsets of itself by defining $g \cdot S = gSg^{-1}$ for any $g \in G$ and $S \in \mathcal{P}(G)$. As above, this defines a group action of G on $\mathcal{P}(G)$. Note that if S is the one element set $\{s\}$ then $g \cdot S$ is the one element set $\{gsg^{-1}\}$ and so this action of G on all subsets of G may be considered as an extension of the action of G on itself by conjugation.

Definition. Two subsets S and T of G are said to be *conjugate in G* if there is some $g \in G$ such that $T = gSg^{-1}$ (i.e., if and only if they are in the same orbit of G acting on its subsets by conjugation).

We now apply Proposition 2 to the action of G by conjugation. Proposition 2 proves that if S is a subset of G , then the number of conjugates of S equals the index $|G : G_S|$ of the stabilizer G_S of S . For action by conjugation

$$G_S = \{g \in G \mid gSg^{-1} = S\} = N_G(S)$$

is the normalizer of S in G . We summarize this as

Proposition 6. The number of conjugates of a subset S in a group G is the index of the normalizer of S , $|G : N_G(S)|$. In particular, the number of conjugates of an element s of G is the index of the centralizer of s , $|G : C_G(s)|$.

Proof: The second assertion of the proposition follows from the observation that $N_G(\{s\}) = C_G(s)$.

The action of G on itself by conjugation partitions G into the conjugacy classes of G , whose orders can be computed by Proposition 6. Since the sum of the orders of these conjugacy classes is the order of G , we obtain the following important relation among these orders.

Theorem 7. (The Class Equation) Let G be a finite group and let g_1, g_2, \dots, g_r be representatives of the distinct conjugacy classes of G not contained in the center $Z(G)$ of G . Then

$$|G| = |Z(G)| + \sum_{i=1}^r |G : C_G(g_i)|.$$

Proof: As noted in Example 2 above the element $\{x\}$ is a conjugacy class of size 1 if and only if $x \in Z(G)$, since then $gxg^{-1} = x$ for all $g \in G$. Let $Z(G) = \{1, z_2, \dots, z_m\}$, let $\mathcal{K}_1, \mathcal{K}_2, \dots, \mathcal{K}_r$ be the conjugacy classes of G not contained in the center, and let g_i be a representative of \mathcal{K}_i for each i . Then the full set of conjugacy classes of G is given by

$$\{1\}, \{z_2\}, \dots, \{z_m\}, \mathcal{K}_1, \mathcal{K}_2, \dots, \mathcal{K}_r.$$

Since these partition G we have

$$\begin{aligned} |G| &= \sum_{i=1}^m 1 + \sum_{i=1}^r |\mathcal{K}_i| \\ &= |Z(G)| + \sum_{i=1}^r |G : C_G(g_i)|, \end{aligned}$$

where $|\mathcal{K}_i|$ is given by Proposition 6. This proves the class equation.

Note in particular that all the summands on the right hand side of the class equation are divisors of the group order since they are indices of subgroups of G . This restricts their possible values (cf. Exercise 6, for example).

Examples

- (1) The class equation gives no information in an abelian group since conjugation is the trivial action and all conjugacy classes have size 1.
- (2) In any group G we have $\langle g \rangle \leq C_G(g)$; this observation helps to minimize computations of conjugacy classes. For example, in the quaternion group Q_8 we see that $\langle i \rangle \leq C_{Q_8}(i) \leq Q_8$. Since $i \notin Z(Q_8)$ and $|Q_8 : \langle i \rangle| = 2$, we must have $C_{Q_8}(i) = \langle i \rangle$. Thus i has precisely 2 conjugates in Q_8 , namely i and $-i = kik^{-1}$. The other conjugacy classes in Q_8 are determined similarly and are

$$\{1\}, \{-1\}, \{\pm i\}, \{\pm j\}, \{\pm k\}.$$

The first two classes form $Z(Q_8)$ and the class equation for this group is

$$|Q_8| = 2 + 2 + 2 + 2.$$

- (3) In D_8 we may also use the fact that the three subgroups of index 2 are abelian to quickly see that if $x \notin Z(D_8)$, then $|C_{D_8}(x)| = 4$. The conjugacy classes of D_8 are

$$\{1\}, \{r^2\}, \{r, r^3\}, \{s, sr^2\}, \{sr, sr^3\}.$$

The first two classes form $Z(D_8)$ and the class equation for this group is

$$|D_8| = 2 + 2 + 2 + 2.$$

Before discussing more examples of conjugacy we give two important consequences of the class equation. The first application of the class equation is to show that groups of prime power order have nontrivial centers, which is the starting point for the study of groups of prime power order (to which we return in Chapter 6).

Theorem 8. If p is a prime and P is a group of prime power order p^α for some $\alpha \geq 1$, then P has a nontrivial center: $Z(P) \neq 1$.

Proof: By the class equation

$$|P| = |Z(P)| + \sum_{i=1}^r |P : C_P(g_i)|$$

where g_1, \dots, g_r are representatives of the distinct non-central conjugacy classes. By definition, $C_P(g_i) \neq P$ for $i = 1, 2, \dots, r$ so p divides $|P : C_P(g_i)|$. Since p also divides $|P|$ it follows that p divides $|Z(P)|$, hence the center must be nontrivial.

Corollary 9. If $|P| = p^2$ for some prime p , then P is abelian. More precisely, P is isomorphic to either Z_{p^2} or $Z_p \times Z_p$.

Proof: Since $Z(P) \neq 1$ by the theorem, it follows that $P/Z(P)$ is cyclic. By Exercise 36, Section 3.1, P is abelian. If P has an element of order p^2 , then P is cyclic. Assume therefore that every nonidentity element of P has order p . Let x be any nonidentity element of P and let $y \in P - \{x\}$. Since $|\langle x, y \rangle| > |\langle x \rangle| = p$, we must have that $P = \langle x, y \rangle$. Both x and y have order p so $\langle x \rangle \times \langle y \rangle = Z_p \times Z_p$. It now follows directly that the map $(x^a, y^b) \mapsto x^a y^b$ is an isomorphism from $\langle x \rangle \times \langle y \rangle$ onto P . This completes the proof.

Conjugacy in S_n

We next consider conjugation in symmetric groups. Readers familiar with linear algebra will recognize that in the matrix group $GL_n(F)$, conjugation is the same as “change of basis”: $A \mapsto PAP^{-1}$. The situation in S_n is analogous:

Proposition 10. Let σ, τ be elements of the symmetric group S_n and suppose σ has cycle decomposition

$$(a_1 a_2 \dots a_{k_1}) (b_1 b_2 \dots b_{k_2}) \dots .$$

Then $\tau\sigma\tau^{-1}$ has cycle decomposition

$$(\tau(a_1) \tau(a_2) \dots \tau(a_{k_1})) (\tau(b_1) \tau(b_2) \dots \tau(b_{k_2})) \dots ,$$

that is, $\tau\sigma\tau^{-1}$ is obtained from σ by replacing each entry i in the cycle decomposition for σ by the entry $\tau(i)$.

Proof: Observe that if $\sigma(i) = j$, then

$$\tau\sigma\tau^{-1}(\tau(i)) = \tau(j).$$

Thus, if the ordered pair i, j appears in the cycle decomposition of σ , then the ordered pair $\tau(i), \tau(j)$ appears in the cycle decomposition of $\tau\sigma\tau^{-1}$. This completes the proof.

Example

Let $\sigma = (1\ 2)(3\ 4\ 5)(6\ 7\ 8\ 9)$ and let $\tau = (1\ 3\ 5\ 7)(2\ 4\ 6\ 8)$. Then

$$\tau\sigma\tau^{-1} = (3\ 4)(5\ 6\ 7)(8\ 1\ 2\ 9).$$

Definition.

- (1) If $\sigma \in S_n$ is the product of disjoint cycles of lengths n_1, n_2, \dots, n_r with $n_1 \leq n_2 \leq \dots \leq n_r$ (including its 1-cycles) then the integers n_1, n_2, \dots, n_r are called the *cycle type* of σ .
- (2) If $n \in \mathbb{Z}^+$, a *partition* of n is any nondecreasing sequence of positive integers whose sum is n .

Note that by the results of the preceding section the cycle type of a permutation is unique. For example, the cycle type of an m -cycle in S_n is $1, 1, \dots, 1, m$, where the m is preceded by $n - m$ ones.

Proposition 11. Two elements of S_n are conjugate in S_n if and only if they have the same cycle type. The number of conjugacy classes of S_n equals the number of partitions of n .

Proof: By Proposition 10, conjugate permutations have the same cycle type. Conversely, suppose the permutations σ_1 and σ_2 have the same cycle type. Order the cycles in nondecreasing length, including 1-cycles (if several cycles of σ_1 and σ_2 have the same length then there are several ways of doing this). Ignoring parentheses, each cycle decomposition is a list in which all the integers from 1 to n appear exactly once. Define τ to be the function which maps the i^{th} integer in the list for σ_1 to the i^{th} integer in the list for σ_2 . Thus τ is a permutation and since the parentheses which delineate the cycle decompositions appear at the same positions in each list, Proposition 10 ensures that $\tau\sigma_1\tau^{-1} = \sigma_2$, so that σ_1 and σ_2 are conjugate.

Since there is a bijection between the conjugacy classes of S_n and the permissible cycle types and each cycle type for a permutation in S_n is a partition of n , the second assertion of the proposition follows, completing the proof.

Examples

- (1) Let $\sigma_1 = (1)(3\ 5)(8\ 9)(2\ 4\ 7\ 6)$ and let $\sigma_2 = (3)(4\ 7)(8\ 1)(5\ 2\ 6\ 9)$. Then define τ by $\tau(1) = 3, \tau(3) = 4, \tau(5) = 7, \tau(8) = 8$, etc. Then

$$\tau = (1\ 3\ 4\ 2\ 5\ 7\ 6\ 9)(8)$$

and $\tau\sigma_1\tau^{-1} = \sigma_2$.

- (2) If in the previous example we had reordered σ_2 as $\sigma_2 = (3)(8\ 1)(4\ 7)(5\ 2\ 6\ 9)$ by interchanging the two cycles of length 2, then the corresponding τ described above is defined by $\tau(1) = 3, \tau(3) = 8, \tau(5) = 1, \tau(8) = 4$, etc., which gives the permutation

$$\tau = (1\ 3\ 8\ 4\ 2\ 5)(6\ 9\ 7)$$

again with $\tau\sigma_1\tau^{-1} = \sigma_2$, which shows that there are many elements conjugating σ_1 into σ_2 .

- (3) If $n = 5$, the partitions of 5 and corresponding representatives of the conjugacy classes (with 1-cycles not written) are as given in the following table:

Partition of 5	Representative of Conjugacy Class
1, 1, 1, 1, 1	1
1, 1, 1, 2	(1 2)
1, 1, 3	(1 2 3)
1, 4	(1 2 3 4)
5	(1 2 3 4 5)
1, 2, 2	(1 2)(3 4)
2, 3	(1 2)(3 4 5)

Proposition 11 and Proposition 6 can be used to exhibit the centralizers of some elements in S_n . For example, if σ is an m -cycle in S_n , then the number of conjugates of σ (i.e., the number of m -cycles) is

$$\frac{n \cdot (n - 1) \cdots (n - m + 1)}{m}.$$

By Proposition 6 this is the index of the centralizer of σ : $\frac{|S_n|}{|C_{S_n}(\sigma)|}$. Since $|S_n| = n!$ we obtain

$$|C_{S_n}(\sigma)| = m \cdot (n - m)!.$$

The element σ certainly commutes with $1, \sigma, \sigma^2, \dots, \sigma^{m-1}$. It also commutes with any permutation in S_n whose cycles are disjoint from σ and there are $(n - m)!$ permutations of this type (the full symmetric group on the numbers not appearing in σ). The product of elements of these two types already accounts for $m \cdot (n - m)!$ elements commuting with σ . By the order computation above, this is the full centralizer of σ in S_n . Explicitly,

if σ is an m -cycle in S_n , then $C_{S_n}(\sigma) = \{\sigma^i \tau \mid 0 \leq i \leq m - 1, \tau \in S_{n-m}\}$

where S_{n-m} denotes the subgroup of S_n which fixes all integers appearing in the m -cycle σ (and is the identity subgroup if $m = n$ or $m = n - 1$).

For example, the centralizer of $\sigma = (1 3 5)$ in S_7 is the subgroup

$$\{(1 3 5)^i \tau \mid i = 0, 1 \text{ or } 2, \text{ and } \tau \text{ fixes } 1, 3 \text{ and } 5\}.$$

Note that $\tau \in S_A$ where $A = \{2, 4, 6, 7\}$, so there are $4!$ choices for τ and the centralizer has order $3 \cdot 4! = 72$.

We shall discuss centralizers of other elements of S_n in the next exercises and in Chapter 5.

We can use this discussion of the conjugacy classes in S_n to give a combinatorial proof of the simplicity of A_5 . We first observe that normal subgroups of a group G are the union of conjugacy classes of G , i.e.,

if $H \trianglelefteq G$, then for every conjugacy class \mathcal{K} of G either $\mathcal{K} \subseteq H$ or $\mathcal{K} \cap H = \emptyset$.

This is because if $x \in \mathcal{K} \cap H$, then $gxg^{-1} \in gHg^{-1}$ for all $g \in G$. Since H is normal, $gHg^{-1} = H$, so that H contains all the conjugates of x , i.e., $\mathcal{K} \subseteq H$.

Theorem 12. A_5 is a simple group.

Proof: We first work out the conjugacy classes of A_5 and their orders. Proposition 11 does not apply directly since two elements of the same cycle type (which are conjugate in S_5) need *not* be conjugate in A_5 . Exercises 19 to 22 analyze the relation of classes in S_n to classes in A_n in detail.

We have already seen that representatives of the cycle types of even permutations can be taken to be

$$1, \quad (1\ 2\ 3), \quad (1\ 2\ 3\ 4\ 5) \quad \text{and} \quad (1\ 2)(3\ 4).$$

The centralizers of 3-cycles and 5-cycles in S_5 were determined above, and checking which of these elements are contained in A_5 we see that

$$C_{A_5}((1\ 2\ 3)) = \langle (1\ 2\ 3) \rangle \quad \text{and} \quad C_{A_5}((1\ 2\ 3\ 4\ 5)) = \langle (1\ 2\ 3\ 4\ 5) \rangle.$$

These groups have orders 3 and 5 (index 20 and 12), respectively, so there are 20 distinct conjugates of $(1\ 2\ 3)$ and 12 distinct conjugates of $(1\ 2\ 3\ 4\ 5)$ in A_5 . Since there are a total of twenty 3-cycles in S_5 (Exercise 16, Section 1.3) and all of these lie in A_5 , we see that

$$\text{all twenty 3-cycles are conjugate in } A_5.$$

There are a total of twenty-four 5-cycles in A_5 but only 12 distinct conjugates of the 5-cycle $(1\ 2\ 3\ 4\ 5)$. Thus some 5-cycle, σ , is *not* conjugate to $(1\ 2\ 3\ 4\ 5)$ in A_5 (in fact, $(1\ 3\ 5\ 2\ 4)$ is not conjugate in A_5 to $(1\ 2\ 3\ 4\ 5)$ since the method of proof in Proposition 11 shows that any element of S_5 conjugating $(1\ 2\ 3\ 4\ 5)$ into $(1\ 3\ 5\ 2\ 4)$ must be an odd permutation). As above we see that σ also has 12 distinct conjugates in A_5 , hence

$$\text{the 5-cycles lie in two conjugacy classes in } A_5, \text{ each of which has 12 elements.}$$

Since the 3-cycles and 5-cycles account for all the nonidentity elements of odd order, the 15 remaining nonidentity elements of A_5 must have order 2 and therefore have cycle type $(2,2)$. It is easy to see that $(1\ 2)(3\ 4)$ commutes with $(1\ 3)(2\ 4)$ but does not commute with any element of odd order in A_5 . It follows that $|C_{A_5}((1\ 2)(3\ 4))| = 4$. Thus $(1\ 2)(3\ 4)$ has 15 distinct conjugates in A_5 , hence

$$\text{all 15 elements of order 2 in } A_5 \text{ are conjugate to } (1\ 2)(3\ 4).$$

In summary, the conjugacy classes of A_5 have orders 1, 15, 20, 12 and 12.

Now, suppose H were a normal subgroup of A_5 . Then as we observed above, H would be the union of conjugacy classes of A_5 . Then the order of H would be both a divisor of 60 (the order of A_5) and be the sum of some collection of the integers $\{1, 12, 12, 15, 20\}$ (the sizes of the conjugacy classes in A_5). A quick check shows the only possibilities are $|H| = 1$ or $|H| = 60$, so that A_5 has no proper, nontrivial normal subgroups.

Right Group Actions

As noted in Section 1.7, in the definition of an action the group elements appear to the left of the set elements and so our notion of an action might more precisely be termed a *left group action*. One can analogously define the notion of a *right group action* of the

group G on the nonempty set A as a map from $A \times G$ to A , denoted by $a \cdot g$ for $a \in A$ and $g \in G$, that satisfies the axioms:

- (1) $(a \cdot g_1) \cdot g_2 = a \cdot (g_1 g_2)$ for all $a \in A$, and $g_1, g_2 \in G$, and
- (2) $a \cdot 1 = a$ for all $a \in A$.

In much of the literature on group theory, conjugation is written as a right group action using the following notation:

$$a^g = g^{-1}ag \quad \text{for all } g, a \in G.$$

Similarly, for subsets S of G one defines $S^g = g^{-1}Sg$. In this notation the two axioms for a right action are verified as follows:

$$(a^{g_1})^{g_2} = g_2^{-1}(g_1^{-1}ag_1)g_2 = (g_1g_2)^{-1}a(g_1g_2) = a^{(g_1g_2)}$$

and

$$a^1 = 1^{-1}a1 = a$$

for all $g_1, g_2, a \in G$. Thus the two axioms for this right action of a group on itself take the form of the familiar “laws of exponentiation.” (Note that the integer power a^n of a group element a is easily distinguished from the conjugate a^g of a by the nature of the exponent: $n \in \mathbb{Z}$ but $g \in G$.) Because conjugation is so ubiquitous in the theory of groups, this notation is a useful and efficient shorthand (as opposed to always writing gag^{-1} or $g \cdot a$ for action on the left by conjugation).

For arbitrary group actions it is an easy exercise to check that if we are given a left group action of G on A then the map $A \times G \rightarrow A$ defined by $a \cdot g = g^{-1} \cdot a$ is a right group action. Conversely, given a right group action of G on A we can form a left group action by $g \cdot a = a \cdot g^{-1}$. Call these pairs *corresponding group actions*. Put another way, for corresponding group actions, g acts on the left in the same way that g^{-1} acts on the right. This is particularly transparent for the action of conjugation because the “left conjugate of a by g ,” namely gag^{-1} , is the same group element as the “right conjugate of a by g^{-1} ,” namely $a^{g^{-1}}$. Thus two elements or subsets of a group are “left conjugate” if and only if they are “right conjugate,” and so the relation “conjugacy” is the same for the left and right corresponding actions. More generally, it is also an exercise (Exercise 1) to see that for any corresponding left and right actions the orbits are the same.

We have consistently used left actions since they are compatible with the notation of applying functions on the left (i.e., with the notation $\varphi(g)$); in this way left multiplication on the left cosets of a subgroup is a left action. Similarly, right multiplication on the right cosets of a subgroup is a right action and the associated permutation representation φ is a homomorphism provided the function $\varphi : G \rightarrow S_A$ is written on the right as $(g_1g_2)\varphi$ (and also provided permutations in S_A are written on the right as functions from A to itself). There are instances where a set admits two actions by a group G : one naturally on the left and the other on the right, so that it is useful to be comfortable with both types of actions.

EXERCISES

Let G be a group.

- Suppose G has a left action on a set A , denoted by $g \cdot a$ for all $g \in G$ and $a \in A$. Denote the corresponding right action on A by $a \cdot g$. Prove that the (equivalence) relations \sim and \sim' defined by

$$a \sim b \quad \text{if and only if} \quad a = g \cdot b \quad \text{for some } g \in G$$

and

$$a \sim' b \quad \text{if and only if} \quad a = b \cdot g \quad \text{for some } g \in G$$

are the same relation (i.e., $a \sim b$ if and only if $a \sim' b$).

- Find all conjugacy classes and their sizes in the following groups:
 (a) D_8 (b) Q_8 (c) A_4 .
- Find all the conjugacy classes and their sizes in the following groups:
 (a) $Z_2 \times S_3$ (b) $S_3 \times S_3$ (c) $Z_3 \times A_4$.
- Prove that if $S \subseteq G$ and $g \in G$ then $gN_G(S)g^{-1} = N_G(gSg^{-1})$ and $gC_G(S)g^{-1} = C_G(gSg^{-1})$.
- If the center of G is of index n , prove that every conjugacy class has at most n elements.
- Assume G is a non-abelian group of order 15. Prove that $Z(G) = 1$. Use the fact that $\langle g \rangle \leq C_G(g)$ for all $g \in G$ to show that there is at most one possible class equation for G . [Use Exercise 36, Section 3.1.]
- For $n = 3, 4, 6$ and 7 make lists of the partitions of n and give representatives for the corresponding conjugacy classes of S_n .
- Prove that $Z(S_n) = 1$ for all $n \geq 3$.
- Show that $|C_{S_n}((1\ 2)(3\ 4))| = 8 \cdot (n - 4)!$ for all $n \geq 4$. Determine the elements in this centralizer explicitly.
- Let σ be the 5-cycle $(1\ 2\ 3\ 4\ 5)$ in S_5 . In each of (a) to (c) find an explicit element $\tau \in S_5$ which accomplishes the specified conjugation:
 (a) $\tau\sigma\tau^{-1} = \sigma^2$
 (b) $\tau\sigma\tau^{-1} = \sigma^{-1}$
 (c) $\tau\sigma\tau^{-1} = \sigma^{-2}$.
- In each of (a) – (d) determine whether σ_1 and σ_2 are conjugate. If they are, give an explicit permutation τ such that $\tau\sigma_1\tau^{-1} = \sigma_2$.
 (a) $\sigma_1 = (1\ 2)(3\ 4\ 5)$ and $\sigma_2 = (1\ 2\ 3)(4\ 5)$
 (b) $\sigma_1 = (1\ 5)(3\ 7\ 2)(10\ 6\ 8\ 11)$ and $\sigma_2 = (3\ 7\ 5\ 10)(4\ 9)(13\ 11\ 2)$
 (c) $\sigma_1 = (1\ 5)(3\ 7\ 2)(10\ 6\ 8\ 11)$ and $\sigma_2 = \sigma_1^3$
 (d) $\sigma_1 = (1\ 3)(2\ 4\ 6)$ and $\sigma_2 = (3\ 5)(2\ 4)(5\ 6)$.
- Find a representative for each conjugacy class of elements of order 4 in S_8 and in S_{12} .
- Find all finite groups which have exactly two conjugacy classes.
- In Exercise 1 of Section 2 two labellings of the elements $\{1, a, b, c\}$ of the Klein 4-group V were chosen to give two versions of the left regular representation of V into S_4 . Let π_1 be the version of regular representation obtained in part (a) of that exercise and let π_2 be the version obtained via the labelling in part (b). Let $\tau = (2\ 4)$. Show that $\tau \circ \pi_1(g) \circ \tau^{-1} = \pi_2(g)$ for each $g \in V$ (i.e., conjugation by τ sends the image of π_1 to the image of π_2 elementwise).

15. Find an element of S_8 which conjugates the subgroup of S_8 obtained in part (a) of Exercise 3, Section 2 to the subgroup of S_8 obtained in part (b) of that same exercise (both of these subgroups are isomorphic to D_8).
16. Find an element of S_4 which conjugates the subgroup of S_4 obtained in part (a) of Exercise 5, Section 2 to the subgroup of S_4 obtained in part (b) of that same exercise (both of these subgroups are isomorphic to D_8).
17. Let A be a nonempty set and let X be any subset of S_A . Let
- $$F(X) = \{a \in A \mid \sigma(a) = a \text{ for all } \sigma \in X\} \quad \text{— the fixed set of } X.$$
- Let $M(X) = A - F(X)$ be the elements which are *moved* by some element of X . Let $D = \{\sigma \in S_A \mid |M(\sigma)| < \infty\}$. Prove that D is a normal subgroup of S_A .
18. Let A be a set, let H be a subgroup of S_A and let $F(H)$ be the fixed points of H on A as defined in the preceding exercise. Prove that if $\tau \in N_{S_A}(H)$ then τ stabilizes the set $F(H)$ and its complement $A - F(H)$.
19. Assume H is a normal subgroup of G , \mathcal{K} is a conjugacy class of G contained in H and $x \in \mathcal{K}$. Prove that \mathcal{K} is a union of k conjugacy classes of equal size in H , where $k = |G : HC_G(x)|$. Deduce that a conjugacy class in S_n which consists of even permutations is either a single conjugacy class under the action of A_n or is a union of two classes of the same size in A_n . [Let $A = C_G(x)$ and $B = H$ so $A \cap B = C_H(x)$. Draw the lattice diagram associated to the Second Isomorphism Theorem and interpret the appropriate indices. See also Exercise 9, Section 1.]
20. Let $\sigma \in A_n$. Show that all elements in the conjugacy class of σ in S_n (i.e., all elements of the same cycle type as σ) are conjugate in A_n if and only if σ commutes with an odd permutation. [Use the preceding exercise.]
21. Let \mathcal{K} be a conjugacy class in S_n and assume that $\mathcal{K} \subseteq A_n$. Show $\sigma \in S_n$ does *not* commute with any odd permutation if and only if the cycle type of σ consists of distinct odd integers. Deduce that \mathcal{K} consists of two conjugacy classes in A_n if and only if the cycle type of an element of \mathcal{K} consists of distinct odd integers. [Assume first that $\sigma \in \mathcal{K}$ does not commute with any odd permutation. Observe that σ commutes with each individual cycle in its cycle decomposition — use this to show that all its cycles must be of odd length. If two cycles have the same odd length, k , find a product of k transpositions which interchanges them and commutes with σ . Conversely, if the cycle type of σ consists of distinct integers, prove that σ commutes *only* with the group generated by the cycles in its cycle decomposition.]
22. Show that if n is odd then the set of all n -cycles consists of two conjugacy classes of equal size in A_n .
23. Recall (cf. Exercise 16, Section 2.4) that a proper subgroup M of G is called *maximal* if whenever $M \leq H \leq G$, either $H = M$ or $H = G$. Prove that if M is a maximal subgroup of G then either $N_G(M) = M$ or $N_G(M) = G$. Deduce that if M is a maximal subgroup of G that is not normal in G then the number of nonidentity elements of G that are contained in conjugates of M is at most $(|M| - 1)|G : M|$.
24. Assume H is a proper subgroup of the finite group G . Prove $G \neq \cup_{g \in G} gHg^{-1}$, i.e., G is not the union of the conjugates of any proper subgroup. [Put H in some maximal subgroup and use the preceding exercise.]
25. Let $G = GL_2(\mathbb{C})$ and let $H = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{C}, ac \neq 0 \right\}$. Prove that every element of G is conjugate to some element of the subgroup H and deduce that G is the union of

- conjugates of H . [Show that every element of $GL_2(\mathbb{C})$ has an eigenvector.]
26. Let G be a transitive permutation group on the finite set A with $|A| > 1$. Show that there is some $\sigma \in G$ such that $\sigma(a) \neq a$ for all $a \in A$ (such an element σ is called *fixed point free*).
27. Let g_1, g_2, \dots, g_r be representatives of the conjugacy classes of the finite group G and assume these elements pairwise commute. Prove that G is abelian.
28. Let p and q be primes with $p < q$. Prove that a non-abelian group G of order pq has a nonnormal subgroup of index q , so that there exists an injective homomorphism into S_q . Deduce that G is isomorphic to a subgroup of the normalizer in S_q of the cyclic group generated by the q -cycle $(1\ 2\ \dots\ q)$.
29. Let p be a prime and let G be a group of order p^α . Prove that G has a subgroup of order p^β , for every β with $0 \leq \beta \leq \alpha$. [Use Theorem 8 and induction on α .]
30. If G is a group of odd order, prove for any nonidentity element $x \in G$ that x and x^{-1} are not conjugate in G .
31. Using the usual generators and relations for the dihedral group D_{2n} (cf. Section 1.2) show that for $n = 2k$ an even integer the conjugacy classes in D_{2n} are the following: $\{1\}$, $\{r^k\}$, $\{r^{\pm 1}\}$, $\{r^{\pm 2}\}$, \dots , $\{r^{\pm(k-1)}\}$, $\{sr^{2b} \mid b = 1, \dots, k\}$ and $\{sr^{2b-1} \mid b = 1, \dots, k\}$. Give the class equation for D_{2n} .
32. For $n = 2k + 1$ an odd integer show that the conjugacy classes in D_{2n} are $\{1\}$, $\{r^{\pm 1}\}$, $\{r^{\pm 2}\}$, \dots , $\{r^{\pm k}\}$, $\{sr^b \mid b = 1, \dots, n\}$. Give the class equation for D_{2n} .
33. This exercise gives a formula for the size of each conjugacy class in S_n . Let σ be a permutation in S_n and let m_1, m_2, \dots, m_s be the *distinct* integers which appear in the cycle type of σ (including 1-cycles). For each $i \in \{1, 2, \dots, s\}$ assume σ has k_i cycles of length m_i (so that $\sum_{i=1}^s k_i m_i = n$). Prove that the number of conjugates of σ is

$$\frac{n!}{(k_1!m_1^{k_1})(k_2!m_2^{k_2}) \dots (k_s!m_s^{k_s})}.$$

- [See Exercises 6 and 7 in Section 1.3 where this formula was given in some special cases.]
34. Prove that if p is a prime and P is a subgroup of S_p of order p , then $|N_{S_p}(P)| = p(p-1)$. [Argue that every conjugate of P contains exactly $p-1$ p -cycles and use the formula for the number of p -cycles to compute the index of $N_{S_p}(P)$ in S_p .]
35. Let p be a prime. Find a formula for the number of conjugacy classes of elements of order p in S_n (using the greatest integer function).
36. Let $\pi : G \rightarrow S_G$ be the left regular representation afforded by the action of G on itself by left multiplication. For each $g \in G$ denote the permutation $\pi(g)$ by σ_g , so that $\sigma_g(x) = gx$ for all $x \in G$. Let $\lambda : G \rightarrow S_G$ be the permutation representation afforded by the corresponding right action of G on itself, and for each $h \in G$ denote the permutation $\lambda(h)$ by τ_h . Thus $\tau_h(x) = xh^{-1}$ for all $x \in G$ (λ is called the *right regular representation* of G).
- (a) Prove that σ_g and τ_h commute for all $g, h \in G$. (Thus the centralizer in S_G of $\pi(G)$ contains the subgroup $\lambda(G)$, which is isomorphic to G .)
- (b) Prove that $\sigma_g = \tau_g$ if and only if g is an element of order 1 or 2 in the center of G .
- (c) Prove that $\sigma_g = \tau_h$ if and only if g and h lie in the center of G . Deduce that $\pi(G) \cap \lambda(G) = \pi(Z(G)) = \lambda(Z(G))$.

4.4 AUTOMORPHISMS

Definition. Let G be a group. An isomorphism from G onto itself is called an *automorphism* of G . The set of all automorphisms of G is denoted by $\text{Aut}(G)$.

We leave as an exercise the simple verification that $\text{Aut}(G)$ is a group under composition of automorphisms, the *automorphism group* of G (composition of automorphisms is defined since the domain and range of each automorphism is the same). Notice that automorphisms of a group G are, in particular, permutations of the set G so $\text{Aut}(G)$ is a subgroup of S_G .

One of the most important examples of an automorphism of a group G is provided by conjugation by a fixed element in G . The next result discusses this in a slightly more general context.

Proposition 13. Let H be a normal subgroup of the group G . Then G acts by conjugation on H as automorphisms of H . More specifically, the action of G on H by conjugation is defined for each $g \in G$ by

$$h \mapsto ghg^{-1} \quad \text{for each } h \in H.$$

For each $g \in G$, conjugation by g is an automorphism of H . The permutation representation afforded by this action is a homomorphism of G into $\text{Aut}(H)$ with kernel $C_G(H)$. In particular, $G/C_G(H)$ is isomorphic to a subgroup of $\text{Aut}(H)$.

Proof: (cf. Exercise 17, Section 1.7) Let φ_g be conjugation by g . Note that because g normalizes H , φ_g maps H to itself. Since we have already seen that conjugation defines an action, it follows that $\varphi_1 = 1$ (the identity map on H) and $\varphi_a \circ \varphi_b = \varphi_{ab}$ for all $a, b \in G$. Thus each φ_g gives a bijection from H to itself since it has a 2-sided inverse $\varphi_{g^{-1}}$. Each φ_g is a homomorphism from H to H because

$$\varphi_g(hk) = g(hk)g^{-1} = gh(gg^{-1})kg^{-1} = (ghg^{-1})(gkg^{-1}) = \varphi_g(h)\varphi_g(k)$$

for all $h, k \in H$. This proves that conjugation by any fixed element of G defines an automorphism of H .

By the preceding remark, the permutation representation $\psi : G \rightarrow S_H$ defined by $\psi(g) = \varphi_g$ (which we have already proved is a homomorphism) has image contained in the subgroup $\text{Aut}(H)$ of S_H . Finally,

$$\begin{aligned} \ker \psi &= \{g \in G \mid \varphi_g = \text{id}\} \\ &= \{g \in G \mid ghg^{-1} = h \text{ for all } h \in H\} \\ &= C_G(H). \end{aligned}$$

The First Isomorphism Theorem implies the final statement of the proposition.

Proposition 13 shows that a group acts by conjugation on a normal subgroup as *structure preserving* permutations, i.e., as automorphisms. In particular, this action must send subgroups to subgroups, elements of order n to elements of order n , etc. Two specific applications of this proposition are described in the next two corollaries.

Corollary 14. If K is any subgroup of the group G and $g \in G$, then $K \cong gKg^{-1}$. Conjugate elements and conjugate subgroups have the same order.

Proof: Letting $G = H$ in the proposition shows that conjugation by $g \in G$ is an automorphism of G , from which the corollary follows.

Corollary 15. For any subgroup H of a group G , the quotient group $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $\text{Aut}(H)$. In particular, $G/Z(G)$ is isomorphic to a subgroup of $\text{Aut}(G)$.

Proof: Since H is a normal subgroup of the group $N_G(H)$, Proposition 13 (applied with $N_G(H)$ playing the role of G) implies the first assertion. The second assertion is the special case when $H = G$, in which case $N_G(G) = G$ and $C_G(G) = Z(G)$.

Definition. Let G be a group and let $g \in G$. Conjugation by g is called an *inner automorphism* of G and the subgroup of $\text{Aut}(G)$ consisting of all inner automorphisms is denoted by $\text{Inn}(G)$.

Note that the collection of inner automorphisms of G is in fact a subgroup of $\text{Aut}(G)$ and that by Corollary 15, $\text{Inn}(G) \cong G/Z(G)$. Note also that if H is a normal subgroup of G , conjugation by an element of G when restricted to H is an automorphism of H but need not be an inner automorphism of H (as we shall see).

Examples

- (1) A group G is abelian if and only if every inner automorphism is trivial. If H is an abelian normal subgroup of G and H is not contained in $Z(G)$, then there is some $g \in G$ such that conjugation by g restricted to H is not an inner automorphism of H . An explicit example of this is $G = A_4$, H is the Klein 4-group in G and g is any 3-cycle.
- (2) Since $Z(Q_8) = \{-1\}$ we have $\text{Inn}(Q_8) \cong V_4$.
- (3) Since $Z(D_8) = \{r^2\}$ we have $\text{Inn}(D_8) \cong V_4$.
- (4) Since for all $n \geq 3$, $Z(S_n) = 1$ we have $\text{Inn}(S_n) \cong S_n$.

Corollary 15 shows that any information we have about the automorphism group of a subgroup H of a group G translates into information about $N_G(H)/C_G(H)$. For example, if $H \cong Z_2$, then since H has unique elements of orders 1 and 2, Corollary 14 forces $\text{Aut}(H) = 1$. Thus if $H \cong Z_2$, $N_G(H) = C_G(H)$; if in addition H is a normal subgroup of G , then $H \leq Z(G)$ (cf. Exercise 10, Section 2.2).

Although the preceding example was fairly trivial, it illustrates that the action of G by conjugation on a *normal* subgroup H can be restricted by knowledge of the automorphism group of H . This in turn can be used to investigate the structure of G and will lead to some classification theorems when we consider semidirect products in Section 5.5.

A notion which will be used in later sections most naturally warrants introduction here:

Definition. A subgroup H of a group G is called *characteristic* in G , denoted $H \operatorname{char} G$, if every automorphism of G maps H to itself, i.e., $\sigma(H) = H$ for all $\sigma \in \operatorname{Aut}(G)$.

Results concerning characteristic subgroups which we shall use later (and whose proofs are relegated to the exercises) are

- (1) characteristic subgroups are normal,
- (2) if H is the unique subgroup of G of a given order, then H is characteristic in G , and
- (3) if $K \operatorname{char} H$ and $H \trianglelefteq G$, then $K \trianglelefteq G$ (so although “normality” is not a transitive property (i.e., a normal subgroup of a normal subgroup need not be normal), a characteristic subgroup of a normal subgroup is normal).

Thus we may think of characteristic subgroups as “strongly normal” subgroups. For example, property (2) and Theorem 2.7 imply that every subgroup of a cyclic group is characteristic.

We close this section with some results on automorphism groups of specific groups.

Proposition 16. The automorphism group of the cyclic group of order n is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$, an abelian group of order $\varphi(n)$ (where φ is Euler’s function).

Proof: Let x be a generator of the cyclic group Z_n . If $\psi \in \operatorname{Aut}(Z_n)$, then $\psi(x) = x^a$ for some $a \in \mathbb{Z}$ and the integer a uniquely determines ψ . Denote this automorphism by ψ_a . As usual, since $|x| = n$, the integer a is only defined mod n . Since ψ_a is an automorphism, x and x^a must have the same order, hence $(a, n) = 1$. Furthermore, for every a relatively prime to n , the map $x \mapsto x^a$ is an automorphism of Z_n . Hence we have a surjective map

$$\begin{aligned}\Psi : \operatorname{Aut}(Z_n) &\rightarrow (\mathbb{Z}/n\mathbb{Z})^\times \\ \psi_a &\mapsto a \pmod{n}.\end{aligned}$$

The map Ψ is a homomorphism because

$$\psi_a \circ \psi_b(x) = \psi_a(x^b) = (x^b)^a = x^{ab} = \psi_{ab}(x)$$

for all $\psi_a, \psi_b \in \operatorname{Aut}(Z_n)$, so that

$$\Psi(\psi_a \circ \psi_b) = \Psi(\psi_{ab}) = ab \pmod{n} = \Psi(\psi_a)\Psi(\psi_b).$$

Finally, Ψ is clearly injective, hence is an isomorphism.

A complete description of the isomorphism type of $\operatorname{Aut}(Z_n)$ is given at the end of Section 9.5.

Example

Assume G is a group of order pq , where p and q are primes (not necessarily distinct) with $p \leq q$. If $p \nmid q - 1$, we prove G is abelian.

If $Z(G) \neq 1$, Lagrange’s Theorem forces $G/Z(G)$ to be cyclic, hence G is abelian by Exercise 36, Section 3.1. Hence we may assume $Z(G) = 1$.

If every nonidentity element of G has order p , then the centralizer of every nonidentity element has index q , so the class equation for G reads

$$pq = 1 + kq.$$

This is impossible since q divides pq and kq but not 1. Thus G contains an element, x , of order q .

Let $H = \langle x \rangle$. Since H has index p and p is the smallest prime dividing $|G|$, the subgroup H is normal in G by Corollary 5. Since $Z(G) = 1$, we must have $C_G(H) = H$. Thus $G/H = N_G(H)/C_G(H)$ is a group of order p isomorphic to a subgroup of $\text{Aut}(H)$ by Corollary 15. But by Proposition 16, $\text{Aut}(H)$ has order $\varphi(q) = q - 1$, which by Lagrange's Theorem would imply $p \mid q - 1$, contrary to assumption. This shows that G must be abelian.

One can check that every group of order pq , where p and q are distinct primes with $p < q$ and $p \nmid q - 1$ is *cyclic* (see the exercises). This is the first instance where there is a unique isomorphism type of group whose order is *composite*. For instance, every group of order 15 is cyclic.

The next proposition summarizes some results on automorphism groups of known groups and will be proved later. Part 3 of this proposition illustrates how the theory of vector spaces comes into play in group theory.

Proposition 17.

- (1) If p is an odd prime and $n \in \mathbb{Z}^+$, then the automorphism group of the cyclic group of order p is cyclic of order $p - 1$. More generally, the automorphism group of the cyclic group of order p^n is cyclic of order $p^{n-1}(p-1)$ (cf. Corollary 20, Section 9.5).
- (2) For all $n \geq 3$ the automorphism group of the cyclic group of order 2^n is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_{2^{n-2}}$, and in particular is not cyclic but has a cyclic subgroup of index 2 (cf. Corollary 20, Section 9.5).
- (3) Let p be a prime and let V be an abelian group (written additively) with the property that $pv = 0$ for all $v \in V$. If $|V| = p^n$, then V is an n -dimensional vector space over the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. The automorphisms of V are precisely the nonsingular linear transformations from V to itself, that is

$$\text{Aut}(V) \cong GL(V) \cong GL_n(\mathbb{F}_p).$$

In particular, the order of $\text{Aut}(V)$ is as given in Section 1.4 (cf. the examples in Sections 10.2 and 11.1).

- (4) For all $n \neq 6$ we have $\text{Aut}(S_n) = \text{Inn}(S_n) \cong S_n$ (cf. Exercise 18). For $n = 6$ we have $|\text{Aut}(S_6)| : |\text{Inn}(S_6)| = 2$ (cf. the following Exercise 19 and also Exercise 10 in Section 6.3).
- (5) $\text{Aut}(D_8) \cong D_8$ and $\text{Aut}(Q_8) \cong S_4$ (cf. the following Exercises 4 and 5 and also Exercise 9 in Section 6.3).

The group V described in Part 3 of the proposition is called the *elementary abelian* group of order p^n (we shall see in Chapter 5 that it is uniquely determined up to isomorphism by p and n). The Klein 4-group, V_4 , is the elementary abelian group of order 4. This proposition asserts that

$$\text{Aut}(V_4) \cong GL_2(\mathbb{F}_2).$$

By the exercises in Section 1.4, the latter group has order 6. But $\text{Aut}(V_4)$ permutes the 3 nonidentity elements of V_4 , and this action of $\text{Aut}(V_4)$ on $V_4 - \{1\}$ gives an injective permutation representation of $\text{Aut}(V_4)$ into S_3 . By order considerations, the homomorphism is onto, so

$$\text{Aut}(V_4) \cong GL_2(\mathbb{F}_2) \cong S_3.$$

Note that V_4 is abelian, so $\text{Inn}(V_4) = 1$.

For any prime p , the elementary abelian group of order p^2 is $Z_p \times Z_p$. Its automorphism group, $GL_2(\mathbb{F}_p)$, has order $p(p-1)^2(p+1)$. Thus Corollary 9 implies that for p a prime

$$\text{if } |P| = p^2, \quad |\text{Aut}(P)| = p(p-1) \text{ or } p(p-1)^2(p+1)$$

according to whether P is cyclic or elementary abelian, respectively.

Example

Suppose G is a group of order $45 = 3^2 5$ with a normal subgroup P of order 3^2 . We show that G is necessarily abelian.

The quotient $G/C_G(P)$ is isomorphic to a subgroup of $\text{Aut}(P)$ by Corollary 15, and $\text{Aut}(P)$ has order 6 or 48 (according to whether P is cyclic or elementary abelian, respectively) by the preceding paragraph. On the other hand, since the order of P is the square of a prime, P is an abelian group, hence $P \leq C_G(P)$. It follows that $|C_G(P)|$ is divisible by 9, which implies $|G/C_G(P)|$ is 1 or 5. Together these imply $|G/C_G(P)| = 1$, i.e., $C_G(P) = G$ and $P \leq Z(G)$. Since then $G/Z(G)$ is cyclic, G must be an abelian group.

EXERCISES

Let G be a group.

- If $\sigma \in \text{Aut}(G)$ and φ_g is conjugation by g prove $\sigma \varphi_g \sigma^{-1} = \varphi_{\sigma(g)}$. Deduce that $\text{Inn}(G) \trianglelefteq \text{Aut}(G)$. (The group $\text{Aut}(G)/\text{Inn}(G)$ is called the *outer automorphism group* of G .)
- Prove that if G is an abelian group of order pq , where p and q are distinct primes, then G is cyclic. [Use Cauchy's Theorem to produce elements of order p and q and consider the order of their product.]
- Prove that under any automorphism of D_8 , r has at most 2 possible images and s has at most 4 possible images (r and s are the usual generators — cf. Section 1.2). Deduce that $|\text{Aut}(D_8)| \leq 8$.
- Use arguments similar to those in the preceding exercise to show $|\text{Aut}(Q_8)| \leq 24$.
- Use the fact that $D_8 \trianglelefteq D_{16}$ to prove that $\text{Aut}(D_8) \cong D_8$.
- Prove that characteristic subgroups are normal. Give an example of a normal subgroup that is not characteristic.
- If H is the unique subgroup of a given order in a group G prove H is characteristic in G .
- Let G be a group with subgroups H and K with $H \leq K$.
 - Prove that if H is characteristic in K and K is normal in G then H is normal in G .
 - Prove that if H is characteristic in K and K is characteristic in G then H is characteristic in G . Use this to prove that the Klein 4-group V_4 is characteristic in S_4 .
 - Give an example to show that if H is normal in K and K is characteristic in G then H need not be normal in G .

9. If r, s are the usual generators for the dihedral group D_{2n} , use the preceding two exercises to deduce that every subgroup of $\langle r \rangle$ is normal in D_{2n} .
10. Let G be a group, let A be an abelian normal subgroup of G , and write $\overline{G} = G/A$. Show that \overline{G} acts (on the left) by conjugation on A by $\overline{g} \cdot a = gag^{-1}$, where g is any representative of the coset \overline{g} (in particular, show that this action is well defined). Give an explicit example to show that this action is not well defined if A is non-abelian.
11. If p is a prime and P is a subgroup of S_p of order p , prove $N_{S_p}(P)/C_{S_p}(P) \cong \text{Aut}(P)$. [Use Exercise 34, Section 3.]
12. Let G be a group of order 3825. Prove that if H is a normal subgroup of order 17 in G then $H \leq Z(G)$.
13. Let G be a group of order 203. Prove that if H is a normal subgroup of order 7 in G then $H \leq Z(G)$. Deduce that G is abelian in this case.
14. Let G be a group of order 1575. Prove that if H is a normal subgroup of order 9 in G then $H \leq Z(G)$.
15. Prove that each of the following (multiplicative) groups is cyclic: $(\mathbb{Z}/5\mathbb{Z})^\times$, $(\mathbb{Z}/9\mathbb{Z})^\times$ and $(\mathbb{Z}/18\mathbb{Z})^\times$.
16. Prove that $(\mathbb{Z}/24\mathbb{Z})^\times$ is an elementary abelian group of order 8. (We shall see later that $(\mathbb{Z}/n\mathbb{Z})^\times$ is an elementary abelian group if and only if $n \mid 24$.)
17. Let $G = \langle x \rangle$ be a cyclic group of order n . For $n = 2, 3, 4, 5, 6$ write out the elements of $\text{Aut}(G)$ explicitly (by Proposition 16 above we know $\text{Aut}(G) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, so for each element $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, write out explicitly what the automorphism ψ_a does to the elements $\{1, x, x^2, \dots, x^{n-1}\}$ of G).
18. This exercise shows that for $n \neq 6$ every automorphism of S_n is inner. Fix an integer $n \geq 2$ with $n \neq 6$.
- Prove that the automorphism group of a group G permutes the conjugacy classes of G , i.e., for each $\sigma \in \text{Aut}(G)$ and each conjugacy class \mathcal{K} of G the set $\sigma(\mathcal{K})$ is also a conjugacy class of G .
 - Let \mathcal{K} be the conjugacy class of transpositions in S_n and let \mathcal{K}' be the conjugacy class of any element of order 2 in S_n that is not a transposition. Prove that $|\mathcal{K}| \neq |\mathcal{K}'|$. Deduce that any automorphism of S_n sends transpositions to transpositions. [See Exercise 33 in Section 3.]
 - Prove that for each $\sigma \in \text{Aut}(S_n)$
- $$\sigma : (1 \ 2) \mapsto (a \ b_2), \quad \sigma : (1 \ 3) \mapsto (a \ b_3), \quad \dots, \quad \sigma : (1 \ n) \mapsto (a \ b_n)$$
- for some distinct integers $a, b_2, b_3, \dots, b_n \in \{1, 2, \dots, n\}$.
- Show that $(1 \ 2), (1 \ 3), \dots, (1 \ n)$ generate S_n and deduce that any automorphism of S_n is uniquely determined by its action on these elements. Use (c) to show that S_n has at most $n!$ automorphisms and conclude that $\text{Aut}(S_n) = \text{Inn}(S_n)$ for $n \neq 6$.
19. This exercise shows that $|\text{Aut}(S_6)| : \text{Inn}(S_6)| \leq 2$ (Exercise 10 in Section 6.3 shows that equality holds by exhibiting an automorphism of S_6 that is not inner).
- Let \mathcal{K} be the conjugacy class of transpositions in S_6 and let \mathcal{K}' be the conjugacy class of any element of order 2 in S_6 that is not a transposition. Prove that $|\mathcal{K}| \neq |\mathcal{K}'|$ unless \mathcal{K}' is the conjugacy class of products of three disjoint transpositions. Deduce that $\text{Aut}(S_6)$ has a subgroup of index at most 2 which sends transpositions to transpositions.
 - Prove that $|\text{Aut}(S_6) : \text{Inn}(S_6)| \leq 2$. [Follow the same steps as in (c) and (d) of the preceding exercise to show that any automorphism that sends transpositions to transpositions is inner.]

The next exercise introduces a subgroup, $J(P)$, which (like the center of P) is defined for an arbitrary finite group P (although in most applications P is a group whose order is a power of a prime). This subgroup was defined by J. Thompson in 1964 and it now plays a pivotal role in the study of finite groups, in particular, in the classification of finite simple groups.

- 20.** For any finite group P let $d(P)$ be the minimum number of generators of P (so, for example, $d(P) = 1$ if and only if P is a nontrivial cyclic group and $d(Q_8) = 2$). Let $m(P)$ be the maximum of the integers $d(A)$ as A runs over all *abelian* subgroups of P (so, for example, $m(Q_8) = 1$ and $m(D_8) = 2$). Define

$$J(P) = \{ A \mid A \text{ is an abelian subgroup of } P \text{ with } d(A) = m(P) \}.$$

$(J(P))$ is called the *Thompson subgroup* of P .

- (a) Prove that $J(P)$ is a characteristic subgroup of P .
- (b) For each of the following groups P list all abelian subgroups A of P that satisfy $d(A) = m(P)$: Q_8 , D_8 , D_{16} and QD_{16} (where QD_{16} is the quasidihedral group of order 16 defined in Exercise 11 of Section 2.5). [Use the lattices of subgroups for these groups in Section 2.5.]
- (c) Show that $J(Q_8) = Q_8$, $J(D_8) = D_8$, $J(D_{16}) = D_{16}$ and $J(QD_{16})$ is a dihedral subgroup of order 8 in QD_{16} .
- (d) Prove that if $Q \leq P$ and $J(P)$ is a subgroup of Q , then $J(P) = J(Q)$. Deduce that if P is a subgroup (not necessarily normal) of the finite group G and $J(P)$ is contained in some subgroup Q of P such that $Q \trianglelefteq G$, then $J(P) \trianglelefteq G$.

4.5 SYLOW'S THEOREM

In this section we prove a partial converse to Lagrange's Theorem and derive numerous consequences, some of which will lead to classification theorems in the next chapter.

Definition. Let G be a group and let p be a prime.

- (1) A group of order p^α for some $\alpha \geq 1$ is called a *p-group*. Subgroups of G which are *p-groups* are called *p-subgroups*.
- (2) If G is a group of order $p^\alpha m$, where $p \nmid m$, then a subgroup of order p^α is called a *Sylow p-subgroup* of G .
- (3) The set of Sylow *p-subgroups* of G will be denoted by $Syl_p(G)$ and the number of Sylow *p-subgroups* of G will be denoted by $n_p(G)$ (or just n_p when G is clear from the context).

Theorem 18. (Sylow's Theorem) Let G be a group of order $p^\alpha m$, where p is a prime not dividing m .

- (1) Sylow *p-subgroups* of G exist, i.e., $Syl_p(G) \neq \emptyset$.
- (2) If P is a Sylow *p-subgroup* of G and Q is any *p-subgroup* of G , then there exists $g \in G$ such that $Q \leq gPg^{-1}$, i.e., Q is contained in some conjugate of P . In particular, any two Sylow *p-subgroups* of G are conjugate in G .
- (3) The number of Sylow *p-subgroups* of G is of the form $1 + kp$, i.e.,

$$n_p \equiv 1 \pmod{p}.$$

Further, n_p is the index in G of the normalizer $N_G(P)$ for any Sylow *p-subgroup* P , hence n_p divides m .

We first prove the following lemma:

Lemma 19. Let $P \in Syl_p(G)$. If Q is any p -subgroup of G , then $Q \cap N_G(P) = Q \cap P$.

Proof: Let $H = N_G(P) \cap Q$. Since $P \leq N_G(P)$ it is clear that $P \cap Q \leq H$, so we must prove the reverse inclusion. Since by definition $H \leq Q$, this is equivalent to showing $H \leq P$. We do this by demonstrating that PH is a p -subgroup of G containing both P and H ; but P is a p -subgroup of G of largest possible order, so we must have $PH = P$, i.e., $H \leq P$.

Since $H \leq N_G(P)$, by Corollary 15 in Section 3.2, PH is a subgroup. By Proposition 13 in the same section

$$|PH| = \frac{|P||H|}{|P \cap H|}.$$

All the numbers in the above quotient are powers of p , so PH is a p -group. Moreover, P is a subgroup of PH so the order of PH is divisible by p^α , the largest power of p which divides $|G|$. These two facts force $|PH| = p^\alpha = |P|$. This in turn implies $P = PH$ and $H \leq P$. This establishes the lemma.

Proof of Sylow's Theorem (1) Proceed by induction on $|G|$. If $|G| = 1$, there is nothing to prove. Assume inductively the existence of Sylow p -subgroups for all groups of order less than $|G|$.

If p divides $|Z(G)|$, then by Cauchy's Theorem for abelian groups (Proposition 21, Section 3.4) $Z(G)$ has a subgroup, N , of order p . Let $\bar{G} = G/N$, so that $|\bar{G}| = p^{\alpha-1}m$. By induction, \bar{G} has a subgroup \bar{P} of order $p^{\alpha-1}$. If we let P be the subgroup of G containing N such that $P/N = \bar{P}$ then $|P| = |P/N| \cdot |N| = p^\alpha$ and P is a Sylow p -subgroup of G . We are reduced to the case when p does not divide $|Z(G)|$.

Let g_1, g_2, \dots, g_r be representatives of the distinct non-central conjugacy classes of G . The class equation for G is

$$|G| = |Z(G)| + \sum_{i=1}^r |G : C_G(g_i)|.$$

If $p \mid |G : C_G(g_i)|$ for all i , then since $p \mid |G|$, we would also have $p \mid |Z(G)|$, a contradiction. Thus for some i , p does not divide $|G : C_G(g_i)|$. For this i let $H = C_G(g_i)$ so that

$$|H| = p^\alpha k, \quad \text{where } p \nmid k.$$

Since $g_i \notin Z(G)$, $|H| < |G|$. By induction, H has a Sylow p -subgroup, P , which of course is also a subgroup of G . Since $|P| = p^\alpha$, P is a Sylow p -subgroup of G . This completes the induction and establishes (1).

Before proving (2) and (3) we make some calculations. By (1) there exists a Sylow p -subgroup, P , of G . Let

$$\{P_1, P_2, \dots, P_r\} = \mathcal{S}$$

be the set of all conjugates of P (i.e., $\mathcal{S} = \{gPg^{-1} \mid g \in G\}$) and let Q be any p -subgroup of G . By definition of \mathcal{S} , G , hence also Q , acts by conjugation on \mathcal{S} . Write \mathcal{S} as a disjoint union of orbits under this action by Q :

$$\mathcal{S} = \mathcal{O}_1 \cup \mathcal{O}_2 \cup \dots \cup \mathcal{O}_s$$

where $r = |\mathcal{O}_1| + \dots + |\mathcal{O}_s|$. Keep in mind that r does not depend on Q but the number of Q -orbits s does (note that by definition, G has only one orbit on \mathcal{S} but a subgroup Q of G may have more than one orbit). Renumber the elements of \mathcal{S} if necessary so that the first s elements of \mathcal{S} are representatives of the Q -orbits: $P_i \in \mathcal{O}_i$, $1 \leq i \leq s$. It follows from Proposition 2 that $|\mathcal{O}_i| = |Q : N_Q(P_i)|$. By definition, $N_Q(P_i) = N_G(P_i) \cap Q$ and by Lemma 19, $N_G(P_i) \cap Q = P_i \cap Q$. Combining these two facts gives

$$|\mathcal{O}_i| = |Q : P_i \cap Q|, \quad 1 \leq i \leq s. \quad (4.1)$$

We are now in a position to prove that $r \equiv 1 \pmod{p}$. Since Q was arbitrary we may take $Q = P_1$ above, so that (1) gives

$$|\mathcal{O}_1| = 1.$$

Now, for all $i > 1$, $P_1 \neq P_i$, so $P_1 \cap P_i < P_1$. By (1)

$$|\mathcal{O}_i| = |P_1 : P_1 \cap P_i| > 1, \quad 2 \leq i \leq s.$$

Since P_1 is a p -group, $|P_1 : P_1 \cap P_i|$ must be a power of p , so that

$$p \mid |\mathcal{O}_i|, \quad 2 \leq i \leq s.$$

Thus

$$r = |\mathcal{O}_1| + (|\mathcal{O}_2| + \dots + |\mathcal{O}_s|) \equiv 1 \pmod{p}.$$

We now prove parts (2) and (3). Let Q be any p -subgroup of G . Suppose Q is not contained in P_i for any $i \in \{1, 2, \dots, r\}$ (i.e., $Q \not\leq gP_1g^{-1}$ for any $g \in G$). In this situation, $Q \cap P_i < Q$ for all i , so by (1)

$$|\mathcal{O}_i| = |Q : Q \cap P_i| > 1, \quad 1 \leq i \leq s.$$

Thus $p \mid |\mathcal{O}_i|$ for all i , so p divides $|\mathcal{O}_1| + \dots + |\mathcal{O}_s| = r$. This contradicts the fact that $r \equiv 1 \pmod{p}$ (remember, r does not depend on the choice of Q). This contradiction proves $Q \leq gP_1g^{-1}$ for some $g \in G$.

To see that all Sylow p -subgroups of G are conjugate, let Q be any Sylow p -subgroup of G . By the preceding argument, $Q \leq gP_1g^{-1}$ for some $g \in G$. Since $|gP_1g^{-1}| = |Q| = p^\alpha$, we must have $gP_1g^{-1} = Q$. This establishes part (2) of the theorem. In particular, $\mathcal{S} = \text{Syl}_p(G)$ since every Sylow p -subgroup of G is conjugate to P , and so $n_p = r \equiv 1 \pmod{p}$, which is the first part of (3).

Finally, since all Sylow p -subgroups are conjugate, Proposition 6 shows that

$$n_p = |G : N_G(P)| \quad \text{for any } P \in \text{Syl}_p(G),$$

completing the proof of Sylow's Theorem.

Note that the conjugacy part of Sylow's Theorem together with Corollary 14 shows that *any two Sylow p -subgroups of a group (for the same prime p) are isomorphic*.

Corollary 20. Let P be a Sylow p -subgroup of G . Then the following are equivalent:

- (1) P is the unique Sylow p -subgroup of G , i.e., $n_p = 1$
- (2) P is normal in G
- (3) P is characteristic in G
- (4) All subgroups generated by elements of p -power order are p -groups, i.e., if X is any subset of G such that $|x|$ is a power of p for all $x \in X$, then $\langle X \rangle$ is a p -group.

Proof: If (1) holds, then $gPg^{-1} = P$ for all $g \in G$ since $gPg^{-1} \in Syl_p(G)$, i.e., P is normal in G . Hence (1) implies (2). Conversely, if $P \trianglelefteq G$ and $Q \in Syl_p(G)$, then by Sylow's Theorem there exists $g \in G$ such that $Q = gPg^{-1} = P$. Thus $Syl_p(G) = \{P\}$ and (2) implies (1).

Since characteristic subgroups are normal, (3) implies (2). Conversely, if $P \trianglelefteq G$, we just proved P is the unique subgroup of G of order p^α , hence $P \operatorname{char} G$. Thus (2) and (3) are equivalent.

Finally, assume (1) holds and suppose X is a subset of G such that $|x|$ is a power of p for all $x \in X$. By the conjugacy part of Sylow's Theorem, for each $x \in X$ there is some $g \in G$ such that $x \in gPg^{-1} = P$. Thus $X \subseteq P$, and so $\langle X \rangle \leq P$, and $\langle X \rangle$ is a p -group. Conversely, if (4) holds, let X be the union of all Sylow p -subgroups of G . If P is any Sylow p -subgroup, P is a subgroup of the p -group $\langle X \rangle$. Since P is a p -subgroup of G of maximal order, we must have $P = \langle X \rangle$, so (1) holds.

Examples

Let G be a finite group and let p be a prime.

- (1) If p does not divide the order of G , the Sylow p -subgroup of G is the trivial group (and all parts of Sylow's Theorem hold trivially). If $|G| = p^\alpha$, G is the unique Sylow p -subgroup of G .
- (2) A finite abelian group has a unique Sylow p -subgroup for each prime p . This subgroup consists of all elements x whose order is a power of p . This is sometimes called the *p -primary component* of the abelian group.
- (3) S_3 has three Sylow 2-subgroups: $\langle (1 2) \rangle$, $\langle (2 3) \rangle$ and $\langle (1 3) \rangle$. It has a unique (hence normal) Sylow 3-subgroup: $\langle (1 2 3) \rangle = A_3$. Note that $3 \equiv 1 \pmod{2}$.
- (4) A_4 has a unique Sylow 2-subgroup: $\langle (1 2)(3 4), (1 3)(2 4) \rangle \cong V_4$. It has four Sylow 3-subgroups: $\langle (1 2 3) \rangle$, $\langle (1 2 4) \rangle$, $\langle (1 3 4) \rangle$ and $\langle (2 3 4) \rangle$. Note that $4 \equiv 1 \pmod{3}$.
- (5) S_4 has $n_2 = 3$ and $n_3 = 4$. Since S_4 contains a subgroup isomorphic to D_8 , every Sylow 2-subgroup of S_4 is isomorphic to D_8 .

Applications of Sylow's Theorem

We now give some applications of Sylow's Theorem. Most of the examples use Sylow's Theorem to prove that a group of a particular order is not simple. After discussing methods of constructing larger groups from smaller ones (for example, the formation of semidirect products) we shall be able to use these results to classify groups of some specific orders n (as we already did for $n = 15$).

Since Sylow's Theorem ensures the existence of p -subgroups of a finite group, it is worthwhile to study groups of prime power order more closely. This will be done in Chapter 6 and many more applications of Sylow's Theorem will be discussed there.

For groups of small order, the congruence condition of Sylow's Theorem alone is often sufficient to force the existence of a *normal* subgroup. The first step in any numerical application of Sylow's Theorem is to factor the group order into prime powers. The largest prime divisors of the group order tend to give the fewest possible values for n_p (for example, the congruence condition on n_2 gives no restriction whatsoever), which limits the structure of the group G . In the following examples we shall see situations where Sylow's Theorem alone does not force the existence of a normal subgroup, however some additional argument (often involving studying the elements of order p for a number of different primes p) proves the existence of a normal Sylow subgroup.

Example: (Groups of order pq , p and q primes with $p < q$)

Suppose $|G| = pq$ for primes p and q with $p < q$. Let $P \in Syl_p(G)$ and let $Q \in Syl_q(G)$. We show that Q is normal in G and if P is also normal in G , then G is cyclic.

Now the three conditions: $n_q = 1 + kq$ for some $k \geq 0$, n_q divides p and $p < q$, together force $k = 0$. Since $n_q = 1$, $Q \trianglelefteq G$.

Since n_p divides the prime q , the only possibilities are $n_p = 1$ or q . In particular, if $p \nmid q - 1$, (that is, if $q \not\equiv 1 \pmod{p}$), then n_p cannot equal q , so $P \trianglelefteq G$.

Let $P = \langle x \rangle$ and $Q = \langle y \rangle$. If $P \trianglelefteq G$, then since $G/C_G(P)$ is isomorphic to a subgroup of $\text{Aut}(Z_p)$ and the latter group has order $p - 1$, Lagrange's Theorem together with the observation that neither p nor q can divide $p - 1$ implies that $G = C_G(P)$. In this case $x \in P \leq Z(G)$ so x and y commute. (Alternatively, this follows immediately from Exercise 42 of Section 3.1.) This means $|xy| = pq$ (cf. the exercises in Section 2.3), hence in this case G is cyclic: $G \cong Z_{pq}$.

If $p \mid q - 1$, we shall see in Chapter 5 that there is a unique non-abelian group of order pq (in which, necessarily, $n_p = q$). We can prove the existence of this group now. Let Q be a Sylow q -subgroup of the symmetric group of degree q , S_q . By Exercise 34 in Section 3, $|N_{S_q}(Q)| = q(q - 1)$. By assumption, $p \mid q - 1$ so by Cauchy's Theorem $N_{S_q}(Q)$ has a subgroup, P , of order p . By Corollary 15 in Section 3.2, PQ is a group of order pq . Since $C_{S_q}(Q) = Q$ (Example 2, Section 3), PQ is a non-abelian group. The essential ingredient in the uniqueness proof of PQ is Theorem 17 on the cyclicity of $\text{Aut}(Z_q)$.

Example: (Groups of order 30)

Let G be a group of order 30. We show that G has a normal subgroup isomorphic to Z_{15} . We shall use this information to classify groups of order 30 in the next chapter. Note that any subgroup of order 15 is necessarily normal (since it is of index 2) and cyclic (by the preceding result) so it is only necessary to show there exists a subgroup of order 15. The quickest way of doing this is to quote Exercise 13 in Section 2. We give an alternate argument which illustrates how Sylow's Theorem can be used in conjunction with a counting of elements of prime order to produce a normal subgroup.

Let $P \in Syl_5(G)$ and let $Q \in Syl_3(G)$. If either P or Q is normal in G , by Corollary 15, Chapter 3, PQ is a group of order 15. Note also that if either P or Q is normal, then both P and Q are characteristic subgroups of PQ , and since $PQ \trianglelefteq G$, both P and Q are normal in G (Exercise 8(a), Section 4). Assume therefore that neither Sylow subgroup is normal. The only possibilities by Part 3 of Sylow's Theorem are $n_5 = 6$ and $n_3 = 10$. Each element of order 5 lies in a Sylow 5-subgroup, each Sylow 5-subgroup contains 4 nonidentity elements and, by Lagrange's Theorem, distinct Sylow 5-subgroups intersect in the identity. Thus the number of elements of order 5 in G is the number of nonidentity elements in one Sylow 5-subgroup times the number of Sylow 5-subgroups. This would

be $4 \cdot 6 = 24$ elements of order 5. By similar reasoning, the number of elements of order 3 would be $2 \cdot 10 = 20$. This is absurd since a group of order 30 cannot contain $24 + 20 = 44$ distinct elements. One of P or Q (hence both) must be normal in G .

This sort of counting technique is frequently useful (cf. also Section 6.2) and works particularly well when the Sylow p -subgroups have order p (as in this example), since then the intersection of two distinct Sylow p -subgroups must be the identity. If the order of the Sylow p -subgroup is p^α with $\alpha \geq 2$, greater care is required in counting elements, since in this case distinct Sylow p -subgroups may have many more elements in common, i.e., the intersection may be nontrivial.

Example: (Groups of order 12)

Let G be a group of order 12. We show that either G has a normal Sylow 3-subgroup or $G \cong A_4$ (in the latter case G has a normal Sylow 2-subgroup). We shall use this information to classify groups of order 12 in the next chapter.

Suppose $n_3 \neq 1$ and let $P \in \text{Syl}_3(G)$. Since $n_3 \mid 4$ and $n_3 \equiv 1 \pmod{3}$, it follows that $n_3 = 4$. Since distinct Sylow 3-subgroups intersect in the identity and each contains two elements of order 3, G contains $2 \cdot 4 = 8$ elements of order 3. Since $|G : N_G(P)| = n_3 = 4$, $N_G(P) = P$. Now G acts by conjugation on its four Sylow 3-subgroups, so this action affords a permutation representation

$$\varphi : G \rightarrow S_4$$

(note that we could also act by left multiplication on the left cosets of P and use Theorem 3). The kernel K of this action is the subgroup of G which normalizes all Sylow 3-subgroups of G . In particular, $K \leq N_G(P) = P$. Since P is not normal in G by assumption, $K = 1$, i.e., φ is injective and

$$G \cong \varphi(G) \leq S_4.$$

Since G contains 8 elements of order 3 and there are precisely 8 elements of order 3 in S_4 , all contained in A_4 , it follows that $\varphi(G)$ intersects A_4 in a subgroup of order at least 8. Since both groups have order 12 it follows that $\varphi(G) = A_4$, so that $G \cong A_4$.

Note that A_4 does indeed have 4 Sylow 3-subgroups (see Example 4 following Corollary 20), so that such a group G does exist. Also, let V be a Sylow 2-subgroup of A_4 . Since $|V| = 4$, it contains all of the remaining elements of A_4 . In particular, there cannot be another Sylow 2-subgroup. Thus $n_2(A_4) = 1$, i.e., $V \trianglelefteq A_4$ (which one can also see directly because V is the identity together with the three elements of S_4 which are products of two disjoint transpositions, that is, V is a union of conjugacy classes).

Example: (Groups of order p^2q , p and q distinct primes)

Let G be a group of order p^2q . We show that G has a normal Sylow subgroup (for either p or q). We shall use this information to classify some groups of this order in the next chapter (cf. Exercises 8 to 12 of Section 5.5). Let $P \in \text{Syl}_p(G)$ and let $Q \in \text{Syl}_q(G)$.

Consider first when $p > q$. Since $n_p \mid q$ and $n_p = 1 + kp$, we must have $n_p = 1$. Thus $P \trianglelefteq G$.

Consider now the case $p < q$. If $n_q = 1$, Q is normal in G . Assume therefore that $n_q > 1$, i.e., $n_q = 1 + tq$, for some $t > 0$. Now n_q divides p^2 so $n_q = p$ or p^2 . Since $q > p$ we cannot have $n_q = p$, hence $n_q = p^2$. Thus

$$tq = p^2 - 1 = (p - 1)(p + 1).$$

Since q is prime, either $q \mid p - 1$ or $q \mid p + 1$. The former is impossible since $q > p$ so the latter holds. Since $q > p$ but $q \mid p + 1$, we must have $q = p + 1$. This forces $p = 2$, $q = 3$ and $|G| = 12$. The result now follows from the preceding example.

Groups of Order 60

We illustrate how Sylow's Theorems can be used to unravel the structure of groups of a given order even if some groups of that order may be simple. Note the technique of changing from one prime to another and the inductive process where we use results on groups of order < 60 to study groups of order 60.

Proposition 21. If $|G| = 60$ and G has more than one Sylow 5-subgroup, then G is simple.

Proof: Suppose by way of contradiction that $|G| = 60$ and $n_5 > 1$ but that there exists H a normal subgroup of G with $H \neq 1$ or G . By Sylow's Theorem the only possibility for n_5 is 6. Let $P \in \text{Syl}_5(G)$, so that $|N_G(P)| = 10$ since its index is n_5 .

If $5 \mid |H|$ then H contains a Sylow 5-subgroup of G and since H is normal, it contains all 6 conjugates of this subgroup. In particular, $|H| \geq 1 + 6 \cdot 4 = 25$, and the only possibility is $|H| = 30$. This leads to a contradiction since a previous example proved that any group of order 30 has a normal (hence unique) Sylow 5-subgroup. This argument shows 5 does not divide $|H|$ for any proper normal subgroup H of G .

If $|H| = 6$ or 12, H has a normal, hence characteristic, Sylow subgroup, which is therefore also normal in G . Replacing H by this subgroup if necessary, we may assume $|H| = 2, 3$ or 4. Let $\bar{G} = G/H$, so $|\bar{G}| = 30, 20$ or 15. In each case, \bar{G} has a normal subgroup \bar{P} of order 5 by previous results. If we let H_1 be the complete preimage of \bar{P} in G , then $H_1 \trianglelefteq G$, $H_1 \neq G$ and $5 \mid |H_1|$. This contradicts the preceding paragraph and so completes the proof.

Corollary 22. A_5 is simple.

Proof: The subgroups $\langle (1\ 2\ 3\ 4\ 5) \rangle$ and $\langle (1\ 3\ 2\ 4\ 5) \rangle$ are distinct Sylow 5-subgroups of A_5 so the result follows immediately from the proposition.

The next proposition shows that there is a unique simple group of order 60.

Proposition 23. If G is a simple group of order 60, then $G \cong A_5$.

Proof: Let G be a simple group of order 60, so $n_2 = 3, 5$ or 15. Let $P \in \text{Syl}_2(G)$ and let $N = N_G(P)$, so $|G : N| = n_2$.

First observe that G has no proper subgroup H of index less than 5, as follows: if H were a subgroup of G of index 4, 3 or 2, then, by Theorem 3, G would have a normal subgroup K contained in H with G/K isomorphic to a subgroup of S_4 , S_3 or S_2 . Since $K \neq G$, simplicity forces $K = 1$. This is impossible since $60 (= |G|)$ does not divide $4!$. This argument shows, in particular, that $n_2 \neq 3$.

If $n_2 = 5$, then N has index 5 in G so the action of G by left multiplication on the set of left cosets of N gives a permutation representation of G into S_5 . Since (as

above) the kernel of this representation is a proper normal subgroup and G is simple, the kernel is 1 and G is isomorphic to a subgroup of S_5 . Identify G with this isomorphic copy so that we may assume $G \leq S_5$. If G is not contained in A_5 , then $S_5 = GA_5$ and, by the Second Isomorphism Theorem, $A_5 \cap G$ is of index 2 in G . Since G has no (normal) subgroup of index 2, this is a contradiction. This argument proves $G \leq A_5$. Since $|G| = |A_5|$, the isomorphic copy of G in S_5 coincides with A_5 , as desired.

Finally, assume $n_2 = 15$. If for every pair of distinct Sylow 2-subgroups P and Q of G , $P \cap Q = 1$, then the number of nonidentity elements in Sylow 2-subgroups of G would be $(4 - 1) \cdot 15 = 45$. But $n_5 = 6$ so the number of elements of order 5 in G is $(5 - 1) \cdot 6 = 24$, accounting for 69 elements. This contradiction proves that there exist distinct Sylow 2-subgroups P and Q with $|P \cap Q| = 2$. Let $M = N_G(P \cap Q)$. Since P and Q are abelian (being groups of order 4), P and Q are subgroups of M and since G is simple, $M \neq G$. Thus 4 divides $|M|$ and $|M| > 4$ (otherwise, $P = M = Q$). The only possibility is $|M| = 12$, i.e., M has index 5 in G (recall M cannot have index 3 or 1). But now the argument of the preceding paragraph applied to M in place of N gives $G \cong A_5$. This leads to a contradiction in this case because $n_2(A_5) = 5$ (cf. the exercises). The proof is complete.

EXERCISES

Let G be a finite group and let p be a prime.

1. Prove that if $P \in \text{Syl}_p(G)$ and H is a subgroup of G containing P then $P \in \text{Syl}_p(H)$. Give an example to show that, in general, a Sylow p -subgroup of a subgroup of G need not be a Sylow p -subgroup of G .
2. Prove that if H is a subgroup of G and $Q \in \text{Syl}_p(H)$ then $gQg^{-1} \in \text{Syl}_p(gHg^{-1})$ for all $g \in G$.
3. Use Sylow's Theorem to prove Cauchy's Theorem. (Note that we only used Cauchy's Theorem for abelian groups — Proposition 3.21 — in the proof of Sylow's Theorem so this line of reasoning is not circular.)
4. Exhibit all Sylow 2-subgroups and Sylow 3-subgroups of D_{12} and $S_3 \times S_3$.
5. Show that a Sylow p -subgroup of D_{2n} is cyclic and normal for every odd prime p .
6. Exhibit all Sylow 3-subgroups of A_4 and all Sylow 3-subgroups of S_4 .
7. Exhibit all Sylow 2-subgroups of S_4 and find elements of S_4 which conjugate one of these into each of the others.
8. Exhibit two distinct Sylow 2-subgroups of S_5 and an element of S_5 that conjugates one into the other.
9. Exhibit all Sylow 3-subgroups of $SL_2(\mathbb{F}_3)$ (cf. Exercise 9, Section 2.1).
10. Prove that the subgroup of $SL_2(\mathbb{F}_3)$ generated by $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ is the unique Sylow 2-subgroup of $SL_2(\mathbb{F}_3)$ (cf. Exercise 10, Section 2.4).
11. Show that the center of $SL_2(\mathbb{F}_3)$ is the group of order 2 consisting of $\pm I$, where I is the identity matrix. Prove that $SL_2(\mathbb{F}_3)/Z(SL_2(\mathbb{F}_3)) \cong A_4$. [Use facts about groups of order 12.]
12. Let $2n = 2^ak$ where k is odd. Prove that the number of Sylow 2-subgroups of D_{2n} is k . [Prove that if $P \in \text{Syl}_2(D_{2n})$ then $N_{D_{2n}}(P) = P$.]

13. Prove that a group of order 56 has a normal Sylow p -subgroup for some prime p dividing its order.
14. Prove that a group of order 312 has a normal Sylow p -subgroup for some prime p dividing its order.
15. Prove that a group of order 351 has a normal Sylow p -subgroup for some prime p dividing its order.
16. Let $|G| = pqr$, where p, q and r are primes with $p < q < r$. Prove that G has a normal Sylow subgroup for either p, q or r .
17. Prove that if $|G| = 105$ then G has a normal Sylow 5-subgroup and a normal Sylow 7-subgroup.
18. Prove that a group of order 200 has a normal Sylow 5-subgroup.
19. Prove that if $|G| = 6545$ then G is not simple.
20. Prove that if $|G| = 1365$ then G is not simple.
21. Prove that if $|G| = 2907$ then G is not simple.
22. Prove that if $|G| = 132$ then G is not simple.
23. Prove that if $|G| = 462$ then G is not simple.
24. Prove that if G is a group of order 231 then $Z(G)$ contains a Sylow 11-subgroup of G and a Sylow 7-subgroup is normal in G .
25. Prove that if G is a group of order 385 then $Z(G)$ contains a Sylow 7-subgroup of G and a Sylow 11-subgroup is normal in G .
26. Let G be a group of order 105. Prove that if a Sylow 3-subgroup of G is normal then G is abelian.
27. Let G be a group of order 315 which has a normal Sylow 3-subgroup. Prove that $Z(G)$ contains a Sylow 3-subgroup of G and deduce that G is abelian.
28. Let G be a group of order 1575. Prove that if a Sylow 3-subgroup of G is normal then a Sylow 5-subgroup and a Sylow 7-subgroup are normal. In this situation prove that G is abelian.
29. If G is a non-abelian simple group of order < 100 , prove that $G \cong A_5$. [Eliminate all orders but 60.]
30. How many elements of order 7 must there be in a simple group of order 168?
31. For $p = 2, 3$ and 5 find $n_p(A_5)$ and $n_p(S_5)$. [Note that $A_4 \leq A_5$.]
32. Let P be a Sylow p -subgroup of H and let H be a subgroup of K . If $P \trianglelefteq H$ and $H \trianglelefteq K$, prove that P is normal in K . Deduce that if $P \in \text{Syl}_p(G)$ and $H = N_G(P)$, then $N_G(H) = H$ (in words: *normalizers of Sylow p -subgroups are self-normalizing*).
33. Let P be a normal Sylow p -subgroup of G and let H be any subgroup of G . Prove that $P \cap H$ is the unique Sylow p -subgroup of H .
34. Let $P \in \text{Syl}_p(G)$ and assume $N \trianglelefteq G$. Use the conjugacy part of Sylow's Theorem to prove that $P \cap N$ is a Sylow p -subgroup of N . Deduce that PN/N is a Sylow p -subgroup of G/N (note that this may also be done by the Second Isomorphism Theorem — cf. Exercise 9, Section 3.3).
35. Let $P \in \text{Syl}_p(G)$ and let $H \leq G$. Prove that $gPg^{-1} \cap H$ is a Sylow p -subgroup of H for some $g \in G$. Give an explicit example showing that $hPh^{-1} \cap H$ is not necessarily a Sylow p -subgroup of H for any $h \in H$ (in particular, we cannot always take $g = 1$ in the first part of this problem, as we could when H was normal in G).

36. Prove that if N is a normal subgroup of G then $n_p(G/N) \leq n_p(G)$.
37. Let R be a normal p -subgroup of G (not necessarily a Sylow subgroup).
- Prove that R is contained in every Sylow p -subgroup of G .
 - If S is another normal p -subgroup of G , prove that RS is also a normal p -subgroup of G .
 - The subgroup $O_p(G)$ is defined to be the group generated by all normal p -subgroups of G . Prove that $O_p(G)$ is the unique largest normal p -subgroup of G and $O_p(G)$ equals the intersection of all Sylow p -subgroups of G .
 - Let $\overline{G} = G/O_p(G)$. Prove that $O_p(\overline{G}) = \overline{1}$ (i.e., \overline{G} has no nontrivial normal p -subgroup).
38. Use the method of proof in Sylow's Theorem to show that if n_p is not congruent to $1(\text{mod } p^2)$ then there are distinct Sylow p -subgroups P and Q of G such that $|P : P \cap Q| = |Q : P \cap Q| = p$.
39. Show that the subgroup of strictly upper triangular matrices in $GL_n(\mathbb{F}_p)$ (cf. Exercise 17, Section 2.1) is a Sylow p -subgroup of this finite group. [Use the order formula in Section 1.4 to find the order of a Sylow p -subgroup of $GL_n(\mathbb{F}_p)$.]
40. Prove that the number of Sylow p -subgroups of $GL_2(\mathbb{F}_p)$ is $p + 1$. [Exhibit two distinct Sylow p -subgroups.]
41. Prove that $SL_2(\mathbb{F}_4) \cong A_5$ (cf. Exercise 9, Section 2.1 for the definition of $SL_2(\mathbb{F}_4)$).
42. Prove that the group of rigid motions in \mathbb{R}^3 of an icosahedron is isomorphic to A_5 . [Recall that the order of this group is 60: Exercise 13, Section 1.2.]
43. Prove that the group of rigid motions in \mathbb{R}^3 of a dodecahedron is isomorphic to A_5 . (As with the cube and the tetrahedron, the icosahedron and the dodecahedron are dual solids.) [Recall that the order of this group is 60: Exercise 12, Section 1.2.]
44. Let p be the smallest prime dividing the order of the finite group G . If $P \in Syl_p(G)$ and P is cyclic prove that $N_G(P) = C_G(P)$.
45. Find generators for a Sylow p -subgroup of S_{2p} , where p is an odd prime. Show that this is an abelian group of order p^2 .
46. Find generators for a Sylow p -subgroup of S_{p^2} , where p is a prime. Show that this is a non-abelian group of order p^{p+1} .
47. Write and execute a computer program which
 - gives each odd number $n < 10,000$ that is not a power of a prime and that has some prime divisor p such that n_p is not forced to be 1 for all groups of order n by the congruence condition of Sylow's Theorem, and
 - gives for each n in (i) the factorization of n into prime powers and gives the list of all permissible values of n_p for all primes p dividing n (i.e., those values not ruled out by Part 3 of Sylow's Theorem).
48. Carry out the same process as in the preceding exercise for all even numbers less than 1000. Explain the relative lengths of the lists versus the number of integers tested.
49. Prove that if $|G| = 2^n m$ where m is odd and G has a cyclic Sylow 2-subgroup then G has a normal subgroup of order m . [Use induction and Exercises 11 and 12 in Section 2.]
50. Prove that if U and W are normal subsets of a Sylow p -subgroup P of G then U is conjugate to W in G if and only if U is conjugate to W in $N_G(P)$. Deduce that two elements in the center of P are conjugate in G if and only if they are conjugate in $N_G(P)$. (A subset U of P is normal in P if $N_P(U) = P$.)

- 51.** Let P be a Sylow p -subgroup of G and let M be any subgroup of G which contains $N_G(P)$. Prove that $|G : M| \equiv 1 \pmod{p}$.

The following sequence of exercises leads to the classification of all numbers n with the property that every group of order n is cyclic (for example, $n = 15$ is such an integer). These arguments are a vastly simplified prototype for the proof that every group of odd order is solvable in the sense that they use the *structure* (commutativity) of the proper subgroups and their *embedding* in the whole group (we shall see that distinct maximal subgroups intersect in the identity) to obtain a contradiction by counting arguments. In the proof that groups of odd order are solvable one uses induction to reduce to the situation in which a minimal counterexample is a simple group — but here every proper subgroup is solvable (not abelian as in our situation). The analysis of the structure and embedding of the maximal subgroups in this situation is much more complicated and the counting arguments are (roughly speaking) replaced by character theory arguments (as will be discussed in Part VI).

- 52.** Suppose G is a finite simple group in which every proper subgroup is abelian. If M and N are distinct maximal subgroups of G prove $M \cap N = 1$. [See Exercise 23 in Section 3.]
- 53.** Use the preceding exercise to prove that if G is any non-abelian group in which every proper subgroup is abelian then G is not simple. [Let G be a counterexample to this assertion and use Exercise 24 in Section 3 to show that G has more than one conjugacy class of maximal subgroups. Use the method of Exercise 23 in Section 3 to count the elements which lie in all conjugates of M and N , where M and N are nonconjugate maximal subgroups of G ; show that this gives more than $|G|$ elements.]
- 54.** Prove the following classification: if G is a finite group of order $p_1 p_2 \dots p_r$ where the p_i 's are distinct primes such that p_i does not divide $p_j - 1$ for all i and j , then G is cyclic. [By induction, every proper subgroup of G is cyclic, so G is not simple by the preceding exercise. If N is a nontrivial proper normal subgroup, N is cyclic and G/N acts as automorphisms of N . Use Proposition 16 to show that $N \leq Z(G)$ and use induction to show $G/Z(G)$ is cyclic, hence G is abelian by Exercise 36 of Section 3.1.]
- 55.** Prove the converse to the preceding exercise: if $n \geq 2$ is an integer such that every group of order n is cyclic, then $n = p_1 p_2 \dots p_r$ is a product of distinct primes and p_i does not divide $p_j - 1$ for all i, j . [If n is not of this form, construct noncyclic groups of order n using direct products of noncyclic groups of order p^2 and pq , where $p \mid q - 1$.]
- 56.** If G is a finite group in which every proper subgroup is abelian, show that G is solvable.

4.6 THE SIMPLICITY OF A_n

There are a number of proofs of the simplicity of A_n , $n \geq 5$. The most elementary involves showing A_n is generated by 3-cycles. Then one shows that a normal subgroup must contain one 3-cycle hence must contain all the 3-cycles so cannot be a proper subgroup. We include a less computational approach.

Note that A_3 is an abelian simple group and that A_4 is not simple ($n_2(A_4) = 1$).

Theorem 24. A_n is simple for all $n \geq 5$.

Proof: By induction on n . The result has already been established for $n = 5$, so assume $n \geq 6$ and let $G = A_n$. Assume there exists $H \trianglelefteq G$ with $H \neq 1$ or G .

For each $i \in \{1, 2, \dots, n\}$ let G_i be the stabilizer of i in the natural action of G on $i \in \{1, 2, \dots, n\}$. Thus $G_i \leq G$ and $G_i \cong A_{n-1}$. By induction, G_i is simple for $1 \leq i \leq n$.

Suppose first that there is some $\tau \in H$ with $\tau \neq 1$ but $\tau(i) = i$ for some $i \in \{1, 2, \dots, n\}$. Since $\tau \in H \cap G_i$ and $H \cap G_i \trianglelefteq G_i$, by the simplicity of G_i we must have $H \cap G_i = G_i$, that is

$$G_i \leq H.$$

By Exercise 2 of Section 1, $\sigma G_i \sigma^{-1} = G_{\sigma(i)}$, so for all i , $\sigma G_i \sigma^{-1} \leq \sigma H \sigma^{-1} = H$. Thus

$$G_j \leq H, \quad \text{for all } j \in \{1, 2, \dots, n\}.$$

Any $\lambda \in A_n$ may be written as a product of an even number, $2t$, of transpositions, so

$$\lambda = \lambda_1 \lambda_2 \cdots \lambda_t,$$

where λ_k is a product of two transpositions. Since $n > 4$ each $\lambda_k \in G_j$, for some j , hence

$$G = \langle G_1, G_2, \dots, G_n \rangle \leq H,$$

which is a contradiction. Therefore if $\tau \neq 1$ is an element of H then $\tau(i) \neq i$ for all $i \in \{1, 2, \dots, n\}$, i.e., no nonidentity element of H fixes any element of $\{1, 2, \dots, n\}$.

It follows that if τ_1, τ_2 are elements of H with

$$\tau_1(i) = \tau_2(i) \text{ for some } i, \text{ then } \tau_1 = \tau_2 \tag{4.2}$$

since then $\tau_2^{-1} \tau_1(i) = i$.

Suppose there exists a $\tau \in H$ such that the cycle decomposition of τ contains a cycle of length ≥ 3 , say

$$\tau = (a_1 a_2 a_3 \dots)(b_1 b_2 \dots) \dots .$$

Let $\sigma \in G$ be an element with $\sigma(a_1) = a_1, \sigma(a_2) = a_2$ but $\sigma(a_3) \neq a_3$ (note that such a σ exists in A_n since $n \geq 5$). By Proposition 10

$$\tau_1 = \sigma \tau \sigma^{-1} = (a_1 a_2 \sigma(a_3) \dots)(\sigma(b_1) \sigma(b_2) \dots) \dots$$

so τ and τ_1 are distinct elements of H with $\tau(a_1) = \tau_1(a_1) = a_2$, contrary to (2). This proves that only 2-cycles can appear in the cycle decomposition of nonidentity elements of H .

Let $\tau \in H$ with $\tau \neq 1$, so that

$$\tau = (a_1 a_2)(a_3 a_4)(a_5 a_6) \dots$$

(note that $n \geq 6$ is used here). Let $\sigma = (a_1 a_2)(a_3 a_5) \in G$. Then

$$\tau_1 = \sigma \tau \sigma^{-1} = (a_1 a_2)(a_5 a_4)(a_3 a_6) \dots,$$

hence τ and τ_1 are distinct elements of H with $\tau(a_1) = \tau_1(a_1) = a_2$, again contrary to (2). This completes the proof of the simplicity of A_n .

EXERCISES

Let G be a group and let Ω be an infinite set.

1. Prove that A_n does not have a proper subgroup of index $< n$ for all $n \geq 5$.
2. Find all normal subgroups of S_n for all $n \geq 5$.
3. Prove that A_n is the only proper subgroup of index $< n$ in S_n for all $n \geq 5$.
4. Prove that A_n is generated by the set of all 3-cycles for each $n \geq 3$.
5. Prove that if there exists a chain of subgroups $G_1 \leq G_2 \leq \dots \leq G$ such that $G = \cup_{i=1}^{\infty} G_i$ and each G_i is simple then G is simple.
6. Let D be the subgroup of S_{Ω} consisting of permutations which move only a finite number of elements of Ω (described in Exercise 17 in Section 3) and let A be the set of all elements $\sigma \in D$ such that σ acts as an even permutation on the (finite) set of points it moves. Prove that A is an infinite simple group. [Show that every pair of elements of D lie in a finite simple subgroup of D .]
7. Under the notation of the preceding exercise prove that if $H \trianglelefteq S_{\Omega}$ and $H \neq 1$ then $A \leq H$, i.e., A is the unique (nontrivial) minimal normal subgroup of S_{Ω} .
8. Under the notation of the preceding two exercises prove that $|D| = |A| = |\Omega|$. Deduce that

$$\text{if } S_{\Omega} \cong S_{\Delta} \text{ then } |\Omega| = |\Delta|.$$

[Use the fact that D is generated by transpositions. You may assume that countable unions and finite direct products of sets of cardinality $|\Omega|$ also have cardinality $|\Omega|$.]

CHAPTER 5

Direct and Semidirect Products and Abelian Groups

In this chapter we consider two of the easier methods for constructing larger groups from smaller ones, namely the notions of direct and semidirect products. This allows us to state the Fundamental Theorem on Finitely Generated Abelian Groups, which in particular completely classifies all finite abelian groups.

5.1 DIRECT PRODUCTS

We begin with the definition of the direct product of a finite and of a countable number of groups (the direct product of an arbitrary collection of groups is considered in the exercises).

Definition.

- (1) The *direct product* $G_1 \times G_2 \times \dots \times G_n$ of the groups G_1, G_2, \dots, G_n with operations $\star_1, \star_2, \dots, \star_n$, respectively, is the set of n -tuples (g_1, g_2, \dots, g_n) where $g_i \in G_i$ with operation defined componentwise:

$$(g_1, g_2, \dots, g_n) \star (h_1, h_2, \dots, h_n) = (g_1 \star_1 h_1, g_2 \star_2 h_2, \dots, g_n \star_n h_n).$$

- (2) Similarly, the *direct product* $G_1 \times G_2 \times \dots$ of the groups G_1, G_2, \dots with operations \star_1, \star_2, \dots , respectively, is the set of sequences (g_1, g_2, \dots) where $g_i \in G_i$ with operation defined componentwise:

$$(g_1, g_2, \dots) \star (h_1, h_2, \dots) = (g_1 \star_1 h_1, g_2 \star_2 h_2, \dots).$$

Although the operations may be different in each of the factors of a direct product, we shall, as usual, write all abstract groups multiplicatively, so that the operation in (1) above, for example, becomes simply

$$(g_1, g_2, \dots, g_n)(h_1, h_2, \dots, h_n) = (g_1 h_1, g_2 h_2, \dots, g_n h_n).$$

Examples

- (1) Suppose $G_i = \mathbb{R}$ (operation addition) for $i = 1, 2, \dots, n$. Then $\mathbb{R} \times \mathbb{R} \times \dots \times \mathbb{R}$ (n -factors) is the familiar Euclidean n -space \mathbb{R}^n with usual vector addition:

$$(a_1, a_2, \dots, a_n) + (b_1, b_2, \dots, b_n) = (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n).$$

- (2) To illustrate that groups forming the direct product (and corresponding operations) may be completely general, let $G_1 = \mathbb{Z}$, let $G_2 = S_3$ and let $G_3 = GL_2(\mathbb{R})$, where the group operations are addition, composition, and matrix multiplication, respectively. Then the operation in $G_1 \times G_2 \times G_3$ is defined by

$$(n, \sigma, \begin{pmatrix} a & b \\ c & d \end{pmatrix})(m, \tau, \begin{pmatrix} p & q \\ r & s \end{pmatrix}) = (n+m, \sigma \circ \tau, \begin{pmatrix} ap+br & aq+bs \\ cp+dr & cq+ds \end{pmatrix}).$$

Proposition 1. If G_1, \dots, G_n are groups, their direct product is a group of order $|G_1| |G_2| \cdots |G_n|$ (if any G_i is infinite, so is the direct product).

Proof: Let $G = G_1 \times G_2 \times \dots \times G_n$. The proof that the group axioms hold for G is straightforward since each axiom is a consequence of the fact that the same axiom holds in each factor, G_i , and the operation on G is defined componentwise. For example, the associative law is verified as follows:

Let $(a_1, a_2, \dots, a_n), (b_1, b_2, \dots, b_n)$, and $(c_1, c_2, \dots, c_n) \in G$. Then

$$\begin{aligned} (a_1, a_2, \dots, a_n) & [(b_1, b_2, \dots, b_n)(c_1, c_2, \dots, c_n)] \\ &= (a_1, a_2, \dots, a_n)(b_1 c_1, b_2 c_2, \dots, b_n c_n) \\ &= (a_1(b_1 c_1), a_2(b_2 c_2), \dots, a_n(b_n c_n)) \\ &= ((a_1 b_1) c_1, (a_2 b_2) c_2, \dots, (a_n b_n) c_n) \\ &= [(a_1, a_2, \dots, a_n)(b_1, b_2, \dots, b_n)](c_1, c_2, \dots, c_n), \end{aligned}$$

where in the third step we have used the associative law in each component. The remaining verification that the direct product is a group is similar: the identity of G is the n -tuple $(1_1, 1_2, \dots, 1_n)$, where 1_i is the identity of G_i and the inverse of (g_1, g_2, \dots, g_n) is $(g_1^{-1}, g_2^{-1}, \dots, g_n^{-1})$, where g_i^{-1} is the inverse of g_i in G_i .

The formula for the order of G is clear.

If the factors of the direct product are rearranged, the resulting direct product is isomorphic to the original one (cf. Exercise 7).

The next proposition shows that a direct product, $G_1 \times G_2 \times \dots \times G_n$, contains an isomorphic copy of each G_i . One can think of these specific copies as the “coordinate axes” of the direct product since, in the case of $\mathbb{R} \times \mathbb{R}$, they coincide with the x and y axes. One should be careful, however, not to think of these “coordinate axes” as the *only* copies of the groups G_i in the direct product. For example in $\mathbb{R} \times \mathbb{R}$ any line through the origin is a subgroup of $\mathbb{R} \times \mathbb{R}$ isomorphic to \mathbb{R} (and $\mathbb{R} \times \mathbb{R}$ has infinitely many pairs of lines which are coordinate axes, viz. any rotation of a given coordinate system). The second part of the proposition shows that there are *projection homomorphisms* onto each of the components.

Proposition 2. Let G_1, G_2, \dots, G_n be groups and let $G = G_1 \times \cdots \times G_n$ be their direct product.

- (1) For each fixed i the set of elements of G which have the identity of G_j in the j^{th} position for all $j \neq i$ and arbitrary elements of G_i in position i is a subgroup of G isomorphic to G_i :

$$G_i \cong \{(1, 1, \dots, 1, g_i, 1, \dots, 1) \mid g_i \in G_i\},$$

(here g_i appears in the i^{th} position). If we identify G_i with this subgroup, then $G_i \trianglelefteq G$ and

$$G/G_i \cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n.$$

- (2) For each fixed i define $\pi_i : G \rightarrow G_i$ by

$$\pi_i((g_1, g_2, \dots, g_n)) = g_i.$$

Then π_i is a surjective homomorphism with

$$\begin{aligned} \ker \pi_i &= \{(g_1, \dots, g_{i-1}, 1, g_{i+1}, \dots, g_n) \mid g_j \in G_j \text{ for all } j \neq i\} \\ &\cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n \end{aligned}$$

(here the 1 appears in position i).

- (3) Under the identifications in part (1), if $x \in G_i$ and $y \in G_j$ for some $i \neq j$, then $xy = yx$.

Proof: (1) Since the operation in G is defined componentwise, it follows easily from the subgroup criterion that $\{(1, 1, \dots, 1, g_i, 1, \dots, 1) \mid g_i \in G_i\}$ is a subgroup of G . Furthermore, the map $g_i \mapsto (1, 1, \dots, 1, g_i, 1, \dots, 1)$ is seen to be an isomorphism of G_i with this subgroup. Identify G_i with this isomorphic copy in G .

To prove the remaining parts of (1) consider the map

$$\varphi : G \longrightarrow G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n$$

defined by

$$\varphi(g_1, g_2, \dots, g_n) = (g_1, \dots, g_{i-1}, g_{i+1}, \dots, g_n)$$

(i.e., φ erases the i^{th} component of G). The map φ is a homomorphism since

$$\begin{aligned} \varphi((g_1, \dots, g_n)(h_1, \dots, h_n)) &= \varphi((g_1 h_1, \dots, g_n h_n)) \\ &= (g_1 h_1, \dots, g_{i-1} h_{i-1}, g_{i+1} h_{i+1}, \dots, g_n h_n) \\ &= (g_1, \dots, g_{i-1}, g_{i+1}, \dots, g_n)(h_1, \dots, h_{i-1}, h_{i+1}, \dots, h_n) \\ &= \varphi((g_1, \dots, g_n))\varphi((h_1, \dots, h_n)). \end{aligned}$$

Since the entries in position j are arbitrary elements of G_j for all j , φ is surjective. Furthermore,

$$\ker \varphi = \{(g_1, \dots, g_n) \mid g_j = 1 \text{ for all } j \neq i\} = G_i.$$

This proves that G_i is a normal subgroup of G (in particular, it again proves this copy of G_i is a subgroup) and the First Isomorphism Theorem gives the final assertion of part (1).

In (2) the argument that π_i is a surjective homomorphism and the kernel is the subgroup described is very similar to that in part (1), so the details are left to the reader.

In part (3) if $x = (1, \dots, 1, g_i, 1, \dots, 1)$ and $y = (1, \dots, 1, g_j, 1, \dots, 1)$, where the indicated entries appear in positions i, j respectively, then

$$xy = (1, \dots, 1, g_i, 1, \dots, 1, g_j, 1, \dots, 1) = yx$$

(where the notation is chosen so that $i < j$). This completes the proof.

A generalization of this proposition appears as Exercise 2.

We shall continue to identify the “coordinate axis” subgroups described in part (1) of the proposition with their isomorphic copies, the G_i ’s. The i^{th} such subgroup is often called the i^{th} *component* or i^{th} *factor* of G . For instance, when we wish to calculate in $Z_n \times Z_m$ we can let x be a generator of the first factor, let y be a generator of the second factor and write the elements of $Z_n \times Z_m$ in the form $x^a y^b$. This replaces the formal ordered pairs $(x, 1)$ and $(1, y)$ with x and y (so $x^a y^b$ replaces (x^a, y^b)).

Examples

- (1) Under the notation of Proposition 2 it follows from part (3) that if $x_i \in G_i$, $1 \leq i \leq n$, then for all $k \in \mathbb{Z}$

$$(x_1 x_2 \dots x_n)^k = x_1^k x_2^k \dots x_n^k.$$

Since the order of $x_1 x_2 \dots x_n$ is the smallest positive integer k such that $x_i^k = 1$ for all i , we see that

$$|x_1 x_2 \dots x_n| = \text{l.c.m.}(|x_1|, |x_2|, \dots, |x_n|)$$

(where this order is infinite if and only if one of the x_i ’s has infinite order).

- (2) Let p be a prime and for $n \in \mathbb{Z}^+$ consider

$$E_{p^n} = Z_p \times Z_p \times \dots \times Z_p \quad (n \text{ factors}).$$

Then E_{p^n} is an abelian group of order p^n with the property that $x^p = 1$ for all $x \in E_{p^n}$. This group is the *elementary abelian* group of order p^n described in Section 4.4.

- (3) For p a prime, we show that the elementary abelian group of order p^2 has exactly $p+1$ subgroups of order p (in particular, there are more than the two obvious ones). Let $E = E_{p^2}$. Since each nonidentity element of E has order p , each of these generates a cyclic subgroup of E of order p . By Lagrange’s Theorem distinct subgroups of order p intersect trivially. Thus the $p^2 - 1$ nonidentity elements of E are partitioned into subsets of size $p - 1$ (i.e., each of these subsets consists of the nonidentity elements of some subgroup of order p). There must therefore be

$$\frac{p^2 - 1}{p - 1} = p + 1$$

subgroups of order p . When $p = 2$, E is the Klein 4-group which we have already seen has 3 subgroups of order 2 (cf. also Exercises 10 and 11).

EXERCISES

1. Show that the center of a direct product is the direct product of the centers:

$$Z(G_1 \times G_2 \times \cdots \times G_n) = Z(G_1) \times Z(G_2) \times \cdots \times Z(G_n).$$

Deduce that a direct product of groups is abelian if and only if each of the factors is abelian.

2. Let G_1, G_2, \dots, G_n be groups and let $G = G_1 \times \cdots \times G_n$. Let I be a proper, nonempty subset of $\{1, \dots, n\}$ and let $J = \{1, \dots, n\} - I$. Define G_I to be the set of elements of G that have the identity of G_j in position j for all $j \in J$.

(a) Prove that G_I is isomorphic to the direct product of the groups $G_i, i \in I$.

(b) Prove that G_I is a normal subgroup of G and $G/G_I \cong G_J$.

(c) Prove that $G \cong G_I \times G_J$.

3. Under the notation of the preceding exercise let I and K be any disjoint nonempty subsets of $\{1, 2, \dots, n\}$ and let G_I and G_K be the subgroups of G defined above. Prove that $xy = yx$ for all $x \in G_I$ and all $y \in G_K$.

4. Let A and B be finite groups and let p be a prime. Prove that any Sylow p -subgroup of $A \times B$ is of the form $P \times Q$, where $P \in Syl_p(A)$ and $Q \in Syl_p(B)$. Prove that $n_p(A \times B) = n_p(A)n_p(B)$. Generalize both of these results to a direct product of any finite number of finite groups (so that the number of Sylow p -subgroups of a direct product is the product of the numbers of Sylow p -subgroups of the factors).

5. Exhibit a nonnormal subgroup of $Q_8 \times Z_4$ (note that every subgroup of each factor is normal).

6. Show that all subgroups of $Q_8 \times E_{2^n}$ are normal.

7. Let G_1, G_2, \dots, G_n be groups and let π be a fixed element of S_n . Prove that the map

$$\varphi_\pi : G_1 \times G_2 \times \cdots \times G_n \rightarrow G_{\pi^{-1}(1)} \times G_{\pi^{-1}(2)} \times \cdots \times G_{\pi^{-1}(n)}$$

defined by

$$\varphi_\pi(g_1, g_2, \dots, g_n) = (g_{\pi^{-1}(1)}, g_{\pi^{-1}(2)}, \dots, g_{\pi^{-1}(n)})$$

is an isomorphism (so that changing the order of the factors in a direct product does not change the isomorphism type).

8. Let $G_1 = G_2 = \cdots = G_n$ and let $G = G_1 \times \cdots \times G_n$. Under the notation of the preceding exercise show that $\varphi_\pi \in \text{Aut}(G)$. Show also that the map $\pi \mapsto \varphi_\pi$ is an injective homomorphism of S_n into $\text{Aut}(G)$. (In particular, $\varphi_{\pi_1} \circ \varphi_{\pi_2} = \varphi_{\pi_1 \pi_2}$. It is at this point that the π^{-1} 's in the definition of φ_π are needed. The underlying reason for this is because if e_i is the n -tuple with 1 in position i and zeros elsewhere, $1 \leq i \leq n$, then S_n acts on $\{e_1, \dots, e_n\}$ by $\pi \cdot e_i = e_{\pi(i)}$; this is a left group action. If the n -tuple (g_1, \dots, g_n) is represented by $g_1 e_1 + \cdots + g_n e_n$, then this left group action on $\{e_1, \dots, e_n\}$ extends to a left group action on sums by

$$\pi \cdot (g_1 e_1 + g_2 e_2 + \cdots + g_n e_n) = g_1 e_{\pi(1)} + g_2 e_{\pi(2)} + \cdots + g_n e_{\pi(n)}.$$

The coefficient of $e_{\pi(i)}$ on the right hand side is g_i , so the coefficient of e_i is $g_{\pi^{-1}(i)}$. Thus the right hand side may be rewritten as $g_{\pi^{-1}(1)} e_1 + g_{\pi^{-1}(2)} e_2 + \cdots + g_{\pi^{-1}(n)} e_n$, which is precisely the sum attached to the n -tuple $(g_{\pi^{-1}(1)}, g_{\pi^{-1}(2)}, \dots, g_{\pi^{-1}(n)})$. In other words, any permutation of the “position vectors” e_1, \dots, e_n (which fixes their coefficients) is the same as the inverse permutation on the coefficients (fixing the e_i 's). If one uses π 's in place of π^{-1} 's in the definition of φ_π then the map $\pi \mapsto \varphi_\pi$ is not necessarily a homomorphism — it corresponds to a *right* group action.)

9. Let G_i be a field F for all i and use the preceding exercise to show that the set of $n \times n$ matrices with one 1 in each row and each column is a subgroup of $GL_n(F)$ isomorphic to S_n (these matrices are called *permutation matrices* since they simply permute the standard basis e_1, \dots, e_n (as above) of the n -dimensional vector space $F \times F \times \dots \times F$).
10. Let p be a prime. Let A and B be two cyclic groups of order p with generators x and y , respectively. Set $E = A \times B$ so that E is the elementary abelian group of order p^2 : E_{p^2} . Prove that the distinct subgroups of E of order p are

$$\langle x \rangle, \quad \langle xy \rangle, \quad \langle xy^2 \rangle, \quad \dots, \quad \langle xy^{p-1} \rangle, \quad \langle y \rangle$$

(note that there are $p + 1$ of them).

11. Let p be a prime and let $n \in \mathbb{Z}^+$. Find a formula for the number of subgroups of order p in the elementary abelian group E_{p^n} .
12. Let A and B be groups. Assume $Z(A)$ contains a subgroup Z_1 and $Z(B)$ contains a subgroup Z_2 with $Z_1 \cong Z_2$. Let this isomorphism be given by the map $x_i \mapsto y_i$ for all $x_i \in Z_1$. A *central product* of A and B is a quotient

$$(A \times B)/Z \quad \text{where} \quad Z = \{(x_i, y_i^{-1}) \mid x_i \in Z_1\}$$

and is denoted by $A * B$ — it is not unique since it depends on Z_1 , Z_2 and the isomorphism between them. (Think of $A * B$ as the direct product of A and B “collapsed” by identifying each element $x_i \in Z_1$ with its corresponding element $y_i \in Z_2$.)

- (a) Prove that the images of A and B in the quotient group $A * B$ are isomorphic to A and B , respectively, and that these images intersect in a central subgroup isomorphic to Z_1 . Find $|A * B|$.
- (b) Let $Z_4 = \langle x \rangle$. Let $D_8 = \langle r, s \rangle$ and $Q_8 = \langle i, j \rangle$ be given by their usual generators and relations. Let $Z_4 * D_8$ be the central product of Z_4 and D_8 which identifies x^2 and r^2 (i.e., $Z_1 = \langle x^2 \rangle$, $Z_2 = \langle r^2 \rangle$ and the isomorphism is $x^2 \mapsto r^2$) and let $Z_4 * Q_8$ be the central product of Z_4 and Q_8 which identifies x^2 and -1 . Prove that $Z_4 * D_8 \cong Z_4 * Q_8$.
13. Give presentations for the groups $Z_4 * D_8$ and $Z_4 * Q_8$ constructed in the preceding exercise.
14. Let $G = A_1 \times A_2 \times \dots \times A_n$ and for each i let B_i be a normal subgroup of A_i . Prove that $B_1 \times B_2 \times \dots \times B_n \trianglelefteq G$ and that

$$(A_1 \times A_2 \times \dots \times A_n)/(B_1 \times B_2 \times \dots \times B_n) \cong (A_1/B_1) \times (A_2/B_2) \times \dots \times (A_n/B_n).$$

The following exercise describes the direct product of an arbitrary collection of groups. The terminology for the Cartesian product of an arbitrary collection of sets may be found in the Appendix.

15. Let I be any nonempty index set and let (G_i, \star_i) be a group for each $i \in I$. The *direct product* of the groups G_i , $i \in I$ is the set $G = \prod_{i \in I} G_i$ (the Cartesian product of the G_i 's) with a binary operation defined as follows: if $\prod a_i$ and $\prod b_i$ are elements of G , then their product in G is given by

$$\left(\prod_{i \in I} a_i \right) \left(\prod_{i \in I} b_i \right) = \prod_{i \in I} (a_i \star_i b_i)$$

(i.e., the group operation in the direct product is defined componentwise).

- (a) Show that this binary operation is well defined and associative.
- (b) Show that the element $\prod 1_i$ satisfies the axiom for the identity of G , where 1_i is the identity of G_i for all i .

- (c) Show that the element $\prod a_i^{-1}$ is the inverse of $\prod a_i$, where the inverse of each component element a_i is taken in the group G_i .

Conclude that the direct product is a group.

(Note that if $I = \{1, 2, \dots, n\}$, this definition of the direct product is the same as the n -tuple definition in the text.)

16. State and prove the generalization of Proposition 2 to arbitrary direct products.
17. Let I be any nonempty index set and let G_i be a group for each $i \in I$. The *restricted direct product* or *direct sum* of the groups G_i is the set of elements of the direct product which are the identity in all but finitely many components, that is, the set of all elements $\prod a_i \in \prod_{i \in I} G_i$ such that $a_i = 1_i$ for all but a finite number of $i \in I$.
 - (a) Prove that the restricted direct product is a subgroup of the direct product.
 - (b) Prove that the restricted direct product is normal in the direct product.
 - (c) Let $I = \mathbb{Z}^+$ and let p_i be the i^{th} integer prime. Show that if $G_i = \mathbb{Z}/p_i\mathbb{Z}$ for all $i \in \mathbb{Z}^+$, then every element of the restricted direct product of the G_i 's has finite order but $\prod_{i \in \mathbb{Z}^+} G_i$ has elements of infinite order. Show that in this example the restricted direct product is the torsion subgroup of the direct product (cf. Exercise 6, Section 2.1).
18. In each of (a) to (e) give an example of a group with the specified properties:
 - (a) an infinite group in which every element has order 1 or 2
 - (b) an infinite group in which every element has finite order but for each positive integer n there is an element of order n
 - (c) a group with an element of infinite order and an element of order 2
 - (d) a group G such that every finite group is isomorphic to some subgroup of G
 - (e) a nontrivial group G such that $G \cong G \times G$.

5.2 THE FUNDAMENTAL THEOREM OF FINITELY GENERATED ABELIAN GROUPS

Definition.

- (1) A group G is *finitely generated* if there is a finite subset A of G such that $G = \langle A \rangle$.
- (2) For each $r \in \mathbb{Z}$ with $r \geq 0$, let $\mathbb{Z}^r = \mathbb{Z} \times \mathbb{Z} \times \dots \times \mathbb{Z}$ be the direct product of r copies of the group \mathbb{Z} , where $\mathbb{Z}^0 = 1$. The group \mathbb{Z}^r is called the *free abelian group of rank r* .

Note that any finite group G is, a fortiori, finitely generated: simply take $A = G$ as a set of generators. Also, \mathbb{Z}^r is finitely generated by e_1, e_2, \dots, e_r , where e_i is the n -tuple with 1 in position i and zeros elsewhere. We can now state the fundamental classification theorem for (finitely generated) abelian groups.

Theorem 3. (Fundamental Theorem of Finitely Generated Abelian Groups) Let G be a finitely generated abelian group. Then

(1)

$$G \cong \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \dots \times \mathbb{Z}_{n_s},$$

for some integers r, n_1, n_2, \dots, n_s satisfying the following conditions:

- (a) $r \geq 0$ and $n_j \geq 2$ for all j , and
 - (b) $n_{i+1} \mid n_i$ for $1 \leq i \leq s-1$
- (2) the expression in (1) is unique: if $G \cong \mathbb{Z}^r \times Z_{m_1} \times Z_{m_2} \times \cdots \times Z_{m_u}$, where t and m_1, m_2, \dots, m_u satisfy (a) and (b) (i.e., $t \geq 0$, $m_j \geq 2$ for all j and $m_{i+1} \mid m_i$ for $1 \leq i \leq u-1$), then $t = r$, $u = s$ and $m_i = n_i$ for all i .

Proof: We shall derive this theorem in Section 12.1 as a consequence of a more general classification theorem. For finite groups we shall give an alternate proof at the end of Section 6.1.

Definition. The integer r in Theorem 3 is called the *free rank* or *Betti number* of G and the integers n_1, n_2, \dots, n_s are called the *invariant factors* of G . The description of G in Theorem 3(1) is called the *invariant factor decomposition* of G .

Theorem 3 asserts that the free rank and (ordered) list of invariant factors of an abelian group are uniquely determined, so that two finitely generated abelian groups are isomorphic if and only if they have the same free rank and the same list of invariant factors. Observe that a finitely generated abelian group is a finite group if and only if its free rank is zero.

The order of a finite abelian group is just the product of its invariant factors (by Proposition 1). If G is a finite abelian group with invariant factors n_1, n_2, \dots, n_s , where $n_{i+1} \mid n_i$, $1 \leq i \leq s-1$, then G is said to be of type (n_1, n_2, \dots, n_s) .

Theorem 3 gives an effective way of listing *all* finite abelian groups of a given order. Namely, to find (up to isomorphism) all abelian groups of a given order n one must find all finite sequences of integers n_1, n_2, \dots, n_s such that

- (1) $n_j \geq 2$ for all $j \in \{1, 2, \dots, s\}$,
- (2) $n_{i+1} \mid n_i$, $1 \leq i \leq s-1$, and
- (3) $n_1 n_2 \cdots n_s = n$.

Theorem 3 states that there is a bijection between the set of such sequences and the set of isomorphism classes of finite abelian groups of order n (where each sequence corresponds to the list of invariant factors of a finite abelian group).

Before illustrating how to find all such sequences for a specific value of n we make some general comments. First note that $n_1 \geq n_2 \geq \cdots \geq n_s$, so n_1 is the largest invariant factor. Also, by property (3) each n_i divides n . If p is any prime divisor of n then by (3) we see that p must divide n_i for some i . Then, by (2), p also divides n_j for all $j \leq i$. It follows that

every prime divisor of n must divide the first invariant factor n_1 .

In particular, if n is the product of distinct primes (all to the first power)¹ we see that $n \mid n_1$, hence $n = n_1$. This proves that if n is squarefree, there is only one possible list of invariant factors for an abelian group of order n (namely, the list $n_1 = n$):

¹Such integers are called *squarefree* since they are not divisible by any square > 1 .

Corollary 4. If n is the product of distinct primes, then up to isomorphism the only abelian group of order n is the cyclic group of order n , Z_n .

The factorization of n into prime powers is the first step in determining all possible lists of invariant factors for abelian groups of order n .

Example

Suppose $n = 180 = 2^2 \cdot 3^2 \cdot 5$. As noted above we must have $2 \cdot 3 \cdot 5 \mid n_1$, so possible values of n_1 are

$$n_1 = 2^2 \cdot 3^2 \cdot 5, \quad 2^2 \cdot 3 \cdot 5, \quad 2 \cdot 3^2 \cdot 5, \quad \text{or} \quad 2 \cdot 3 \cdot 5.$$

For each of these one must work out all possible n_2 's (subject to $n_2 \mid n_1$ and $n_1 n_2 \mid n$). For each resulting pair n_1, n_2 one must work out all possible n_3 's etc. until all lists satisfying (1) to (3) are obtained.

For instance, if $n_1 = 2 \cdot 3^2 \cdot 5$, the only number n_2 dividing n_1 with $n_1 n_2$ dividing n is $n_2 = 2$. In this case $n_1 n_2 = n$, so this list is complete: $2 \cdot 3^2 \cdot 5, 2$. The abelian group corresponding to this list is $Z_{90} \times Z_2$.

If $n_1 = 2 \cdot 3 \cdot 5$, the only candidates for n_2 are $n_2 = 2, 3$ or 6 . If $n_2 = 2$ or 3 , then since $n_3 \mid n_2$ we would necessarily have $n_3 = n_2$ (and there must be a third term in the list by property (3)). This leads to a contradiction because $n_1 n_2 n_3$ would be divisible by 2^3 or 3^3 respectively, but n is not divisible by either of these numbers. Thus the only list of invariant factors whose first term is $2 \cdot 3 \cdot 5$ is $2 \cdot 3 \cdot 5, 2 \cdot 3$. The corresponding abelian group is $Z_{30} \times Z_6$.

Similarly, all permissible lists of invariant factors and the corresponding abelian groups of order 180 are easily seen to be the following:

Invariant Factors	Abelian Groups
$2^2 \cdot 3^2 \cdot 5$	Z_{180}
$2 \cdot 3^2 \cdot 5, 2$	$Z_{90} \times Z_2$
$2^2 \cdot 3 \cdot 5, 3$	$Z_{60} \times Z_3$
$2 \cdot 3 \cdot 5, 2 \cdot 3$	$Z_{30} \times Z_6$

The process we carried out above was somewhat *ad hoc*, however it indicates that the determination of lists of invariant factors of all abelian groups of a given order n relies strongly on the factorization of n . The following theorem (which we shall see is equivalent to the Fundamental Theorem in the case of finite abelian groups) gives a more systematic and computationally much faster way of determining all finite abelian groups of a given order. More specifically, if the factorization of n is

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

it shows that all permissible lists of invariant factors for abelian groups of order n may be determined by finding permissible lists for groups of order $p_i^{\alpha_i}$ for each i . For a prime power, p^α , we shall see that the problem of determining all permissible lists is equivalent to the determination of all partitions of α (and does not depend on p).

Theorem 5. Let G be an abelian group of order $n > 1$ and let the unique factorization of n into distinct prime powers be

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}.$$

Then

- (1) $G \cong A_1 \times A_2 \times \cdots \times A_k$, where $|A_i| = p_i^{\alpha_i}$
- (2) for each $A \in \{A_1, A_2, \dots, A_k\}$ with $|A| = p^\alpha$,

$$A \cong Z_{p^{\beta_1}} \times Z_{p^{\beta_2}} \times \cdots \times Z_{p^{\beta_t}}$$

with $\beta_1 \geq \beta_2 \geq \cdots \geq \beta_t \geq 1$ and $\beta_1 + \beta_2 + \cdots + \beta_t = \alpha$ (where t and β_1, \dots, β_t depend on i)

- (3) the decomposition in (1) and (2) is unique, i.e., if $G \cong B_1 \times B_2 \times \cdots \times B_m$, with $|B_i| = p_i^{\alpha_i}$ for all i , then $B_i \cong A_i$ and B_i and A_i have the same invariant factors.

Definition. The integers p^{β_j} described in the preceding theorem are called the *elementary divisors* of G . The description of G in Theorem 5(1) and 5(2) is called the *elementary divisor decomposition* of G .

The subgroups A_i described in part (1) of the theorem are the Sylow p_i -subgroups of G . Thus (1) says that G is isomorphic to the direct product of its Sylow subgroups (note that they are normal—since G is abelian—hence unique). Part 1 is often referred to as *The Primary Decomposition Theorem* for finite abelian groups.² As with Theorem 3, we shall prove this theorem later.

Note that for p a prime, $p^\beta \mid p^\gamma$ if and only if $\beta \leq \gamma$. Furthermore, $p^{\beta_1} \cdots p^{\beta_t} = p^\alpha$ if and only if $\beta_1 + \cdots + \beta_t = \alpha$. Thus the decomposition of A appearing in part (2) of Theorem 5 is the invariant factor decomposition of A with the “divisibility” conditions on the integers p^{β_j} translated into “additive” conditions on their exponents. The *elementary divisors* of G are now seen to be the *invariant factors of the Sylow p -subgroups* as p runs over all prime divisors of G .

By Theorem 5, in order to find all abelian groups of order $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ one must find for each i , $1 \leq i \leq k$, all possible lists of invariant factors for groups of order $p_i^{\alpha_i}$. The set of elementary divisors of each abelian group is then obtained by taking one set of invariant factors from each of the k lists. The abelian groups are the direct products of the cyclic groups whose orders are the elementary divisors (and distinct lists of elementary divisors give nonisomorphic groups). The advantage of this process over the one described following Theorem 2 is that it is easier to systematize how to obtain all possible lists of invariant factors, $p^{\beta_1}, p^{\beta_2}, \dots, p^{\beta_t}$, for a group of prime power order p^β . Conditions (1) to (3) for invariant factors described earlier then become

- (1) $\beta_j \geq 1$ for all $j \in \{1, 2, \dots, t\}$,
- (2) $\beta_i \geq \beta_{i+1}$ for all i , and
- (3) $\beta_1 + \beta_2 + \cdots + \beta_t = \beta$.

²Recall that for abelian groups the Sylow p -subgroups are sometimes called the p -primary components.

Hence, each list of invariant factors in this case is simply a *partition* of β (ordered in descending order). In particular, the number of nonisomorphic abelian groups of order p^β (= the number of distinct lists) equals the number of partitions of β . This number is independent of the prime p . For example the number of abelian groups of order p^5 is obtained from the list of partitions of 5:

Invariant Factors	Abelian Groups
5	Z_{p^5}
4, 1	$Z_{p^4} \times Z_p$
3, 2	$Z_{p^3} \times Z_{p^2}$
3, 1, 1	$Z_{p^3} \times Z_p \times Z_p$
2, 2, 1	$Z_{p^2} \times Z_{p^2} \times Z_p$
2, 1, 1, 1	$Z_{p^2} \times Z_p \times Z_p \times Z_p$
1, 1, 1, 1, 1	$Z_p \times Z_p \times Z_p \times Z_p \times Z_p$

Thus there are precisely 7 nonisomorphic groups of order p^5 , the first in the list being the cyclic group, Z_{p^5} , and the last in the list being the elementary abelian group, E_{p^5} .

If $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ and q_i is the number of partitions of α_i , we see that the number of (distinct, nonisomorphic) abelian groups of order n equals $q_1 q_2 \cdots q_k$.

Example

If $n = 1800 = 2^3 3^2 5^2$ we list the abelian groups of this order as follows:

Order p^β	Partitions of β	Abelian Groups
2^3	3; 2, 1; 1, 1, 1	$Z_8, Z_4 \times Z_2, Z_2 \times Z_2 \times Z_2$
3^2	2; 1, 1	$Z_9, Z_3 \times Z_3$
5^2	2; 1, 1	$Z_{25}, Z_5 \times Z_5$

We obtain the abelian groups of order 1800 by taking one abelian group from each of the three lists (right hand column above) and taking their direct product. Doing this in all possible ways gives all isomorphism types:

$$\begin{array}{ll}
 Z_8 \times Z_9 \times Z_{25} & Z_4 \times Z_2 \times Z_3 \times Z_3 \times Z_{25} \\
 Z_8 \times Z_9 \times Z_5 \times Z_5 & Z_4 \times Z_2 \times Z_3 \times Z_3 \times Z_5 \times Z_5 \\
 Z_8 \times Z_3 \times Z_3 \times Z_{25} & Z_2 \times Z_2 \times Z_2 \times Z_9 \times Z_{25} \\
 Z_8 \times Z_3 \times Z_3 \times Z_5 \times Z_5 & Z_2 \times Z_2 \times Z_2 \times Z_9 \times Z_5 \times Z_5 \\
 Z_4 \times Z_2 \times Z_9 \times Z_{25} & Z_2 \times Z_2 \times Z_2 \times Z_3 \times Z_3 \times Z_{25} \\
 Z_4 \times Z_2 \times Z_9 \times Z_5 \times Z_5 & Z_2 \times Z_2 \times Z_2 \times Z_3 \times Z_3 \times Z_5 \times Z_5
 \end{array}$$

By the Fundamental Theorems above, this is a *complete list* of all abelian groups of order 1800 — every abelian group of this order is isomorphic to precisely one of the groups above and no two of the groups in this list are isomorphic.

We emphasize that the elementary divisors of G are not invariant factors of G (but invariant factors of *subgroups* of G). For instance, in case 1 above the elementary divisors 8, 9, 25 do not satisfy the divisibility criterion of a list of invariant factors.

Our next aim is to illustrate how to pass from a list of invariant factors of a finite abelian group to its list of elementary divisors and vice versa. We show how to determine these invariants of the group no matter how it is given as a direct product of cyclic groups. We need the following proposition.

Proposition 6. Let $m, n \in \mathbb{Z}^+$.

- (1) $Z_m \times Z_n \cong Z_{mn}$ if and only if $(m, n) = 1$.
- (2) If $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ then $Z_n \cong Z_{p_1^{\alpha_1}} \times Z_{p_2^{\alpha_2}} \times \cdots \times Z_{p_k^{\alpha_k}}$.

Proof: Since (2) is an easy exercise using (1) and induction on k , we concentrate on proving (1). Let $Z_m = \langle x \rangle$, $Z_n = \langle y \rangle$ and let $l = \text{l.c.m.}(m, n)$. Note that $l = mn$ if and only if $(m, n) = 1$. Let $x^a y^b$ be a typical element of $Z_m \times Z_n$. Then (as noted in Example 1, Section 1)

$$\begin{aligned} (x^a y^b)^l &= x^{la} y^{lb} \\ &= 1^a 1^b = 1 \quad (\text{because } m \mid l \text{ and } n \mid l). \end{aligned}$$

If $(m, n) \neq 1$, every element of $Z_m \times Z_n$ has order at most l , hence has order strictly less than mn , so $Z_m \times Z_n$ cannot be isomorphic to Z_{mn} .

Conversely, if $(m, n) = 1$, then $|xy| = \text{l.c.m.}(|x|, |y|) = mn$. Thus, by order considerations, $Z_m \times Z_n = \langle xy \rangle$ is cyclic, completing the proof.

Obtaining Elementary Divisors from Invariant Factors

Suppose G is given as an abelian group of type (n_1, n_2, \dots, n_s) , that is

$$G \cong Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_s}.$$

Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = n_1 n_2 \cdots n_s$. Factor each n_i as

$$n_i = p_1^{\beta_{i1}} p_2^{\beta_{i2}} \cdots p_k^{\beta_{ik}}, \quad \text{where } \beta_{ij} \geq 0.$$

By the proposition above,

$$Z_{n_i} \cong Z_{p_1^{\beta_{i1}}} \times \cdots \times Z_{p_k^{\beta_{ik}}},$$

for each i . If $\beta_{ij} = 0$, $Z_{p_j^{\beta_{ij}}} = 1$ and this factor may be deleted from the direct product without changing the isomorphism type. Then the elementary divisors of G are precisely the integers

$$p_j^{\beta_{ij}}, \quad 1 \leq j \leq k, \quad 1 \leq i \leq s \text{ such that } \beta_{ij} \neq 0.$$

For example, if $|G| = 2^3 \cdot 3^2 \cdot 5^2$ and G is of type $(30, 30, 2)$, then

$$G \cong Z_{30} \times Z_{30} \times Z_2.$$

Since $Z_{30} \cong Z_2 \times Z_3 \times Z_5$, $G \cong Z_2 \times Z_3 \times Z_5 \times Z_2 \times Z_3 \times Z_5 \times Z_2$. The elementary divisors of G are therefore 2, 3, 5, 2, 3, 5, 2, or, grouping like primes together (note that rearranging the order of the factors in a direct product does not affect the isomorphism type (Exercise 7 of Section 1)), 2, 2, 2, 3, 3, 5, 5. In particular, G is isomorphic to the last group in the list in the example above.

If for each j one collects all the factors $Z_{p_j^{\beta_j}}$ together, the resulting direct product forms the Sylow p_j -subgroup, A_j , of G . Thus the Sylow 2-subgroup of the group in the preceding paragraph is isomorphic to $Z_2 \times Z_2 \times Z_2$ (i.e., the elementary abelian group of order 8).

Obtaining Elementary Divisors from any cyclic decomposition

The same process described above will give the elementary divisors of a finite abelian group G whenever G is given as a direct product of cyclic groups (not just when the orders of the cyclic components are the invariant factors). For example, if $G = Z_6 \times Z_{15}$, the list 6, 15 is neither that of the invariant factors (the divisibility condition fails) nor that of elementary divisors (they are not prime powers). To find the elementary divisors, factor $6 = 2 \cdot 3$ and $15 = 3 \cdot 5$. Then the prime powers 2, 3, 3, 5 are the elementary divisors and

$$G \cong Z_2 \times Z_3 \times Z_3 \times Z_5.$$

Obtaining Invariant Factors from Elementary Divisors

Suppose G is an abelian group of order n , where $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ and we are given the elementary divisors of G . The invariant factors of G are obtained by following these steps:

- (1) First group all elementary divisors which are powers of the same prime together. In this way we obtain k lists of integers (one for each p_j).
- (2) In each of these k lists arrange the integers in nonincreasing order.
- (3) Among these k lists suppose that the longest (i.e., the one with the most terms) consists of t integers. Make each of the k lists of length t by appending an appropriate number of 1's at the end of each list.
- (4) For each $i \in \{1, 2, \dots, t\}$ the i^{th} invariant factor, n_i , is obtained by taking the product of the i^{th} integer in each of the t (ordered) lists.

The point of ordering the lists in this way is to ensure that we have the divisibility condition $n_{i+1} \mid n_i$.

Suppose, for example, that the elementary divisors of G are given as 2, 3, 2, 25, 3, 2 (so $|G| = 2^3 \cdot 3^2 \cdot 5^2$). Regrouping and increasing each list to have 3 ($= t$) members gives:

$p = 2$	$p = 3$	$p = 5$
2	3	25
2	3	1
2	1	1

so the invariant factors of G are $2 \cdot 3 \cdot 25$, $2 \cdot 3 \cdot 1$, $2 \cdot 1 \cdot 1$ and

$$G \cong Z_{150} \times Z_6 \times Z_2.$$

Note that this is the penultimate group in the list classifying abelian groups of order 1800 computed above.

The invariant factor decompositions of the abelian groups of order 1800 are as follows, where the i^{th} group in this list is isomorphic to the i^{th} group computed in the

previous list:

Z_{1800}	$Z_{300} \times Z_6$
$Z_{360} \times Z_5$	$Z_{60} \times Z_{30}$
$Z_{600} \times Z_3$	$Z_{450} \times Z_2 \times Z_2$
$Z_{120} \times Z_{15}$	$Z_{90} \times Z_{10} \times Z_2$
$Z_{900} \times Z_2$	$Z_{150} \times Z_6 \times Z_2$
$Z_{180} \times Z_{10}$	$Z_{30} \times Z_{30} \times Z_2.$

Using the uniqueness statements of the Fundamental Theorems 3 and 5, we can use these processes to determine whether any two direct products of finite cyclic groups are isomorphic. For instance, if one wanted to know whether $Z_6 \times Z_{15} \cong Z_{10} \times Z_9$, first determine whether they have the same order (both are of order 90) and then (the easiest way in general) determine whether they have the same elementary divisors:

$Z_6 \times Z_{15}$ has elementary divisors 2, 3, 3, 5 and is isomorphic to $Z_2 \times Z_3 \times Z_3 \times Z_5$

$Z_{10} \times Z_9$ has elementary divisors 2, 5, 9 and is isomorphic to $Z_2 \times Z_5 \times Z_9$.

The lists of elementary divisors are different so (by Theorem 5) they are not isomorphic. Note that $Z_6 \times Z_{15}$ has no element of order 9 whereas $Z_{10} \times Z_9$ does (cf. Exercise 5).

The processes we described above (with some elaboration) form a proof (via Proposition 6) that for finite abelian groups Theorems 3 and 5 are equivalent (i.e., one implies the other). We leave the details to the reader.

One can now better understand some of the power and some of the limitations of classification theorems. On one hand, given any positive integer n one can explicitly describe all abelian groups of order n , a significant achievement. On the other hand, the amount of information necessary to determine which of the isomorphism types of groups of order n a particular group belongs to may be considerable (and is large if n is divisible by large powers of primes).

We close this section with some terminology which will be useful in later sections.

Definition.

- (1) If G is a finite abelian group of type (n_1, n_2, \dots, n_t) , the integer t is called the *rank* of G (the free rank of G is 0 so there will be no confusion).
- (2) If G is any group, the *exponent* of G is the smallest positive integer n such that $x^n = 1$ for all $x \in G$ (if no such integer exists the exponent of G is ∞).

EXERCISES

1. In each of parts (a) to (e) give the number of nonisomorphic abelian groups of the specified order — do not list the groups: (a) order 100, (b) order 576, (c) order 1155, (d) order 42875, (e) order 2704.
2. In each of parts (a) to (e) give the lists of invariant factors for all abelian groups of the specified order:
(a) order 270, (b) order 9801, (c) order 320, (d) order 105, (e) order 44100.
3. In each of parts (a) to (e) give the lists of elementary divisors for all abelian groups of the specified order and then match each list with the corresponding list of invariant factors

found in the preceding exercise:

(a) order 270, (b) order 9801, (c) order 320, (d) order 105, (e) order 44100.

4. In each of parts (a) to (d) determine which pairs of abelian groups listed are isomorphic (here the expression $\{a_1, a_2, \dots, a_k\}$ denotes the abelian group $Z_{a_1} \times Z_{a_2} \times \dots \times Z_{a_k}$).
 - (a) $\{4, 9\}, \{6, 6\}, \{8, 3\}, \{9, 4\}, \{6, 4\}, \{64\}$.
 - (b) $\{2^2, 2 \cdot 3^2\}, \{2^2 \cdot 3, 2 \cdot 3\}, \{2^3 \cdot 3^2\}, \{2^2 \cdot 3^2, 2\}$.
 - (c) $\{5^2 \cdot 7^2, 3^2 \cdot 5 \cdot 7\}, \{3^2 \cdot 5^2 \cdot 7, 5 \cdot 7^2\}, \{3 \cdot 5^2, 7^2, 3 \cdot 5 \cdot 7\}, \{5^2 \cdot 7, 3^2 \cdot 5, 7^2\}$.
 - (d) $\{2^2 \cdot 5 \cdot 7, 2^3 \cdot 5^3, 2 \cdot 5^2\}, \{2^3 \cdot 5^3 \cdot 7, 2^3 \cdot 5^3\}, \{2^2, 2 \cdot 7, 2^3, 5^3, 5^3\}, \{2 \cdot 5^3, 2^2 \cdot 5^3, 2^3, 7\}$.
5. Let G be a finite abelian group of type (n_1, n_2, \dots, n_t) . Prove that G contains an element of order m if and only if $m \mid n_1$. Deduce that G is of exponent n_1 .
6. Prove that any finite group has a finite exponent. Give an example of an infinite group with finite exponent. Does a finite group of exponent m always contain an element of order m ?
7. Let p be a prime and let $A = \langle x_1 \rangle \times \langle x_2 \rangle \times \dots \times \langle x_n \rangle$ be an abelian p -group, where $|x_i| = p^{\alpha_i} > 1$ for all i . Define the p^{th} -power map

$$\varphi : A \rightarrow A \quad \text{by} \quad \varphi : x \mapsto x^p.$$

- (a) Prove that φ is a homomorphism.
- (b) Describe the image and kernel of φ in terms of the given generators.
- (c) Prove both $\ker \varphi$ and $A/\ker \varphi$ have rank n (i.e., have the same rank as A) and prove these groups are both isomorphic to the elementary abelian group, E_{p^n} , of order p^n .
8. Let A be a finite abelian group (written multiplicatively) and let p be a prime. Let

$$A^p = \{a^p \mid a \in A\} \quad \text{and} \quad A_p = \{x \mid x^p = 1\}$$

(so A^p and A_p are the image and kernel of the p^{th} -power map, respectively).

- (a) Prove that $A/A^p \cong A_p$. [Show that they are both elementary abelian and they have the same order.]
- (b) Prove that the number of subgroups of A of order p equals the number of subgroups of A of index p . [Reduce to the case where A is an elementary abelian p -group.]
9. Let $A = Z_{60} \times Z_{45} \times Z_{12} \times Z_{36}$. Find the number of elements of order 2 and the number of subgroups of index 2 in A .
10. Let n and k be positive integers and let A be the free abelian group of rank n (written additively). Prove that A/kA is isomorphic to the direct product of n copies of $\mathbb{Z}/k\mathbb{Z}$ (here $kA = \{ka \mid a \in A\}$). [See Exercise 14, Section 1.]
11. Let G be a nontrivial finite abelian group of rank t .
 - (a) Prove that the rank of G equals the maximum of the ranks of its Sylow subgroups.
 - (b) Prove that G can be generated by t elements but no subset with fewer than t elements generates G . [One way of doing this is by using part (a) together with Exercise 7.]
12. Let n and m be positive integers with $d = (n, m)$. Let $Z_n = \langle x \rangle$ and $Z_m = \langle y \rangle$. Let A be the central product of $\langle x \rangle$ and $\langle y \rangle$ with an element of order d identified, which has presentation $\langle x, y \mid x^n = y^m = 1, xy = yx, x^{\frac{n}{d}} = y^{\frac{m}{d}} \rangle$. Describe A as a direct product of two cyclic groups.
13. Let $A = \langle x_1 \rangle \times \dots \times \langle x_r \rangle$ be a finite abelian group with $|x_i| = n_i$ for $1 \leq i \leq r$. Find a presentation for A . Prove that if G is any group containing commuting elements g_1, \dots, g_r such that $g_i^{n_i} = 1$ for $1 \leq i \leq r$, then there is a unique homomorphism from A to G which sends x_i to g_i for all i .

- 14.** For any group G define the *dual group* of G (denoted \widehat{G}) to be the set of all homomorphisms from G into the multiplicative group of roots of unity in \mathbb{C} . Define a group operation in \widehat{G} by pointwise multiplication of functions: if χ, ψ are homomorphisms from G into the group of roots of unity then $\chi\psi$ is the homomorphism given by $(\chi\psi)(g) = \chi(g)\psi(g)$ for all $g \in G$, where the latter multiplication takes place in \mathbb{C} .
- (a) Show that this operation on \widehat{G} makes \widehat{G} into an abelian group. [Show that the identity is the map $g \mapsto 1$ for all $g \in G$ and the inverse of $\chi \in \widehat{G}$ is the map $g \mapsto \chi(g)^{-1}$.]
- (b) If G is a finite abelian group, prove that $\widehat{G} \cong G$. [Write G as $\langle x_1 \rangle \times \cdots \times \langle x_r \rangle$ and if $n_i = |x_i|$ define χ_i to be the homomorphism which sends x_i to $e^{2\pi i / n_i}$ and sends x_j to 1, for all $j \neq i$. Prove χ_i has order n_i in \widehat{G} and $\widehat{G} = \langle \chi_1 \rangle \times \cdots \times \langle \chi_r \rangle$.]
- (This result is often phrased: a finite abelian group is self-dual. It implies that the lattice diagram of a finite abelian group is the same when it is turned upside down. Note however that there is no *natural* isomorphism between G and its dual (the isomorphism depends on a choice of a set of generators for G). This is frequently stated in the form: a finite abelian group is *noncanonically* isomorphic to its dual.)
- 15.** Let $G = \langle x \rangle \times \langle y \rangle$ where $|x| = 8$ and $|y| = 4$.
- (a) Find all pairs a, b in G such that $G = \langle a \rangle \times \langle b \rangle$ (where a and b are expressed in terms of x and y).
- (b) Let $H = \langle x^2y, y^2 \rangle \cong \mathbb{Z}_4 \times \mathbb{Z}_2$. Prove that there are no elements a, b of G such that $G = \langle a \rangle \times \langle b \rangle$ and $H = \langle a^2 \rangle \times \langle b^2 \rangle$ (i.e., one cannot pick direct product generators for G in such a way that some powers of these are direct product generators for H).
- 16.** Prove that no finitely generated abelian group is divisible (cf. Exercise 19, Section 2.4).

5.3 TABLE OF GROUPS OF SMALL ORDER

At this point we can give a table of the isomorphism types for most of the groups of small order.

Each of the unfamiliar non-abelian groups in the table on the following page will be constructed in Section 5 on semidirect products (which will also explain the notation used for them). For the present we give generators and relations for each of them (i.e., presentations of them).

The group $Z_3 \rtimes Z_4$ of order 12 can be described by the generators and relations:

$$\langle x, y \mid x^4 = y^3 = 1, x^{-1}yx = y^{-1} \rangle,$$

namely, it has a normal Sylow 3-subgroup ($\langle y \rangle$) which is inverted by an element of order 4 (x) acting by conjugation (x^2 centralizes y).

The group $(Z_3 \times Z_3) \rtimes Z_2$ has generators and relations:

$$\langle x, y, z \mid x^2 = y^3 = z^3 = 1, yz = zy, x^{-1}yx = y^{-1}, x^{-1}zx = z^{-1} \rangle,$$

namely, it has a normal Sylow 3-subgroup isomorphic to $Z_3 \times Z_3$ ($\langle y, z \rangle$) inverted by an element of order 2 (x) acting by conjugation.

The group $Z_5 \rtimes Z_4$ of order 20 has generators and relations:

$$\langle x, y \mid x^4 = y^5 = 1, x^{-1}yx = y^{-1} \rangle,$$

namely, it has a normal Sylow 5-subgroup ($\langle y \rangle$) which is inverted by an element of order 4 (x) acting by conjugation (x^2 centralizes y).

7	1	Z_7	none
8	5	$Z_8, Z_4 \times Z_2,$ $Z_2 \times Z_2 \times Z_2$	D_8, Q_8
9	2	$Z_9, Z_3 \times Z_3$	none
10	2	Z_{10}	D_{10}
11	1	Z_{11}	none
12	5	$Z_{12}, Z_6 \times Z_2$	$A_4, D_{12}, Z_3 \rtimes Z_4$
13	1	Z_{13}	none
14	2	Z_{14}	D_{14}
15	1	Z_{15}	none
16	14	$Z_{16}, Z_8 \times Z_2,$ $Z_4 \times Z_4, Z_4 \times Z_2 \times Z_2,$ $Z_2 \times Z_2 \times Z_2 \times Z_2$	not listed
17	1	Z_{17}	none
18	5	$Z_{18}, Z_6 \times Z_3$	$D_{18}, S_3 \times Z_3,$ $(Z_3 \times Z_3) \rtimes Z_2$
19	1	Z_{19}	none
20	5	$Z_{20}, Z_{10} \times Z_2$	D_{20} $Z_5 \rtimes Z_4, F_{20}$

The group F_{20} of order 20 has generators and relations:

$$\langle x, y \mid x^4 = y^5 = 1, xyx^{-1} = y^2 \rangle,$$

namely, it has a normal Sylow 5-subgroup ($\langle y \rangle$) which is squared by an element of order (x) acting by conjugation. One can check that this group occurs as the normalizer of Sylow 5-subgroup in S_5 , e.g.,

$$F_{20} = ((2\ 3\ 5\ 4), (1\ 2\ 3\ 4\ 5)).$$

This group is called the *Frobenius group* of order 20.

EXERCISE

- 1.** Prove that D_{16} , $Z_2 \times D_8$, $Z_2 \times Q_8$, $Z_4 * D_8$, QD_{16} and M are nonisomorphic non-abelian groups of order 16 (where $Z_4 * D_8$ is described in Exercise 12, Section 1 and QD_{16} and M are described in the exercises in Section 2.5).

5.4 RECOGNIZING DIRECT PRODUCTS

So far we have seen that direct products may be used to both construct “larger” groups from “smaller” ones and to decompose finitely generated abelian groups into cyclic factors. Even certain non-abelian groups, which may be given in some other form, may be decomposed as direct products of smaller groups. The purpose of this section is to indicate a criterion to recognize when a group is the direct product of some of its subgroups and to illustrate the criterion with some examples.

Before doing so we introduce some standard notation and elementary results on commutators which will streamline the presentation and which will be used again in Chapter 6 when we consider nilpotent groups.

Definition. Let G be a group, let $x, y \in G$ and let A, B be nonempty subsets of G .

- (1) Define $[x, y] = x^{-1}y^{-1}xy$, called the *commutator* of x and y .
- (2) Define $[A, B] = \langle [a, b] \mid a \in A, b \in B \rangle$, the group generated by commutators of elements from A and from B .
- (3) Define $G' = \langle [x, y] \mid x, y \in G \rangle$, the subgroup of G generated by commutators of elements from G , called the *commutator subgroup* of G .

The commutator of x and y is 1 if and only if x and y commute, which explains the terminology. The following proposition shows how commutators measure the “difference” in G between xy and yx .

Proposition 7. Let G be a group, let $x, y \in G$ and let $H \leq G$. Then

- (1) $xy = yx[x, y]$ (in particular, $xy = yx$ if and only if $[x, y] = 1$).
- (2) $H \trianglelefteq G$ if and only if $[H, G] \leq H$.
- (3) $\sigma[x, y] = [\sigma(x), \sigma(y)]$ for any automorphism σ of G , G' char G and G/G' is abelian.
- (4) G/G' is the largest abelian quotient of G in the sense that if $H \trianglelefteq G$ and G/H is abelian, then $G' \leq H$. Conversely, if $G' \leq H$, then $H \trianglelefteq G$ and G/H is abelian.
- (5) If $\varphi : G \rightarrow A$ is any homomorphism of G into an abelian group A , then φ factors through G' i.e., $G' \leq \ker \varphi$ and the following diagram commutes:

$$\begin{array}{ccc} G & \xrightarrow{\quad} & G/G' \\ & \searrow \varphi & \downarrow \\ & A & \end{array}$$

Proof: (1) This is immediate from the definition of $[x, y]$.

(2) By definition, $H \trianglelefteq G$ if and only if $g^{-1}hg \in H$ for all $g \in G$ and all $h \in H$. For $h \in H$, $g^{-1}hg \in H$ if and only if $h^{-1}g^{-1}hg \in H$, so that $H \trianglelefteq G$ if and only if $[h, g] \in H$ for all $h \in H$ and all $g \in G$. Thus $H \trianglelefteq G$ if and only if $[H, G] \leq H$, which is (2).

(3) Let $\sigma \in \text{Aut}(G)$ be an automorphism of G and let $x, y \in G$. Then

$$\begin{aligned}\sigma([x, y]) &= \sigma(x^{-1}y^{-1}xy) \\ &= \sigma(x)^{-1}\sigma(y)^{-1}\sigma(x)\sigma(y) \\ &= [\sigma(x), \sigma(y)].\end{aligned}$$

Thus for every commutator $[x, y]$ of G' , $\sigma([x, y])$ is again a commutator. Since σ has a 2-sided inverse, it follows that it maps the set of commutators bijectively onto itself. Since the commutators are a generating set for G' , $\sigma(G') = G'$, that is, $G' \text{ char } G$.

To see that G/G' is abelian, let xG' and yG' be arbitrary elements of G/G' . By definition of the group operation in G/G' and since $[x, y] \in G'$ we have

$$\begin{aligned}(xG')(yG') &= (xy)G' \\ &= (yx[x, y])G' \\ &= (yx)G' = (yG')(xG'),\end{aligned}$$

which completes the proof of (3).

(4) Suppose $H \trianglelefteq G$ and G/H is abelian. Then for all $x, y \in G$ we have $(xH)(yH) = (yH)(xH)$, so

$$\begin{aligned}1H &= (xH)^{-1}(yH)^{-1}(xH)(yH) \\ &= x^{-1}y^{-1}xyH \\ &= [x, y]H.\end{aligned}$$

Thus $[x, y] \in H$ for all $x, y \in G$, so that $G' \leq H$.

Conversely, if $G' \leq H$, then since G/G' is abelian by (3), every subgroup of G/G' is normal. In particular, $H/G' \trianglelefteq G/G'$. By the Lattice Isomorphism Theorem $H \trianglelefteq G$. By the Third Isomorphism Theorem

$$G/H \cong (G/G')/(H/G')$$

hence G/H is abelian (being isomorphic to a quotient of the abelian group G/G'). This proves (4).

(5) This is (4) phrased in terms of homomorphisms.

Passing to the quotient by the commutator subgroup of G collapses all commutators to the identity so that all elements in the quotient group commute. As (4) indicates, a strong converse to this also holds: a quotient of G by H is abelian if and only if the commutator subgroup is contained in H (i.e., if and only if G' is mapped to the identity in the quotient G/H).

We shall exhibit a group (of order 96) in the next section with the property that one of the elements of its commutator subgroup *cannot* be written as a single commutator $[x, y]$ for any x and y . Thus G' does not necessarily consist only of the set of (single) commutators (but is the group *generated* by these elements).

Examples

- (1) A group G is abelian if and only if $G' = 1$.
- (2) Sometimes it is possible to compute the commutator subgroup of a group without actually calculating commutators explicitly. For instance, if $G = D_8$, then since $Z(D_8) = \langle r^2 \rangle \trianglelefteq D_8$ and $D_8/Z(D_8)$ is abelian (the Klein 4-group), the commutator subgroup D'_8 is a subgroup of $Z(D_8)$. Since D_8 is not itself abelian its commutator subgroup is nontrivial. The only possibility is that $D'_8 = Z(D_8)$. By a similar argument, $Q'_8 = Z(Q_8) = \langle -1 \rangle$. More generally, if G is any non-abelian group of order p^3 , where p is a prime, $G' = Z(G)$ and $|G'| = p$ (Exercise 7).
- (3) Let $D_{2n} = \langle r, s \mid r^n = s^2 = 1, s^{-1}rs = r^{-1} \rangle$. Since $[r, s] = r^{-2}$, we have $\langle r^{-2} \rangle = \langle r^2 \rangle \leq D'_{2n}$. Furthermore, $\langle r^2 \rangle \trianglelefteq D_{2n}$ and the images of r and s in $D_{2n}/\langle r^2 \rangle$ generate this quotient. They are commuting elements of order ≤ 2 , so the quotient is abelian and $D'_{2n} \leq \langle r^2 \rangle$. Thus $D'_{2n} = \langle r^2 \rangle$. Finally, note that if $n (= |r|)$ is odd, $\langle r^2 \rangle = \langle r \rangle$ whereas if n is even, $\langle r^2 \rangle$ is of index 2 in $\langle r \rangle$. Hence D'_{2n} is of index 2 or 4 in D_{2n} according to whether n is odd or even, respectively.
- (4) Since conjugation by $g \in G$ is an automorphism of G , $[a^g, b^g] = [a, b]^g$ for all $a, b \in G$ by (3) of the proposition, i.e., conjugates of commutators are also commutators. For example, once we exhibit an element of one cycle type in S_n as a commutator, every element of the same cycle type is also a commutator (cf. Section 4.3). For example, every 5-cycle is a commutator in S_5 as follows: labelling the vertices of a pentagon as $1, \dots, 5$ we see that $D_{10} \leq S_5$ (a subgroup of A_5 in fact). By the preceding example an element of order 5 is a commutator in D_{10} , hence also in S_5 . Explicitly, $(14253) = [(12345), (25)(43)]$.

The next result actually follows from the proof of Proposition 3.13 but we isolate it explicitly for reference:

Proposition 8. Let H and K be subgroups of the group G . The number of distinct ways of writing each element of the set HK in the form hk , for some $h \in H$ and $k \in K$ is $|H \cap K|$. In particular, if $H \cap K = 1$, then each element of HK can be written uniquely as a product hk , for some $h \in H$ and $k \in K$.

Proof: Exercise.

The main result of this section is the following *recognition theorem*.

Theorem 9. Suppose G is a group with subgroups H and K such that

- (1) H and K are normal in G , and
- (2) $H \cap K = 1$.

Then $HK \cong H \times K$.

Proof: Observe that by hypothesis (1), HK is a subgroup of G (see Corollary 3.15). Let $h \in H$ and let $k \in K$. Since $H \trianglelefteq G$, $k^{-1}hk \in H$, so that $h^{-1}(k^{-1}hk) \in H$. Similarly, $(h^{-1}k^{-1}h)k \in K$. Since $H \cap K = 1$ it follows that $h^{-1}k^{-1}hk = 1$, i.e., $hk = kh$ so that every element of H commutes with every element of K .

By the preceding proposition each element of HK can be written uniquely as a product hk , with $h \in H$ and $k \in K$. Thus the map

$$\begin{aligned}\varphi : HK &\rightarrow H \times K \\ hk &\mapsto (h, k)\end{aligned}$$

is well defined. To see that φ is a homomorphism note that if $h_1, h_2 \in H$ and $k_1, k_2 \in K$, then we have seen that h_2 and k_1 commute. Thus

$$(h_1k_1)(h_2k_2) = (h_1h_2)(k_1k_2)$$

and the latter product is the unique way of writing $(h_1k_1)(h_2k_2)$ in the form hk with $h \in H$ and $k \in K$. This shows that

$$\begin{aligned}\varphi(h_1k_1h_2k_2) &= \varphi(h_1h_2k_1k_2) \\ &= (h_1h_2, k_1k_2) \\ &= (h_1, k_1)(h_2, k_2) = \varphi(h_1k_1)\varphi(h_2k_2)\end{aligned}$$

so that φ is a homomorphism. The homomorphism φ is a bijection since the representation of each element of HK as a product of the form hk is unique, which proves that φ is an isomorphism.

Definition. If G is a group and H and K are normal subgroups of G with $H \cap K = 1$, we call HK the *internal direct product* of H and K . We shall (when emphasis is called for) call $H \times K$ the *external direct product* of H and K .

The distinction between internal and external direct product is (by Theorem 9) purely notational: the elements of the internal direct product are written in the form hk , whereas those of the external direct product are written as ordered pairs (h, k) . We have in previous instances passed between these. For example, when $Z_n = \langle a \rangle$ and $Z_m = \langle b \rangle$ we wrote $x = (a, 1)$ and $y = (1, b)$ so that every element of $Z_n \times Z_m$ was written in the form $x^r y^s$.

Examples

(1) If n is a positive odd integer, we show $D_{4n} \cong D_{2n} \times Z_2$. To see this let

$$D_{4n} = \langle r, s \mid r^{2n} = s^2 = 1, srs = r^{-1} \rangle$$

be the usual presentation of D_{4n} . Let $H = \langle s, r^2 \rangle$ and let $K = \langle r^n \rangle$. Geometrically, if D_{4n} is the group of symmetries of a regular $2n$ -gon, H is the group of symmetries of the regular n -gon inscribed in the $2n$ -gon by joining vertex $2i$ to vertex $2i + 2$, for all $i \bmod 2n$ (and if one lets $r_1 = r^2$, H has the usual presentation of the dihedral group of order $2n$ with generators r_1 and s). Note that $H \trianglelefteq D_{4n}$ (it has index 2). Since $|r| = 2n$, $|r^n| = 2$. Since $srs = r^{-1}$, we have $sr^n s = r^{-n} = r^n$, that is, s centralizes r^n . Since clearly r centralizes r^n , $K \leq Z(D_{4n})$. Thus $K \trianglelefteq D_{4n}$. Finally, $K \not\leq H$ since r^2 has odd order (or because r^n sends vertex i into vertex $i + n$, hence does not preserve the set of even vertices of the $2n$ -gon). Thus $H \cap K = 1$ by Lagrange. Theorem 9 now completes the proof.

(2) Let I be a subset of $\{1, 2, \dots, n\}$ and let G be the setwise stabilizer of I in S_n , i.e.,

$$G = \{\sigma \in S_n \mid \sigma(i) \in I \text{ for all } i \in I\}.$$

Let $J = \{1, 2, \dots, n\} - I$ be the complement of I and note that G is also the setwise stabilizer of J . Let H be the *pointwise* stabilizer of I and let K be the *pointwise* stabilizer of $\{1, 2, \dots, n\} - I$, i.e.,

$$\begin{aligned} H &= \{\sigma \in G \mid \sigma(i) = i \text{ for all } i \in I\} \\ K &= \{\tau \in G \mid \tau(j) = j \text{ for all } j \in J\}. \end{aligned}$$

It is easy to see that H and K are normal subgroups of G (in fact they are kernels of the actions of G on I and J , respectively). Since any element of $H \cap K$ fixes all of $\{1, 2, \dots, n\}$, we have $H \cap K = 1$. Finally, since every element σ of G stabilizes the sets I and J , each cycle in the cycle decomposition of σ involves only elements of I or only elements of J . Thus σ may be written as a product $\sigma_I \sigma_J$, where $\sigma_I \in H$ and $\sigma_J \in K$. This proves $G = HK$. By Theorem 9, $G \cong H \times K$. Now any permutation of J can be extended to a permutation in S_n by letting it act as the identity on I . These are precisely the permutations in H (and similarly the permutations in K are the permutations of I which are the identity on J), so

$$H \cong S_J \quad K \cong S_I \quad \text{and} \quad G \cong S_m \times S_{n-m},$$

where $m = |J|$ (and, by convention, $S_0 = 1$).

- (3) Let $\sigma \in S_n$ and let I be the subset of $\{1, 2, \dots, n\}$ fixed pointwise by σ :

$$I = \{i \in \{1, 2, \dots, n\} \mid \sigma(i) = i\}.$$

If $C = C_{S_n}(\sigma)$, then by Exercise 18 of Section 4.3, C stabilizes the set I and its complement J . By the preceding example, C is isomorphic to a subgroup of $H \times K$, where H is the subgroup of all permutations in S_n fixing I pointwise and K is the set of all permutations fixing J pointwise. Note that $\sigma \in H$. Thus each element, α , of C can be written (uniquely) as $\alpha = \alpha_I \alpha_J$, for some $\alpha_I \in H$ and $\alpha_J \in K$. Note further that if τ is any permutation of $\{1, 2, \dots, n\}$ which fixes each $j \in J$ (i.e., any element of K), then σ and τ commute (since they move no common integers). Thus C contains all such τ , i.e., C contains the subgroup K . This proves that the group C consists of all elements $\alpha_I \alpha_J \in H \times K$ such that α_J is arbitrary in K and α_I commutes with σ in H :

$$\begin{aligned} C_{S_n}(\sigma) &= C_H(\sigma) \times K \\ &\cong C_{S_J}(\sigma) \times S_I. \end{aligned}$$

In particular, if σ is an m -cycle in S_n ,

$$C_{S_n}(\sigma) = \langle \sigma \rangle \times S_{n-m}.$$

The latter group has order $m(n - m)!$, as computed in Section 4.3.

EXERCISES

Let G be a group.

- Prove that if $x, y \in G$ then $[y, x] = [x, y]^{-1}$. Deduce that for any subsets A and B of G , $[A, B] = [B, A]$ (recall that $[A, B]$ is the *subgroup* of G generated by the commutators $[a, b]$).
- Prove that a subgroup H of G is normal if and only if $[G, H] \leq H$.
- Let $a, b, c \in G$. Prove that
 - $[a, bc] = [a, c](c^{-1}[a, b]c)$

- (b) $[ab, c] = (b^{-1}[a, c]b)[b, c]$.
4. Find the commutator subgroups of S_4 and A_4 .
 5. Prove that A_n is the commutator subgroup of S_n for all $n \geq 5$.
 6. Exhibit a representative of each cycle type of A_5 as a commutator in S_5 .
 7. Prove that if p is a prime and P is a non-abelian group of order p^3 then $P' = Z(P)$.
 8. Assume $x, y \in G$ and both x and y commute with $[x, y]$. Prove that for all $n \in \mathbb{Z}^+$, $(xy)^n = x^n y^n [y, x]^{\frac{n(n-1)}{2}}$.
 9. Prove that if p is an odd prime and P is a group of order p^3 then the p^{th} power map $x \mapsto x^p$ is a homomorphism of P into $Z(P)$. If P is not cyclic, show that the kernel of the p^{th} power map has order p^2 or p^3 . Is the squaring map a homomorphism in non-abelian groups of order 8? Where is the oddness of p needed in the above proof? [Use Exercise 8.]
 10. Prove that a finite abelian group is the direct product of its Sylow subgroups.
 11. Prove that if $G = HK$ where H and K are characteristic subgroups of G with $H \cap K = 1$ then $\text{Aut}(G) \cong \text{Aut}(H) \times \text{Aut}(K)$. Deduce that if G is an abelian group of finite order then $\text{Aut}(G)$ is isomorphic to the direct product of the automorphism groups of its Sylow subgroups.
 12. Use Theorem 4.17 to describe the automorphism group of a finite cyclic group.
 13. Prove that D_{8n} is not isomorphic to $D_{4n} \times Z_2$.
 14. Let $G = \{(a_{ij}) \in GL_n(F) \mid a_{ij} = 0 \text{ if } i > j, \text{ and } a_{11} = a_{22} = \dots = a_{nn}\}$, where F is a field, be the group of upper triangular matrices all of whose diagonal entries are equal. Prove that $G \cong D \times U$, where D is the group of all nonzero multiples of the identity matrix and U is the group of upper triangular matrices with 1's down the diagonal.
 15. If A and B are normal subgroups of G such that G/A and G/B are both abelian, prove that $G/(A \cap B)$ is abelian.
 16. Prove that if K is a normal subgroup of G then $K' \trianglelefteq G$.
 17. If K is a normal subgroup of G and K is cyclic, prove that $G' \leq C_G(K)$. [Recall that the automorphism group of a cyclic group is abelian.]
 18. Let K_1, K_2, \dots, K_n be non-abelian simple groups and let $G = K_1 \times K_2 \times \dots \times K_n$. Prove that every normal subgroup of G is of the form G_I for some subset I of $\{1, 2, \dots, n\}$ (where G_I is defined in Exercise 2 of Section 1). [If $N \trianglelefteq G$ and $x = (a_1, \dots, a_n) \in N$ with some $a_i \neq 1$, then show that there is some $g_i \in G_i$ not commuting with a_i . Show $[(1, \dots, g_i, \dots, 1), x] \in K_i \cap N$ and deduce $K_i \leq N$.]
 19. A group H is called *perfect* if $H' = H$ (i.e., H equals its own commutator subgroup).
 - (a) Prove that every non-abelian simple group is perfect.
 - (b) Prove that if H and K are perfect subgroups of a group G then (H, K) is also perfect. Extend this to show that the subgroup of G generated by any collection of perfect subgroups is perfect.
 - (c) Prove that any conjugate of a perfect subgroup is perfect.
 - (d) Prove that any group G has a unique maximal perfect subgroup and that this subgroup is normal.
 20. Let $H(F)$ be the Heisenberg group over the field F , cf. Exercise 11 of Section 1.4. Find an explicit formula for the commutator $[X, Y]$, where $X, Y \in H(F)$, and show that the commutator subgroup of $H(F)$ equals the center of $H(F)$ (cf. Section 2.2, Exercise 14).

5.5 SEMIDIRECT PRODUCTS

In this section we study the “semidirect product” of two groups H and K , which is a generalization of the notion of the direct product of H and K obtained by relaxing the requirement that both H and K be normal. This construction will enable us (in certain circumstances) to build a “larger” group from the groups H and K in such a way that G contains subgroups isomorphic to H and K , respectively, as in the case of direct products. In this case the subgroup H will be normal in G but the subgroup K will not necessarily be normal (as it is for direct products). Thus, for instance, we shall be able to construct non-abelian groups even if H and K are abelian. This construction will allow us to enlarge considerably the set of examples of groups at our disposal. As in the preceding section, we shall then prove a recognition theorem that will enable us to decompose some familiar groups into smaller “factors,” from which we shall be able to derive some classification theorems.

By way of motivation suppose we already have a group G containing subgroups H and K such that

- (a) $H \trianglelefteq G$ (but K is not necessarily normal in G), and
- (b) $H \cap K = 1$.

It is still true that HK is a subgroup of G (Corollary 3.15) and, by Proposition 8, every element of HK can be written uniquely as a product hk , for some $h \in H$ and $k \in K$, i.e., there is a bijection between HK and the collection of ordered pairs (h, k) , given by $hk \mapsto (h, k)$ (so the group H appears as the set of elements $(h, 1)$ and K appears as the set of elements $(1, k)$). Given two elements h_1k_1 and h_2k_2 of HK , we first see how to write their product (in G) in the same form:

$$\begin{aligned} (h_1k_1)(h_2k_2) &= h_1k_1h_2(k_1^{-1}k_1)k_2 \\ &= h_1(k_1h_2k_1^{-1})k_1k_2 \\ &= h_3k_3, \end{aligned} \tag{5.1}$$

where $h_3 = h_1(k_1h_2k_1^{-1})$ and $k_3 = k_1k_2$. Note that since $H \trianglelefteq G$, $k_1h_2k_1^{-1} \in H$, so $h_3 \in H$ and $k_3 \in K$.

These calculations were predicated on the assumption that there *already existed* a group G containing subgroups H and K with $H \trianglelefteq G$ and $H \cap K = 1$. The basic idea of the semidirect product is to turn this construction around, namely start with two (abstract) groups H and K and try to *define* a group containing (an isomorphic copy of) them in such a way that (a) and (b) above hold. To do this, we write equation (1), which defines the multiplication of elements in our group, in a way that makes sense even if we do not already know there is a group containing H and K as above. The point is that k_3 in equation (1) is obtained only from multiplication in K (namely k_1k_2) and h_3 is obtained from multiplying h_1 and $k_1h_2k_1^{-1}$ in H . If we can understand where the element $k_1h_2k_1^{-1}$ arises (in terms of H and K and without reference to G), then the group HK will have been described entirely in terms of H and K . We can then use this description to *define* the group HK using equation (1) to define the multiplication.

Since H is normal in G , the group K acts on H by conjugation:

$$k \cdot h = khk^{-1} \quad \text{for } h \in H, k \in K$$

(we use the symbol \cdot to emphasize the action) so that (1) can be written

$$(h_1k_1)(h_2k_2) = (h_1k_1 \cdot h_2)(k_1k_2). \quad (5.2)$$

The action of K on H by conjugation gives a homomorphism φ of K into $\text{Aut}(H)$, so (2) shows that the multiplication in HK depends only on the multiplication in H , the multiplication in K and the homomorphism φ , hence is defined intrinsically in terms of H and K .

We now use this interpretation to define a group given two groups H and K and a homomorphism φ from K to $\text{Aut}(H)$ (which will turn out to define conjugation in the resulting group).

Theorem 10. Let H and K be groups and let φ be a homomorphism from K into $\text{Aut}(H)$. Let \cdot denote the (left) action of K on H determined by φ . Let G be the set of ordered pairs (h, k) with $h \in H$ and $k \in K$ and define the following multiplication on G :

$$(h_1, k_1)(h_2, k_2) = (h_1k_1 \cdot h_2, k_1k_2).$$

- (1) This multiplication makes G into a group of order $|G| = |H||K|$.
- (2) The sets $\{(h, 1) \mid h \in H\}$ and $\{(1, k) \mid k \in K\}$ are subgroups of G and the maps $h \mapsto (h, 1)$ for $h \in H$ and $k \mapsto (1, k)$ for $k \in K$ are isomorphisms of these subgroups with the groups H and K respectively:

$$H \cong \{(h, 1) \mid h \in H\} \quad \text{and} \quad K \cong \{(1, k) \mid k \in K\}.$$

Identifying H and K with their isomorphic copies in G described in (2) we have

- (3) $H \trianglelefteq G$
- (4) $H \cap K = 1$
- (5) for all $h \in H$ and $k \in K$, $khk^{-1} = k \cdot h = \varphi(k)(h)$.

Proof: It is straightforward to check that G is a group under this multiplication using the fact that \cdot is an action of K on H . For example, the associative law is verified as follows:

$$\begin{aligned} ((a, x)(b, y))(c, z) &= (a \cdot x \cdot b, xy)(c, z) \\ &= (a \cdot x \cdot b \cdot (xy) \cdot c, xyz) \\ &= (a \cdot x \cdot b \cdot x \cdot (y \cdot c), xyz) \\ &= (a \cdot x \cdot (b \cdot y \cdot c), xyz) \\ &= (a, x)(b \cdot y \cdot c, yz) \\ &= (a, x)((b, y)(c, z)) \end{aligned}$$

for all $(a, x), (b, y), (c, z) \in G$. We leave as an exercise the verification that (1,1) is the identity of G and that

$$(h, k)^{-1} = (k^{-1} \cdot h^{-1}, k^{-1})$$

for each $(h, k) \in G$. The order of the group G is clearly the product of the orders of H and K , which proves (1).

Let $\tilde{H} = \{(h, 1) \mid h \in H\}$ and $\tilde{K} = \{(1, k) \mid k \in K\}$. We have

$$(a, 1)(b, 1) = (a \cdot b, 1) = (ab, 1)$$

for all $a, b \in H$ and

$$(1, x)(1, y) = (1, xy)$$

for all $x, y \in K$, which show that \tilde{H} and \tilde{K} are subgroups of G and that the maps in (2) are isomorphisms.

It is clear that $\tilde{H} \cap \tilde{K} = 1$, which is (4). Now,

$$\begin{aligned}(1, k)(h, 1)(1, k)^{-1} &= ((1, k)(h, 1))(1, k^{-1}) \\ &= (k \cdot h, k)(1, k^{-1}) \\ &= (k \cdot h \cdot k^{-1}, kk^{-1}) \\ &= (k \cdot h, 1)\end{aligned}$$

so that identifying $(h, 1)$ with h and $(1, k)$ with k by the isomorphisms in (2) we have $khk^{-1} = k \cdot h$, which is (5).

Finally, we have just seen that (under the identifications in (2)) $K \leq N_G(H)$. Since $G = HK$ and certainly $H \leq N_G(H)$, we have $N_G(H) = G$, i.e., $H \trianglelefteq G$, which proves (3) and completes the proof.

Definition. Let H and K be groups and let φ be a homomorphism from K into $\text{Aut}(H)$. The group described in Theorem 10 is called the *semidirect product* of H and K with respect to φ and will be denoted by $H \rtimes_{\varphi} K$ (when there is no danger of confusion we shall simply write $H \rtimes K$).

The notation is chosen to remind us that the copy of H in $H \rtimes K$ is the normal “factor” and that the construction of a semidirect product is not symmetric in H and K (unlike that of a direct product). Before giving some examples we clarify exactly when the semidirect product of H and K is their direct product (in particular, we see that direct products are a special case of semidirect products). See also Exercise 1.

Proposition 11. Let H and K be groups and let $\varphi : K \rightarrow \text{Aut}(H)$ be a homomorphism. Then the following are equivalent:

- (1) the identity (set) map between $H \rtimes K$ and $H \times K$ is a group homomorphism (hence an isomorphism)
- (2) φ is the trivial homomorphism from K into $\text{Aut}(H)$
- (3) $K \trianglelefteq H \rtimes K$.

Proof: (1) \Rightarrow (2) By definition of the group operation in $H \rtimes K$

$$(h_1, k_1)(h_2, k_2) = (h_1 k_1 \cdot h_2, k_1 k_2)$$

for all $h_1, h_2 \in H$ and $k_1, k_2 \in K$. By assumption (1), $(h_1, k_1)(h_2, k_2) = (h_1 h_2, k_1 k_2)$. Equating the first factors of these ordered pairs gives $k_1 \cdot h_2 = h_2$ for all $h_2 \in H$ and all $k_1 \in K$, i.e., K acts trivially on H . This is (2).

(2) \Rightarrow (3) If φ is trivial, then the action of K on H is trivial, so that the elements of H commute with those of K by Theorem 10(5). In particular, H normalizes K . Since K normalizes itself, $G = HK$ normalizes K , which is (3).

(3) \Rightarrow (1) If K is normal in $H \rtimes K$ then (as in the proof of Theorem 9) for all $h \in H$ and $k \in K$, $[h, k] \in H \cap K = 1$. Thus $hk = kh$ and the action of K on H is trivial. The multiplication in the semidirect product is then the same as that in the direct product:

$$(h_1, k_1)(h_2, k_2) = (h_1 h_2, k_1 k_2)$$

for all $h_1, h_2 \in H$ and $k_1, k_2 \in K$. This gives (1) and completes the proof.

Examples

In all examples H and K are groups and φ is a homomorphism from K into $\text{Aut}(H)$ with associated action of K on H denoted by a dot. Let $G = H \rtimes K$ and as in Theorem 10 we identify H and K as subgroups of G . We shall use Propositions 4.16 and 4.17 to determine homomorphisms φ for some specific groups H . In each of the following examples the proof that φ is a homomorphism is easy (since K will often be cyclic) so the details are omitted.

- (1) Let H be any abelian group (even of infinite order) and let $K = \langle x \rangle \cong Z_2$ be the group of order 2. Define $\varphi : K \rightarrow \text{Aut}(H)$ by mapping x to the automorphism of inversion on H so that the associated action is $x \cdot h = h^{-1}$, for all $h \in H$. Then G contains the subgroup H of index 2 and

$$xhx^{-1} = h^{-1} \quad \text{for all } h \in H.$$

Of particular interest is the case when H is cyclic: if $H = Z_n$, one recognizes G as D_{2n} and if $H = \mathbb{Z}$ we denote G by D_∞ .

- (2) We can generalize the preceding example in a number of ways. One way is to let H be any abelian group and to let $K = \langle x \rangle \cong Z_{2n}$ be cyclic of order $2n$. Define φ again by mapping x to inversion, so that x^2 acts as the identity on H . In G , $xhx^{-1} = h^{-1}$ and $x^2hx^{-2} = h$ for all $h \in H$. Thus $x^2 \in Z(G)$. In particular, if $H = Z_3$ and $K = Z_4$, G is a non-abelian group of order 12 which is not isomorphic to A_4 or D_{12} (since its Sylow 2-subgroup, K , is cyclic of order 4).
- (3) Following up on the preceding example let $H = \langle h \rangle \cong Z_{2^n}$ and let $K = \langle x \rangle \cong Z_4$ with $xhx^{-1} = h^{-1}$ in G . As noted above, $x^2 \in Z(G)$. Since x inverts h (i.e., inverts H), x inverts the unique subgroup $\langle z \rangle$ of order 2 in H , where $z = h^{2^{n-1}}$. Thus $xzx^{-1} = z^{-1} = z$, so x centralizes z . It follows that $z \in Z(G)$. Thus $x^2z \in Z(G)$ hence $\langle x^2z \rangle \trianglelefteq G$. Let $\bar{G} = G/\langle x^2z \rangle$. Since x^2 and z are distinct commuting elements of order 2, the order of x^2z is 2, so $|\bar{G}| = \frac{1}{2}|G| = 2^{n+1}$. By factoring out the product x^2z to form \bar{G} we identify x^2 and $h^{2^{n-1}}$ in the quotient. In particular, when $n = 2$, both \bar{x} and \bar{h} have order 4, \bar{x} inverts \bar{h} and $\bar{h}^2 = \bar{x}^2$. It follows that $\bar{G} \cong Q_8$ in this case. In general, one can check that \bar{G} has a unique subgroup of order 2 (namely $\langle \bar{x}^2 \rangle$) which equals the center of \bar{G} . The group \bar{G} is called the *generalized quaternion group* of order 2^{n+1} and is denoted by $Q_{2^{n+1}}$:

$$Q_{2^{n+1}} = \langle h, x \mid h^{2^n} = x^4 = 1, x^{-1}hx = h^{-1}, h^{2^{n-1}} = x^2 \rangle.$$

- (4) Let $H = \mathbb{Q}$ (under addition) and let $K = \langle x \rangle \cong \mathbb{Z}$. Define φ by mapping x to the map “multiplication by 2” on H , so that x acts on $h \in H$ by $x \cdot h = 2h$. Note that multiplication by 2 is an automorphism of H because it has a 2-sided inverse, namely

multiplication by $\frac{1}{2}$. In the group G , $\mathbb{Z} \leq \mathbb{Q}$ and the conjugate $x\mathbb{Z}x^{-1}$ of \mathbb{Z} is a *proper* subgroup of \mathbb{Z} (namely $2\mathbb{Z}$). Thus $x \notin N_G(\mathbb{Z})$ even though $x\mathbb{Z}x^{-1} \leq \mathbb{Z}$ (note that $x^{-1}\mathbb{Z}x$ is not contained in \mathbb{Z}). This shows that in order to prove an element g normalizes a subgroup A in an *infinite* group it is not sufficient in general to show that the conjugate of A by g is just *contained* in A (which is sufficient for finite groups).

- (5) For H any group let $K = \text{Aut}(H)$ with φ the identity map from K to $\text{Aut}(H)$. The semidirect product $H \rtimes \text{Aut}(H)$ is called the *holomorph* of H and will be denoted by $\text{Hol}(H)$. Some holomorphs are described below; verifications of these isomorphisms are given as exercises at the end of this chapter.

- (a) $\text{Hol}(Z_2 \times Z_2) \cong S_4$.
- (b) If $|G| = n$ and $\pi : G \rightarrow S_n$ is the left regular representation (Section 4.2), then $N_{S_n}(\pi(G)) \cong \text{Hol}(G)$. In particular, since the left regular representation of a generator of Z_n is an n -cycle in S_n we obtain that for any n -cycle $(1 2 \dots n)$:

$$N_{S_n}((1 2 \dots n)) \cong \text{Hol}(Z_n) = Z_n \rtimes \text{Aut}(Z_n).$$

Note that the latter group has order $n\varphi(n)$.

- (6) Let p and q be primes with $p < q$, let $H = Z_q$ and let $K = Z_p$. We have already seen that if p does not divide $q - 1$ then every group of order pq is cyclic (see the example following Proposition 4.16). This is consistent with the fact that if p does not divide $q - 1$, there is no nontrivial homomorphism from Z_p into $\text{Aut}(Z_q)$ (the latter group is cyclic of order $q - 1$ by Proposition 4.17). Assume now that $p \mid q - 1$. By Cauchy's Theorem, $\text{Aut}(Z_q)$ contains a subgroup of order p (which is unique because $\text{Aut}(Z_q)$ is cyclic). Thus there is a nontrivial homomorphism, φ , from K into $\text{Aut}(H)$. The associated group $G = H \rtimes K$ has order pq and K is not normal in G (Proposition 11). In particular, G is non-abelian. We shall prove shortly that G is (up to isomorphism) the unique non-abelian group of order pq . If $p = 2$, G must be isomorphic to D_{2q} .
- (7) Let p be an odd prime. We construct two nonisomorphic non-abelian groups of order p^3 (we shall later prove that any non-abelian group of order p^3 is isomorphic to one of these two).

Let $H = Z_p \times Z_p$ and let $K = Z_p$. By Proposition 4.17, $\text{Aut}(H) \cong GL_2(\mathbb{F}_p)$ and $|GL_2(\mathbb{F}_p)| = (p^2 - 1)(p^2 - p)$. Since $p \mid |\text{Aut}(H)|$, by Cauchy's Theorem H has an automorphism of order p . Thus there is a nontrivial homomorphism, φ , from K into $\text{Aut}(H)$ and so the associated group $H \rtimes K$ is a non-abelian group of order p^3 . More explicitly, if $H = \langle a \rangle \times \langle b \rangle$, and x is a generator for K then x acts on a and b by

$$x \cdot a = ab \quad \text{and} \quad x \cdot b = b$$

which defines the action of x on all of H . With respect to the \mathbb{F}_p -basis a, b of the 2-dimensional vector space H the action of x (which can be considered in additive notation as a nonsingular linear transformation) has matrix

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in GL_2(\mathbb{F}_p).$$

The resulting semidirect product has the presentation

$$\langle x, a, b \mid x^p = a^p = b^p = 1, ab = ba, xax^{-1} = ab, xbx^{-1} = b \rangle$$

(in fact, this group is generated by $\{x, a\}$, and is called the *Heisenberg group* over $\mathbb{Z}/p\mathbb{Z}$, cf. Exercise 25).

Next let $H = Z_{p^2}$ and $K = Z_p$. Again by Proposition 4.17, $\text{Aut}(H) \cong Z_{p(p-1)}$, so H admits an automorphism of order p . Thus there is a nontrivial homomorphism,

φ , from K into $\text{Aut}(H)$ and so the group $H \rtimes K$ is non-abelian and of order p^3 . More explicitly, if $H = \langle y \rangle$, and x is a generator for K then x acts on y by

$$x \cdot y = y^{1+p}.$$

The resulting semidirect product has the presentation

$$\langle x, y \mid x^p = y^{p^2} = 1, xyx^{-1} = y^{1+p} \rangle.$$

These two groups are not isomorphic (the former contains no element of order p^2 , cf. Exercise 25, and the latter clearly does, namely y).

- (8) Let $H = Q_8 \times (Z_2 \times Z_2) = \langle i, j \rangle \times (\langle a \rangle \times \langle b \rangle)$ and let $K = \langle y \rangle \cong Z_3$. The map defined by

$$i \mapsto j \quad j \mapsto k = ij \quad a \mapsto b \quad b \mapsto ab$$

is easily seen to give an automorphism of H of order 3. Let φ be the homomorphism from K to $\text{Aut}(H)$ defined by mapping y to this automorphism, and let G be the associated semidirect product, so that $y \in G$ acts by

$$y \cdot i = j \quad y \cdot j = k \quad y \cdot a = b \quad y \cdot b = ab.$$

The group $G = H \rtimes K$ is a non-abelian group of order 96 with the property that the element $i^2a \in G'$ but i^2a cannot be expressed as a single commutator $[x, y]$, for any $x, y \in G$ (checking the latter assertion is an elementary calculation).

As in the case of direct products we now prove a recognition theorem for semidirect products. This theorem will enable us to “break down” or “factor” all groups of certain orders and, as a result, classify groups of those orders. The strategy is discussed in greater detail following this theorem.

Theorem 12. Suppose G is a group with subgroups H and K such that

- (1) $H \trianglelefteq G$, and
- (2) $H \cap K = 1$.

Let $\varphi : K \rightarrow \text{Aut}(H)$ be the homomorphism defined by mapping $k \in K$ to the automorphism of left conjugation by k on H . Then $HK \cong H \rtimes K$. In particular, if $G = HK$ with H and K satisfying (1) and (2), then G is the semidirect product of H and K .

Proof: Note that since $H \trianglelefteq G$, HK is a subgroup of G . By Proposition 8 every element of HK can be written uniquely in the form hk , for some $h \in H$ and $k \in K$. Thus the map $hk \mapsto (h, k)$ is a *set* bijection from HK onto $H \rtimes K$. The fact that this map is a homomorphism is the computation at the beginning of this section which led us to the formulation of the definition of the semidirect product.

Definition. Let H be a subgroup of the group G . A subgroup K of G is called a *complement* for H in G if $G = HK$ and $H \cap K = 1$.

With this terminology, the criterion for recognizing a semidirect product is simply that there must exist a complement for some proper *normal* subgroup of G . Not every group is the semidirect product of two of its proper subgroups (for example, if the group is simple), but as we have seen, the notion of a semidirect product greatly increases our list of known groups.

Some Classifications

We now apply Theorem 12 to classify groups of order n for certain values of n . The basic idea in each of the following arguments is to

- (a) show every group of order n has proper subgroups H and K satisfying the hypothesis of Theorem 12 with $G = HK$
- (b) find all possible isomorphism types for H and K
- (c) for each pair H, K found in (b) find all possible homomorphisms $\varphi : K \rightarrow \text{Aut}(H)$
- (d) for each triple H, K, φ found in (c) form the semidirect product $H \rtimes K$ (so any group G of order n is isomorphic to one of these explicitly constructed groups) and among all these semidirect products determine which pairs are isomorphic. This results in a list of the distinct isomorphism types of groups of order n .

In order to start this process we must first find subgroups H and K (of an arbitrary group G of order n) satisfying the above conditions. In the case of “small” values of n we can often do this by Sylow’s Theorem. To show *normality* of H we use the conjugacy part of Sylow’s Theorem or other normality criteria established in Chapter 4 (e.g., Corollary 4.5). Some of this work has already been done in the examples in Section 4.5. In many of the examples that follow, $|H|$ and $|K|$ are relatively prime, so $H \cap K = 1$ holds by Lagrange’s Theorem.

Since H and K are proper subgroups of G one should think of the determination of H and K as being achieved inductively. In the examples we discuss, H and K will have sufficiently small order that we shall know all possible isomorphism types from previous results. For example, in most instances H and K will be of prime or prime squared order.

There will be relatively few possible homomorphisms $\varphi : K \rightarrow \text{Aut}(H)$ in our examples, particularly after we take into account certain symmetries (such as replacing one generator of K by another when K is cyclic).

Finally, the semidirect products which emerge from this process will, in our examples, be small in number and we shall find that, for the most part, they are (pairwise) *not* isomorphic. In general, this can be a more delicate problem, as Exercise 4 indicates.

We emphasize that this approach to “factoring” every group of some given order n as a semidirect product does not work for arbitrary n . For example, Q_8 is not a semidirect product since no proper subgroup has a complement (although we saw that it is a *quotient* of a semidirect product). Empirically, this process generally works well when the group order n is not divisible by a large power of any prime. At the other extreme, only a small percentage of the groups of order p^α for large α (p a prime) are nontrivial semidirect products.

Example: (Groups of Order pq , p and q primes with $p < q$)

Let G be any group of order pq , let $P \in \text{Syl}_p(G)$ and let $Q \in \text{Syl}_q(G)$. In Example 1 of the applications of Sylow’s Theorems we proved that $G \cong Q \times P$, for some $\varphi : P \rightarrow \text{Aut}(Q)$. Since P and Q are of prime order, they are cyclic. The group $\text{Aut}(Q)$ is cyclic of order $q - 1$. If p does not divide $q - 1$, the only homomorphism from P to $\text{Aut}(Q)$ is the trivial homomorphism, hence the only semidirect product in this case is the direct product, i.e., G is cyclic.

Consider now the case when $p \mid q - 1$ and let $P = \langle y \rangle$. Since $\text{Aut}(Q)$ is cyclic it contains a unique subgroup of order p , say $\langle \gamma \rangle$, and any homomorphism $\varphi : P \rightarrow \text{Aut}(Q)$

must map y to a power of γ . There are therefore p homomorphisms $\varphi_i : P \rightarrow \text{Aut}(Q)$ given by $\varphi_i(y) = \gamma^i$, $0 \leq i \leq p - 1$. Since φ_0 is the trivial homomorphism, $Q \rtimes_{\varphi_0} P \cong Q \times P$ as before. Each φ_i for $i \neq 0$ gives rise to a non-abelian group, G_i , of order pq . It is straightforward to check that these groups are all isomorphic because for each φ_i , $i > 0$, there is some generator y_i of P such that $\varphi_i(y_i) = \gamma$. Thus, up to a choice for the (arbitrary) generator of P , these semidirect products are all the same (see Exercise 6. See also Exercise 28 of Section 4.3).

Example: (Groups of Order 30)

By the examples following Sylow's Theorem every group G of order 30 contains a subgroup H of order 15. By the preceding example H is cyclic and H is normal in G (index 2). By Sylow's Theorem there is a subgroup K of G of order 2. Thus $G = HK$ and $H \cap K = 1$ so $G \cong H \rtimes K$, for some $\varphi : K \rightarrow \text{Aut}(H)$. By Proposition 4.16,

$$\text{Aut}(Z_{15}) \cong (\mathbb{Z}/15\mathbb{Z})^\times \cong Z_4 \times Z_2.$$

The latter isomorphism can be computed directly, or one can use Exercise 11 of the preceding section: writing H as $\langle a \rangle \times \langle b \rangle \cong Z_5 \times Z_3$, we have (since these two subgroups are characteristic in H)

$$\text{Aut}(H) \cong \text{Aut}(Z_5) \times \text{Aut}(Z_3).$$

In particular, $\text{Aut}(H)$ contains precisely three elements of order 2, whose actions on the group $H = \langle a \rangle \times \langle b \rangle$ are the following:

$$\begin{cases} a &\mapsto &a \\ b &\mapsto &b^{-1} \end{cases} \quad \begin{cases} a &\mapsto &a^{-1} \\ b &\mapsto &b \end{cases} \quad \begin{cases} a &\mapsto &a^{-1} \\ b &\mapsto &b^{-1} \end{cases}.$$

Thus there are three nontrivial homomorphisms from K into $\text{Aut}(H)$ given by sending the generator of K into one of these three elements of order 2 (as usual, the trivial homomorphism gives the direct product: $H \times K \cong Z_{30}$).

Let $K = \langle k \rangle$. If the homomorphism $\varphi_1 : K \rightarrow \text{Aut}(H)$ is defined by mapping k to the first automorphism above (so that $k \cdot a = a$ and $k \cdot b = b^{-1}$ gives the action of k on H) then $G_1 = H \rtimes_{\varphi_1} K$ is easily seen to be isomorphic to $Z_5 \times D_6$ (note that in this semidirect product k centralizes the element a of H of order 5, so the factorization as a direct product is $\langle a \rangle \times \langle b, k \rangle$).

If φ_2 is defined by mapping k to the second automorphism above, then $G_2 = H \rtimes_{\varphi_2} K$ is easily seen to be isomorphic to $Z_3 \times D_{10}$ (note that in this semidirect product k centralizes the element b of H of order 3, so the factorization as a direct product is $\langle b \rangle \times \langle a, k \rangle$).

If φ_3 is defined by mapping k to the third automorphism above then $G_3 = H \rtimes_{\varphi_3} K$ is easily seen to be isomorphic to D_{30} .

Note that these groups are all nonisomorphic since their centers have orders 30 (in the abelian case), 5 (for G_1), 3 (for G_2), and 1 (for G_3).

We emphasize that although (in hindsight) this procedure does not give rise to any groups we could not already have constructed using only direct products, the argument proves that this is the *complete* list of isomorphism types of groups of order 30.

Example: (Groups of Order 12)

Let G be a group of order 12, let $V \in \text{Syl}_2(G)$ and let $T \in \text{Syl}_3(G)$. By the discussion of groups of order 12 in Section 4.5 we know that either V or T is normal in G (for purposes of illustration we shall not invoke the full force of our results from Chapter 4, namely that either $T \trianglelefteq G$ or $G \cong A_4$). By Lagrange's Theorem $V \cap T = 1$. Thus G is a semidirect product. Note that $V \cong Z_4$ or $Z_2 \times Z_2$ and $T \cong Z_3$.

Case 1: $V \trianglelefteq G$

We must determine all possible homomorphisms from T into $\text{Aut}(V)$. If $V \cong Z_4$, then $\text{Aut}(V) \cong Z_2$ and there are no nontrivial homomorphisms from T into $\text{Aut}(V)$. Thus the only group of order 12 with a normal cyclic Sylow 2-subgroup is Z_{12} .

Assume therefore that $V \cong Z_2 \times Z_2$. In this case $\text{Aut}(V) \cong S_3$ and there is a unique subgroup of $\text{Aut}(V)$ of order 3, say $\langle \gamma \rangle$. Thus if $T = \langle y \rangle$, there are three possible homomorphisms from T into $\text{Aut}(V)$:

$$\varphi_i : T \rightarrow \text{Aut}(V) \quad \text{defined by} \quad \varphi_i(y) = \gamma^i, \quad i = 0, 1, 2.$$

As usual, φ_0 is the trivial homomorphism, which gives rise to the direct product $Z_2 \times Z_2 \times Z_3$. Homomorphisms φ_1 and φ_2 give rise to isomorphic semidirect products because they differ only in the choice of a generator for T (i.e., $\varphi_1(y) = \gamma$ and $\varphi_2(y') = \gamma$, where $y' = y^2$ and y' is another choice of generator for T — see also Exercise 6). The unique non-abelian group in this case is A_4 .

Case 2: $T \trianglelefteq G$

We must determine all possible homomorphisms from V into $\text{Aut}(T)$. Note that $\text{Aut}(T) = \langle \lambda \rangle \cong Z_2$, where λ inverts T . If $V = \langle x \rangle \cong Z_4$, there are precisely two homomorphisms from V into $\text{Aut}(T)$: the trivial homomorphism and the homomorphism which sends x to λ . As usual, the trivial homomorphism gives rise to the direct product: $Z_3 \times Z_4 \cong Z_{12}$. The nontrivial homomorphism gives the semidirect product which was discussed in Example 2 following Proposition 11 of this section.

Finally, assume $V = \langle a \rangle \times \langle b \rangle \cong Z_2 \times Z_2$. There are precisely three nontrivial homomorphisms from V into $\text{Aut}(T)$ determined by specifying their kernels as one of the three subgroups of order 2 in V . For example, $\varphi_1(a) = \lambda$ and $\varphi_1(b) = \lambda$ has kernel $\langle ab \rangle$, that is, in this semidirect product both a and b act by inverting T and ab centralizes T . If φ_2 and φ_3 have kernels $\langle a \rangle$ and $\langle b \rangle$, respectively, then one easily checks that the resulting three semidirect products are all isomorphic to $S_3 \times Z_2$, where the Z_2 direct factor is the kernel of φ_i . For example,

$$T \rtimes_{\varphi_1} V = \langle a, T \rangle \times \langle ab \rangle.$$

In summary, there are precisely 5 groups of order 12, three of which are non-abelian.

Example: (Groups of Order p^3 , p an odd prime)

Let G be a group of order p^3 , p an odd prime, and assume G is not cyclic. By Exercise 9 of the previous section the map $x \mapsto x^p$ is a homomorphism from G into $Z(G)$ and the kernel of this homomorphism has order p^2 or p^3 . In the former case G must contain an element of order p^2 and in the latter case every nonidentity element of G has order p .

Case 1: G has an element of order p^2

Let x be an element of order p^2 and let $H = \langle x \rangle$. Note that since H has index p , H is normal in G by Corollary 4.5. If E is the kernel of the p^{th} power map, then in this case $E \cong Z_p \times Z_p$ and $E \cap H = \langle x^p \rangle$. Let y be any element of $E - H$ and let $K = \langle y \rangle$. By construction, $H \cap K = 1$ and so G is isomorphic to $Z_{p^2} \times Z_p$, for some $\varphi : K \rightarrow \text{Aut}(H)$. If φ is the trivial homomorphism, $G \cong Z_{p^2} \times Z_p$, so we need only consider the nontrivial homomorphisms. By Proposition 4.17 $\text{Aut}(H) \cong Z_{p(p-1)}$ is cyclic and so contains a unique subgroup of order p , explicitly given by $\langle \gamma \rangle$ where

$$\gamma(x) = x^{1+p}.$$

As usual, up to choice of a generator for the cyclic group K , there is only one nontrivial homomorphism, φ , from K into $\text{Aut}(H)$, given by $\varphi(y) = \gamma$; hence up to isomorphism

there is a unique non-abelian group $H \rtimes K$ in this case. This group is described in Example 7 above.

Case 2: every nonidentity element of G has order p

In this case let H be any subgroup of G of order p^2 (see Exercise 29, Section 4.3). Necessarily $H \cong Z_p \times Z_p$. Let $K = \langle y \rangle$ for any element y of $G - H$. Since H has index p , $H \trianglelefteq G$ and since K has order p but is not contained in H , $H \cap K = 1$. Then G is isomorphic to $(Z_p \times Z_p) \rtimes Z_p$, for some $\varphi : K \rightarrow \text{Aut}(H)$. If φ is trivial, $G \cong Z_p \times Z_p \times Z_p$ (the elementary abelian group), so we may assume φ is nontrivial. By Proposition 4.17,

$$\text{Aut}(H) \cong GL_2(\mathbb{F}_p)$$

so $|\text{Aut}(H)| = (p^2 - 1)(p^2 - p)$. Note that a Sylow p -subgroup of $\text{Aut}(H)$ has order p so all subgroups of order p in $\text{Aut}(H)$ are conjugate in $\text{Aut}(H)$ by Sylow's Theorem. Explicitly, (as discussed in Example 7 above) every subgroup of order p in $\text{Aut}(H)$ is conjugate to $\langle \gamma \rangle$, where if $H = \langle a \rangle \times \langle b \rangle$, the automorphism γ is defined by

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

With respect to the \mathbb{F}_p -basis a, b of the 2-dimensional vector space H the automorphism has matrix

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in GL_2(\mathbb{F}_p).$$

Thus (again quoting Exercise 6) there is a unique isomorphism type of semidirect product in this case.

Finally, since the two non-abelian groups have different orders for the kernels of the p^{th} power maps, they are not isomorphic. A presentation for this group is also given in Example 7 above.

EXERCISES

Let H and K be groups, let φ be a homomorphism from K into $\text{Aut}(H)$ and, as usual, identify H and K as subgroups of $G = H \rtimes_{\varphi} K$.

1. Prove that $C_K(H) = \ker \varphi$ (recall that $C_K(H) = C_G(H) \cap K$).
2. Prove that $C_H(K) = N_H(K)$.
3. In Example 1 following the proof of Proposition 11 prove that every element of $G - H$ has order 2. Prove that G is abelian if and only if $h^2 = 1$ for all $h \in H$.
4. Let $p = 2$ and check that the construction of the two non-abelian groups of order p^3 is valid in this case. Prove that *both* resulting groups are isomorphic to D_8 .
5. Let $G = \text{Hol}(Z_2 \times Z_2)$.
 - (a) Prove that $G = H \rtimes K$ where $H = Z_2 \times Z_2$ and $K \cong S_3$. Deduce that $|G| = 24$.
 - (b) Prove that G is isomorphic to S_4 . [Obtain a homomorphism from G into S_4 by letting G act on the left cosets of K . Use Exercise 1 to show this representation is faithful.]
6. Assume that K is a cyclic group, H is an arbitrary group and φ_1 and φ_2 are homomorphisms from K into $\text{Aut}(H)$ such that $\varphi_1(K)$ and $\varphi_2(K)$ are conjugate subgroups of $\text{Aut}(H)$. If K is infinite assume φ_1 and φ_2 are injective. Prove by constructing an explicit isomorphism that $H \rtimes_{\varphi_1} K \cong H \rtimes_{\varphi_2} K$ (in particular, if the subgroups $\varphi_1(K)$ and $\varphi_2(K)$ are equal in $\text{Aut}(H)$, then the resulting semidirect products are isomorphic). [Suppose $\sigma \varphi_1(k) \sigma^{-1} = \varphi_2(k)$ so that for some $a \in \mathbb{Z}$ we have $\sigma \varphi_1(k) \sigma^{-1} = \varphi_2(k)^a$ for all $k \in K$. Show that the map

$\psi : H \times_{\varphi_1} K \rightarrow H \times_{\varphi_2} K$ defined by $\psi((h, k)) = (\sigma(h), k^a)$ is a homomorphism. Show ψ is bijective by constructing a 2-sided inverse.]

7. This exercise describes thirteen isomorphism types of groups of order 56. (It is not too difficult to show that every group of order 56 is isomorphic to one of these.)
 - (a) Prove that there are three abelian groups of order 56.
 - (b) Prove that every group of order 56 has either a normal Sylow 2-subgroup or a normal Sylow 7-subgroup.
 - (c) Construct the following non-abelian groups of order 56 which have a normal Sylow 7-subgroup and whose Sylow 2-subgroup S is as specified:
 - one group when $S \cong Z_2 \times Z_2 \times Z_2$
 - two nonisomorphic groups when $S \cong Z_4 \times Z_2$
 - one group when $S \cong Z_8$
 - two nonisomorphic groups when $S \cong Q_8$
 - three nonisomorphic groups when $S \cong D_8$.

[For a particular S , two groups are not isomorphic if the kernels of the maps from S into $\text{Aut}(Z_7)$ are not isomorphic.]
 - (d) Let G be a group of order 56 with a nonnormal Sylow 7-subgroup. Prove that if S is the Sylow 2-subgroup of G then $S \cong Z_2 \times Z_2 \times Z_2$. [Let an element of order 7 act by conjugation on the seven nonidentity elements of S and deduce that they all have the same order.]
 - (e) Prove that there is a unique group of order 56 with a nonnormal Sylow 7-subgroup. [For existence use the fact that $|GL_3(\mathbb{F}_2)| = 168$; for uniqueness use Exercise 6.]
8. Construct a non-abelian group of order 75. Classify all groups of order 75 (there are three of them). [Use Exercise 6 to show that the non-abelian group is unique.] (The classification of groups of order pq^2 , where p and q are primes with $p < q$ and p not dividing $q - 1$, is quite similar.)
9. Show that the matrix $\begin{pmatrix} 0 & -1 \\ 1 & 4 \end{pmatrix}$ is an element of order 5 in $GL_2(\mathbb{F}_{19})$. Use this matrix to construct a non-abelian group of order 1805 and give a presentation of this group. Classify groups of order 1805 (there are three isomorphism types). [Use Exercise 6 to prove uniqueness of the non-abelian group.] (A general method for finding elements of prime order in $GL_n(\mathbb{F}_p)$ is described in the exercises in Section 12.2; this particular matrix of order 5 in $GL_2(\mathbb{F}_{19})$ appears in Exercise 16 of that section as an illustration of the method.)
10. This exercise classifies the groups of order 147 (there are six isomorphism types).
 - (a) Prove that there are two abelian groups of order 147.
 - (b) Prove that every group of order 147 has a normal Sylow 7-subgroup.
 - (c) Prove that there is a unique non-abelian group whose Sylow 7-subgroup is cyclic.
 - (d) Let $t_1 = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ and $t_2 = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ be elements of $GL_2(\mathbb{F}_7)$. Prove $P = \langle t_1, t_2 \rangle$ is a Sylow 3-subgroup of $GL_2(\mathbb{F}_7)$ and that $P \cong Z_3 \times Z_3$. Deduce that every subgroup of $GL_2(\mathbb{F}_7)$ of order 3 is conjugate in $GL_2(\mathbb{F}_7)$ to a subgroup of P .
 - (e) By Example 3 in Section 1 the group P has four subgroups of order 3 and these are: $P_1 = \langle t_1 \rangle$, $P_2 = \langle t_2 \rangle$, $P_3 = \langle t_1 t_2 \rangle$, and $P_4 = \langle t_1 t_2^2 \rangle$. For $i = 1, 2, 3, 4$ let $G_i = (Z_7 \times Z_7) \times_{\varphi_i} Z_3$, where φ_i is an isomorphism of Z_3 with the subgroup P_i of $\text{Aut}(Z_7 \times Z_7)$. For each i describe G_i in terms of generators and relations. Deduce that $G_1 \cong G_2$.
 - (f) Prove that G_1 is not isomorphic to either G_3 or G_4 . [Show that the center of G_1 has

order 7 whereas the centers of G_3 and G_4 are trivial.]

- (g) Prove that G_3 is not isomorphic to G_4 . [Show that every subgroup of order 7 in G_3 is normal in G_3 but that G_4 has subgroups of order 7 that are not normal.]
- (h) Classify the groups of order 147 by showing that the six nonisomorphic groups described above (two from part (a), one from part (c) and G_1 , G_3 , and G_4) are all the groups of order 147. [Use Exercise 6 and part (d).] (The classification of groups of order pq^2 , where p and q are primes with $p < q$ and $p \mid q - 1$, is quite similar.)

11. Classify groups of order 28 (there are four isomorphism types).
12. Classify the groups of order 20 (there are five isomorphism types).
13. Classify groups of order $4p$, where p is a prime greater than 3. [There are four isomorphism types when $p \equiv 3(\text{mod } 4)$ and five isomorphism types when $p \equiv 1(\text{mod } 4)$.]
14. This exercise classifies the groups of order 60 (there are thirteen isomorphism types). Let G be a group of order 60, let P be a Sylow 5-subgroup of G and let Q be a Sylow 3-subgroup of G .
- (a) Prove that if P is not normal in G then $G \cong A_5$. [See Section 4.5.]
 - (b) Prove that if $P \trianglelefteq G$ but Q is not normal in G then $G \cong A_4 \times Z_5$. [Show in this case that $P \leq Z(G)$, $G/P \cong A_4$, a Sylow 2-subgroup T of G is normal and $TQ \cong A_4$.]
 - (c) Prove that if both P and Q are normal in G then $G \cong Z_{15} \rtimes T$ where $T \cong Z_4$ or $Z_2 \times Z_2$. Show in this case that there are six isomorphism types when T is cyclic (one abelian) and there are five isomorphism types when T is the Klein 4-group (one abelian). [Use the same ideas as in the classifications of groups of orders 30 and 20.]
15. Let p be an odd prime. Prove that every element of order 2 in $GL_2(\mathbb{F}_p)$ is conjugate to a diagonal matrix with ± 1 's on the diagonal. Classify the groups of order $2p^2$. [If A is a 2×2 matrix with $A^2 = I$ and v_1, v_2 is a basis for the underlying vector space, look at A acting on the vectors $w_1 = v_1 + v_2$ and $w_2 = v_1 - v_2$.]
16. Show that there are exactly 4 distinct homomorphisms from Z_2 into $\text{Aut}(Z_8)$. Prove that the resulting semidirect products are the groups: $Z_8 \times Z_2$, D_{16} , the quasidihedral group QD_{16} and the modular group M (cf. the exercises in Section 2.5).
17. Show that for any $n \geq 3$ there are exactly 4 distinct homomorphisms from Z_2 into $\text{Aut}(Z_{2^n})$. Prove that the resulting semidirect products give 4 nonisomorphic groups of order 2^{n+1} . [Recall Exercises 21 to 23 in Section 2.3.] (These four groups together with the cyclic group and the generalized quaternion group, $Q_{2^{n+1}}$, are all the groups of order 2^{n+1} which possess a cyclic subgroup of index 2.)
18. Show that if H is any group then there is a group G that contains H as a normal subgroup with the property that for every automorphism σ of H there is an element $g \in G$ such that conjugation by g when restricted to H is the given automorphism σ , i.e., every automorphism of H is obtained as an inner automorphism of G restricted to H .
19. Let H be a group of order n , let $K = \text{Aut}(H)$ and form $G = \text{Hol}(H) = H \rtimes K$ (where φ is the identity homomorphism). Let G act by left multiplication on the left cosets of K in G and let π be the associated permutation representation $\pi : G \rightarrow S_n$.
- (a) Prove the elements of H are coset representatives for the left cosets of K in G and with this choice of coset representatives π restricted to H is the regular representation of H .
 - (b) Prove $\pi(G)$ is the normalizer in S_n of $\pi(H)$. Deduce that under the regular representation of any finite group H of order n , the normalizer in S_n of the image of H is isomorphic to $\text{Hol}(H)$. [Show $|G| = |N_{S_n}(\pi(H))|$ using Exercises 1 and 2 above.]
 - (c) Deduce that the normalizer of the group generated by an n -cycle in S_n is isomorphic to $\text{Hol}(Z_n)$ and has order $n\varphi(n)$.

20. Let p be an odd prime. Prove that if P is a non-cyclic p -group then P contains a normal subgroup U with $U \cong Z_p \times Z_p$. Deduce that for odd primes p a p -group that contains a unique subgroup of order p is cyclic. (For $p = 2$ it is a theorem that the generalized quaternion groups Q_{2^n} are the only non-cyclic 2-groups which contain a unique subgroup of order 2). [Proceed by induction on $|P|$. Let Z be a subgroup of order p in $Z(P)$ and let $\bar{P} = P/Z$. If \bar{P} is cyclic then P is abelian by Exercise 36 in Section 3.1 — show the result is true for abelian groups. When \bar{P} is not cyclic use induction to produce a normal subgroup \bar{H} of \bar{P} with $\bar{H} \cong Z_p \times Z_p$. Let H be the complete preimage of \bar{H} in P , so $|H| = p^3$. Let $H_0 = \{x \in H \mid x^p = 1\}$ so that H_0 is a characteristic subgroup of H of order p^2 or p^3 by Exercise 9 in Section 4. Show that a suitable subgroup of H_0 gives the desired normal subgroup U .]
21. Let p be an odd prime and let P be a p -group. Prove that if every subgroup of P is normal then P is abelian. (Note that Q_8 is a non-abelian 2-group with this property, so the result is false for $p = 2$). [Use the preceding exercises and Exercise 15 of Section 4.]
22. Let F be a field let n be a positive integer and let G be the group of upper triangular matrices in $GL_n(F)$ (cf. Exercise 16, Section 2.1)
- (a) Prove that G is the semidirect product $U \rtimes D$ where U is the set of upper triangular matrices with 1's down the diagonal (cf. Exercise 17, Section 2.1) and D is the set of diagonal matrices in $GL_n(F)$.
 - (b) Let $n=2$. Recall that $U \cong F$ and $D \cong F^\times \times F^\times$ (cf. Exercise 11 in Section 3.1). Describe the homomorphism from D into $\text{Aut}(U)$ explicitly in terms of these isomorphisms (i.e., show how each element of $F^\times \times F^\times$ acts as an automorphism on F).
23. Let K and L be groups, let n be a positive integer, let $\rho : K \rightarrow S_n$ be a homomorphism and let H be the direct product of n copies of L . In Exercise 8 of Section 1 an injective homomorphism ψ from S_n into $\text{Aut}(H)$ was constructed by letting the elements of S_n permute the n factors of H . The composition $\psi \circ \rho$ is a homomorphism from G into $\text{Aut}(H)$. The *wreath product* of L by K is the semidirect product $H \rtimes K$ with respect to this homomorphism and is denoted by $L \wr K$ (this wreath product depends on the choice of permutation representation ρ of K — if none is given explicitly, ρ is assumed to be the left regular representation of K).
- (a) Assume K and L are finite groups and ρ is the left regular representation of K . Find $|L \wr K|$ in terms of $|K|$ and $|L|$.
 - (b) Let p be a prime, let $K = L = Z_p$ and let ρ be the left regular representation of K . Prove that $Z_p \wr Z_p$ is a non-abelian group of order p^{p+1} and is isomorphic to a Sylow p -subgroup of S_{p^2} . [The p copies of Z_p whose direct product makes up H may be represented by p disjoint p -cycles; these are cyclically permuted by K .]
24. Let n be an integer > 1 . Prove the following classification: every group of order n is abelian if and only if $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, where p_1, \dots, p_r are distinct primes, $\alpha_i = 1$ or 2 for all $i \in \{1, \dots, r\}$ and p_i does not divide $p_j^{\alpha_j} - 1$ for all i and j . [See Exercise 56 in Section 4.5.]
25. Let $H(\mathbb{F}_p)$ be the Heisenberg group over the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (cf. Exercise 20 in Section 4). Prove that $H(\mathbb{F}_2) \cong D_8$, and that $H(\mathbb{F}_p)$ has exponent p and is isomorphic to the first non-abelian group in Example 7.

CHAPTER 6

Further Topics in Group Theory

6.1 p -GROUPS, NILPOTENT GROUPS, AND SOLVABLE GROUPS

Let p be a prime and let G be a finite group of order $p^a n$, where p does not divide n . Recall that a (finite) p -group is any group whose order is a power of p . Sylow's Theorem shows that p -groups abound as subgroups of G and in order to exploit this phenomenon to unravel the structure of finite groups it will be necessary to establish some basic properties of p -groups. In the next section we shall apply these results in many specific instances.

Before giving the results on p -groups we first recall a definition that has appeared in some earlier exercises.

Definition. A *maximal subgroup* of a group G is a proper subgroup M of G such that there are no subgroups H of G with $M < H < G$.

By order considerations every proper subgroup of a finite group is contained in some maximal subgroup. In contrast, infinite groups may or may not have maximal subgroups. For example, $p\mathbb{Z}$ is a maximal subgroup of \mathbb{Z} whereas \mathbb{Q} (under $+$) has no maximal subgroups (cf. Exercise 16 at the end of this section).

We now collect all the properties of p -groups we shall need into an omnibus theorem:

Theorem 1. Let p be a prime and let P be a group of order p^a , $a \geq 1$. Then

- (1) The center of P is nontrivial: $Z(P) \neq 1$.
- (2) If H is a nontrivial normal subgroup of P then H intersects the center nontrivially: $H \cap Z(P) \neq 1$. In particular, every normal subgroup of order p is contained in the center.
- (3) If H is a normal subgroup of P then H contains a subgroup of order p^b that is normal in P for each divisor p^b of $|H|$. In particular, P has a normal subgroup of order p^b for every $b \in \{0, 1, \dots, a\}$.
- (4) If $H < P$ then $H < N_P(H)$ (i.e., every proper subgroup of P is a proper subgroup of its normalizer in P).
- (5) Every maximal subgroup of P is of index p and is normal in P .

Proof: These results rely ultimately on the class equation and it may be useful for the reader to review Section 4.3.

Part 1 is Theorem 8 of Chapter 4 and is also the special case of part 2 when $H = P$. We therefore begin by proving (2); we shall not quote Theorem 8 of Chapter 4 although the argument that follows is only a slight generalization of the one in Chapter 4. Let H be a nontrivial normal subgroup of P . Recall that for each conjugacy class \mathcal{C} of P , either $\mathcal{C} \subseteq H$ or $\mathcal{C} \cap H = \emptyset$ because H is normal (this easy fact was shown in a remark preceding Theorem 4.12). Pick representatives of the conjugacy classes of P :

$$a_1, a_2, \dots, a_r$$

with $a_1, \dots, a_k \in H$ and $a_{k+1}, \dots, a_r \notin H$. Let \mathcal{C}_i be the conjugacy class of a_i in P , for all i . Thus

$$\mathcal{C}_i \subseteq H, \quad 1 \leq i \leq k \quad \text{and} \quad \mathcal{C}_i \cap H = \emptyset, \quad k+1 \leq i \leq r.$$

By renumbering a_1, \dots, a_k if necessary we may assume a_1, \dots, a_s represent classes of size 1 (i.e., are in the center of P) and a_{s+1}, \dots, a_k represent classes of size > 1 . Since H is the disjoint union of these we have

$$|H| = |H \cap Z(P)| + \sum_{i=s+1}^k \frac{|P|}{|C_P(a_i)|}.$$

Now p divides $|H|$ and p divides each term in the sum $\sum_{i=s+1}^k |P : C_P(a_i)|$ so p divides their difference: $|H \cap Z(P)|$. This proves $H \cap Z(P) \neq 1$. If $|H| = p$, since $H \cap Z(P) \neq 1$ we must have $H \leq Z(P)$. This completes the proof of (2).

Next we prove (3) by induction on a . If $a \leq 1$ or $H = 1$, the result is trivial. Assume therefore that $a > 1$ and $H \neq 1$. By part 2, $H \cap Z(P) \neq 1$ so by Cauchy's Theorem $H \cap Z(P)$ contains a (normal) subgroup Z of order p . Use bar notation to denote passage to the quotient group P/Z . This quotient has order p^{a-1} and $\bar{H} \trianglelefteq \bar{P}$. By induction, for every nonnegative integer b such that p^b divides $|\bar{H}|$ there is a subgroup \bar{K} of \bar{H} of order p^b that is normal in \bar{P} . If K is the complete preimage of \bar{K} in P then $|K| = p^{b+1}$. The set of all subgroups of H obtained by this process together with the identity subgroup provides a subgroup of H that is normal in P for each divisor of $|H|$. The second assertion of part 3 is the special case $H = P$. This establishes part 3.

We prove (4) also by induction on $|P|$. If P is abelian then all subgroups of P are normal in P and the result is trivial. We may therefore assume $|P| > p$ (in fact, $|P| > p^2$ by Corollary 4.9). Let H be a proper subgroup of P . Since all elements of $Z(P)$ commute with all elements of P , $Z(P)$ normalizes every subgroup of P . By part 1 we have that $Z(P) \neq 1$. If $Z(P)$ is not contained in H , then H is properly contained in $(H, Z(P))$ and the latter subgroup is contained in $N_P(H)$ so (4) holds. We may therefore assume $Z(P) \leq H$. Use bar notation to denote passage to the quotient $P/Z(P)$. Since \bar{P} has smaller order than P by (1), by induction \bar{H} is properly contained in $N_{\bar{P}}(\bar{H})$. It follows directly from the Lattice Isomorphism Theorem that $N_P(H)$ is the complete preimage in P of $N_{\bar{P}}(\bar{H})$, hence we obtain proper containment of H in its normalizer in this case as well. This completes the induction.

To prove (5) let M be a maximal subgroup of P . By definition, $M < P$ so by part 4, $M < N_P(M)$. By definition of maximality we must therefore have $N_P(M) = P$, i.e., $M \trianglelefteq P$. The Lattice Isomorphism Theorem shows that P/M is a p -group with no proper nontrivial subgroups because M is a maximal subgroup. By part 3, however,

P/M has subgroups of every order dividing $|P/M|$. The only possibility is $|P/M| = p$. This proves (5) and completes the proof of the theorem.

Definition.

- (1) For any (finite or infinite) group G define the following subgroups inductively:

$$Z_0(G) = 1, \quad Z_1(G) = Z(G)$$

and $Z_{i+1}(G)$ is the subgroup of G containing $Z_i(G)$ such that

$$Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$$

(i.e., $Z_{i+1}(G)$ is the complete preimage in G of the center of $G/Z_i(G)$ under the natural projection). The chain of subgroups

$$Z_0(G) \leq Z_1(G) \leq Z_2(G) \leq \dots$$

is called the *upper central series of G* . (The use of the term “upper” indicates that $Z_i(G) \leq Z_{i+1}(G)$.)

- (2) A group G is called *nilpotent* if $Z_c(G) = G$ for some $c \in \mathbb{Z}$. The smallest such c is called the *nilpotence class* of G .

One of the exercises at the end of this section shows that $Z_i(G)$ is a characteristic (hence normal) subgroup of G for all i . We use this fact freely from now on.

Remarks:

- (1) If G is abelian then G is nilpotent (of class 1, provided $|G| > 1$), since in this case $G = Z(G) = Z_1(G)$. One should think of nilpotent groups as lying between abelian and solvable groups in the hierarchy of structure (recall that solvable groups were introduced in Section 3.4; we shall discuss solvable groups further at the end of this section):

cyclic groups \subset *abelian groups* \subset *nilpotent groups* \subset *solvable groups* \subset *all groups*

(all of the above containments are proper, as we shall verify shortly).

- (2) For any finite group there must, by order considerations, be an integer n such that

$$Z_n(G) = Z_{n+1}(G) = Z_{n+2}(G) = \dots$$

For example, $Z_n(S_3) = 1$ for all $n \in \mathbb{Z}^+$. Once two terms in the upper central series are the same, the chain stabilizes at that point (i.e., all terms thereafter are equal to these two). For example, if $G = Z_2 \times S_3$,

$$Z(G) = Z_1(G) = Z_2(G) = Z_n(G) \text{ has order 2 for all } n.$$

By definition, $Z_n(G)$ is a proper subgroup of G for all n for non-nilpotent groups.

- (3) For infinite groups G it may happen that all $Z_i(G)$ are proper subgroups of G (so G is not nilpotent) but

$$G = \bigcup_{i=0}^{\infty} Z_i(G).$$

Groups for which this hold are called *hypernilpotent* — they enjoy some (but not all) of the properties of nilpotent groups. While we shall be dealing mainly with finite nilpotent groups, results that do not involve the notion of order, Sylow subgroups etc. also hold for infinite groups. Even for infinite groups one of the main techniques for dealing with nilpotent groups is induction on the nilpotence class.

Proposition 2. Let p be a prime and let P be a group of order p^a . Then P is nilpotent of nilpotence class at most $a - 1$.

Proof: For each $i \geq 0$, $P/Z_i(P)$ is a p -group, so

$$\text{if } |P/Z_i(P)| > 1 \text{ then } Z(P/Z_i(P)) \neq 1$$

by Theorem 1(1). Thus if $Z_i(P) \neq G$ then $|Z_{i+1}(P)| \geq p|Z_i(P)|$ and so $|Z_{i+1}(P)| \geq p^{i+1}$. In particular, $|Z_a(P)| \geq p^a$, so $P = Z_a(P)$. Thus P is nilpotent of class $\leq a$. The only way P could be of nilpotence class exactly equal to a would be if $|Z_i(P)| = p^i$ for all i . In this case, however, $Z_{a-2}(P)$ would have index p^2 in P , so $P/Z_{a-2}(P)$ would be abelian (by Corollary 4.9). But then $P/Z_{a-2}(P)$ would equal its center and so $Z_{a-1}(P)$ would equal P , a contradiction. This proves that the class of P is $\leq a - 1$.

Example

Both D_8 and Q_8 are nilpotent of class 2. More generally, D_{2^n} is nilpotent of class $n - 1$. This can be proved inductively by showing that $|Z(D_{2^n})| = 2$ and $D_{2^n}/Z(D_{2^n}) \cong D_{2^{n-1}}$ for $n \geq 3$ (the details are left as an exercise). If n is not a power of 2, D_{2^n} is not nilpotent (cf. Exercise 10).

We now give some equivalent (and often more workable) characterizations of nilpotence for *finite* groups:

Theorem 3. Let G be a finite group, let p_1, p_2, \dots, p_s be the distinct primes dividing its order and let $P_i \in \text{Syl}_{p_i}(G)$, $1 \leq i \leq s$. Then the following are equivalent:

- (1) G is nilpotent
- (2) if $H < G$ then $H < N_G(H)$, i.e., every proper subgroup of G is a proper subgroup of its normalizer in G
- (3) $P_i \trianglelefteq G$ for $1 \leq i \leq s$, i.e., every Sylow subgroup is normal in G
- (4) $G \cong P_1 \times P_2 \times \cdots \times P_s$.

Proof: The proof that (1) implies (2) is the same argument as for p -groups — the only fact we needed was if G is nilpotent then so is $G/Z(G)$ — so the details are omitted (cf. the exercises).

To show that (2) implies (3) let $P = P_i$ for some i and let $N = N_G(P)$. Since $P \trianglelefteq N$, Corollary 4.20 gives that P is characteristic in N . Since $P \text{ char } N \trianglelefteq N_G(N)$ we get that $P \trianglelefteq N_G(N)$. This means $N_G(N) \leq N$ and hence $N_G(N) = N$. By (2) we must therefore have $N = G$, which gives (3).

Next we prove (3) implies (4). For any t , $1 \leq t \leq s$ we show inductively that

$$P_1 P_2 \cdots P_t \cong P_1 \times P_2 \times \cdots \times P_t.$$

Note first that each P_i is normal in G so $P_1 \cdots P_t$ is a subgroup of G . Let H be the product $P_1 \cdots P_{t-1}$ and let $K = P_t$, so by induction $H \cong P_1 \times \cdots \times P_{t-1}$. In particular, $|H| = |P_1| \cdot |P_2| \cdots |P_{t-1}|$. Since $|K| = |P_t|$, the orders of H and K are relatively prime. Lagrange's Theorem implies $H \cap K = 1$. By definition, $P_1 \cdots P_t = HK$, hence Theorem 5.9 gives

$$HK \cong H \times K = (P_1 \times \cdots \times P_{t-1}) \times P_t \cong P_1 \times \cdots \times P_t$$

which completes the induction. Now take $t = s$ to obtain (4).

Finally, to prove (4) implies (1) use Exercise 1 of Section 5.1 to obtain

$$Z(P_1 \times \cdots \times P_s) \cong Z(P_1) \times \cdots \times Z(P_s).$$

By Exercise 14 in Section 5.1,

$$G/Z(G) = (P_1/Z(P_1)) \times \cdots \times (P_s/Z(P_s)).$$

Thus the hypotheses of (4) also hold for $G/Z(G)$. By Theorem 1, if $P_i \neq 1$ then $Z(P_i) \neq 1$, so if $G \neq 1$, $|G/Z(G)| < |G|$. By induction, $G/Z(G)$ is nilpotent, so by Exercise 6, G is nilpotent. This completes the proof.

Note that the first part of the Fundamental Theorem of Finite Abelian Groups (Theorem 5 in Section 5.2) follows immediately from the above theorem (we shall give another proof later as a consequence of the Chinese Remainder Theorem):

Corollary 4. A finite abelian group is the direct product of its Sylow subgroups.

Next we prove a proposition which will be used later to show that the multiplicative group of a finite field is cyclic (without using the Fundamental Theorem of Finite Abelian Groups).

Proposition 5. If G is a finite group such that for all positive integers n dividing its order, G contains at most n elements x satisfying $x^n = 1$, then G is cyclic.

Proof: Let $|G| = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ and let P_i be a Sylow p_i -subgroup of G for $i = 1, 2, \dots, s$. Since $p_i^{\alpha_i} \mid |G|$ and the $p_i^{\alpha_i}$ elements of P_i are solutions of $x^{p_i^{\alpha_i}} = 1$, by hypothesis P_i must contain *all* solutions to this equation in G . It follows that P_i is the unique (hence normal) Sylow p_i -subgroup of G . By Theorem 3, G is the direct product of its Sylow subgroups. By Theorem 1, each P_i possesses a normal subgroup M_i of index p_i . Since $|M_i| = p_i^{\alpha_i-1}$ and G has at most $p_i^{\alpha_i-1}$ solutions to $x^{p_i^{\alpha_i-1}} = 1$, by Lagrange's Theorem (Corollary 9, Section 3.2) M contains all elements x of G satisfying $x^{p_i^{\alpha_i-1}} = 1$. Thus any element of P_i not contained in M_i satisfies $x^{p_i^{\alpha_i}} = 1$ but $x^{p_i^{\alpha_i-1}} \neq 1$, i.e., x is an element of order $p_i^{\alpha_i}$. This proves P_i is cyclic for all i , so G is the direct product of cyclic groups of relatively prime order, hence is cyclic.

The next proposition is called Frattini's Argument. We shall apply it to give another characterization of finite nilpotent groups. It will also be a valuable tool in the next section.

Proposition 6. (Frattini's Argument) Let G be a finite group, let H be a normal subgroup of G and let P be a Sylow p -subgroup of H . Then $G = HN_G(P)$ and $|G : H|$ divides $|N_G(P)|$.

Proof: By Corollary 3.15, $HN_G(P)$ is a subgroup of G and $HN_G(P) = N_G(P)H$ since H is a normal subgroup of G . Let $g \in G$. Since $P^g \leq H^g = H$, both P and P^g are Sylow p -subgroups of H . By Sylow's Theorem applied in H , there exists $x \in H$ such that $P^g = P^x$. Thus $gx^{-1} \in N_G(P)$ and so $g \in N_G(P)x$. Since g was an arbitrary element of G , this proves $G = N_G(P)H$.

Apply the Second Isomorphism Theorem to $G = N_G(P)H$ to conclude that

$$|G : H| = |N_G(P) : N_G(P) \cap H|$$

so $|G : H|$ divides $|N_G(P)|$, completing the proof.

Proposition 7. A finite group is nilpotent if and only if every maximal subgroup is normal.

Proof: Let G be a finite nilpotent group and let M be a maximal subgroup of G . As in the proof of Theorem 1, since $M < N_G(M)$ (by Theorem 3(2)) maximality of M forces $N_G(M) = G$, i.e., $M \trianglelefteq G$.

Conversely, assume every maximal subgroup of the finite group G is normal. Let P be a Sylow p -subgroup of G . We prove $P \trianglelefteq G$ and conclude that G is nilpotent by Theorem 3(3). If P is not normal in G let M be a maximal subgroup of G containing $N_G(P)$. By hypothesis, $M \trianglelefteq G$ hence by Frattini's Argument $G = MN_G(P)$. Since $N_G(P) \leq M$ we have $MN_G(P) = M$, a contradiction. This establishes the converse.

Commutators and the Lower Central Series

For the sake of completeness we include the definition of the *lower central series* of a group and state its relation to the upper central series. Since we shall not be using these results in the future, the proofs are left as (straightforward) exercises.

Recall that the commutator of two elements x, y in a group G is defined as

$$[x, y] = x^{-1}y^{-1}xy,$$

and the commutator of two subgroups H and K of G is

$$[H, K] = \langle [h, k] \mid h \in H, k \in K \rangle.$$

Basic properties of commutators and the commutator subgroup were established in Section 5.4.

Definition. For any (finite or infinite) group G define the following subgroups inductively:

$$G^0 = G, \quad G^1 = [G, G] \quad \text{and} \quad G^{i+1} = [G, G^i].$$

The chain of groups

$$G^0 \geq G^1 \geq G^2 \geq \dots$$

is called the *lower central series* of G . (The term “lower” indicates that $G^i \geq G^{i+1}$.)

As with the upper central series we include in the exercises at the end of this section the verification that G^i is a characteristic subgroup of G for all i . The next theorem shows the relation between the upper and lower central series of a group.

Theorem 8. A group G is nilpotent if and only if $G^n = 1$ for some $n \geq 0$. More precisely, G is nilpotent of class c if and only if c is the smallest nonnegative integer such that $G^c = 1$. If G is nilpotent of class c then

$$Z_i(G) \leq G^{c-i-1} \leq Z_{i+1}(G) \quad \text{for all } i \in \{0, 1, \dots, c-1\}.$$

Proof: This is proved by a straightforward induction on the length of either the upper or lower central series.

The terms of the upper and lower central series do not necessarily coincide in general although in some groups this does occur.

Remarks:

- (1) If G is abelian, we have already seen that $G' = G^1 = 1$ so the lower central series terminates in the identity after one term.
- (2) As with the upper central series, for any finite group there must, by order considerations, be an integer n such that

$$G^n = G^{n+1} = G^{n+2} = \dots$$

For non-nilpotent groups, G^n is a nontrivial subgroup of G . For example, in Section 5.4 we showed that $S_3' = S_3^1 = A_3$. Since S_3 is not nilpotent, we must have $S_3^2 = A_3$. In fact

$$(123) = [(12), (132)] \in [S_3, S_3^1] = S_3^2.$$

Once two terms in the lower central series are the same, the chain stabilizes at that point i.e., all terms thereafter are equal to these two. Thus $S_3^i = A_3$ for all $i \geq 2$. Note that S_3 is an example where the lower central series has two distinct terms whereas all terms in the upper central series are equal to the identity (in particular, for non-nilpotent groups these series need not have the same length).

Solvable Groups and the Derived Series

Recall that in Section 3.4 a solvable group was defined as one possessing a series:

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \dots \trianglelefteq H_s = G$$

such that each factor H_{i+1}/H_i is abelian. We now give another characterization of solvability in terms of a descending series of characteristic subgroups.

Definition. For any group G define the following sequence of subgroups inductively:

$$G^{(0)} = G, \quad G^{(1)} = [G, G] \quad \text{and} \quad G^{(i+1)} = [G^{(i)}, G^{(i)}] \quad \text{for all } i \geq 1.$$

This series of subgroups is called the *derived* or *commutator* series of G .

The terms of this series are also often written as: $G^{(1)} = G'$, $G^{(2)} = G''$, etc. Again it is left as an exercise to show that each $G^{(i)}$ is characteristic in G for all i .

It is important to note that although $G^{(0)} = G^0$ and $G^{(1)} = G^1$, it is not in general true that $G^{(i)} = G^i$. The difference is that the definition of the $i+1^{\text{st}}$ term in the lower central series is the commutator of the i^{th} term with the *whole* group G whereas the $i+1^{\text{st}}$ term in the derived series is the commutator of the i^{th} term with itself. Hence

$$G^{(i)} \leq G^i \quad \text{for all } i$$

and the containment can be proper. For example, in $G = S_3$ we have already seen that $G^1 = G' = A_3$ and $G^2 = [S_3, A_3] = A_3$, whereas $G^{(2)} = [A_3, A_3] = 1$ (A_3 being abelian).

Theorem 9. A group G is solvable if and only if $G^{(n)} = 1$ for some $n \geq 0$.

Proof: Assume first that G is solvable and so possesses a series

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_s = G$$

such that each factor H_{i+1}/H_i is abelian. We prove by induction that $G^{(i)} \leq H_{s-i}$. This is true for $i = 0$, so assume $G^{(i)} \leq H_{s-i}$. Then

$$G^{(i+1)} = [G^{(i)}, G^{(i)}] \leq [H_{s-i}, H_{s-i}].$$

Since H_{s-i}/H_{s-i-1} is abelian, by Proposition 5.7(4), $[H_{s-i}, H_{s-i}] \leq H_{s-i-1}$. Thus $G^{(i+1)} \leq H_{s-i-1}$, which completes the induction. Since $H_0 = 1$ we have $G^{(s)} = 1$.

Conversely, if $G^{(n)} = 1$ for some $n \geq 0$, Proposition 5.7(4) shows that if we take H_i to be $G^{(n-i)}$ then H_i is a normal subgroup of H_{i+1} with abelian quotient, so the derived series itself satisfies the defining condition for solvability of G . This completes the proof.

If G is solvable, the smallest nonnegative n for which $G^{(n)} = 1$ is called the *solvable length* of G . The derived series is a series of shortest length whose successive quotients are abelian and it has the additional property that it consists of subgroups that are characteristic in the *whole* group (as opposed to each just being normal in the *next* in the initial definition of solvability). Its “intrinsic” definition also makes it easier to work with in many instances, as the following proposition (which reproves some results and exercises from Section 3.4) illustrates.

Proposition 10. Let G and K be groups, let H be a subgroup of G and let $\varphi : G \rightarrow K$ be a surjective homomorphism.

(1) $H^{(i)} \leq G^{(i)}$ for all $i \geq 0$. In particular, if G is solvable, then so is H , i.e., subgroups of solvable groups are solvable (and the solvable length of H is less than or equal to the solvable length of G).

(2) $\varphi(G^{(i)}) = K^{(i)}$. In particular, homomorphic images and quotient groups of solvable groups are solvable (of solvable length less than or equal to that of the domain group).

(3) If N is normal in G and both N and G/N are solvable then so is G .

Proof: Part 1 follows from the observation that since $H \leq G$, by definition of commutator subgroups, $[H, H] \leq [G, G]$, i.e., $H^{(1)} \leq G^{(1)}$. Then, by induction,

$$H^{(i)} \leq G^{(i)} \quad \text{for all } i \in \mathbb{Z}^+.$$

In particular, if $G^{(n)} = 1$ for some n , then also $H^{(n)} = 1$. This establishes (1).

To prove (2) note that by definition of commutators,

$$\varphi([x, y]) = [\varphi(x), \varphi(y)]$$

so by induction $\varphi(G^{(i)}) \leq K^{(i)}$. Since φ is surjective, every commutator in K is the image of a commutator in G , hence again by induction we obtain equality for all i . Again, if $G^{(n)} = 1$ for some n then $K^{(n)} = 1$. This proves (2).

Finally, if G/N and N are solvable, of lengths n and m respectively then by (2) applied to the natural projection $\varphi : G \rightarrow G/N$ we obtain

$$\varphi(G^{(n)}) = (G/N)^{(n)} = 1N$$

i.e., $G^{(n)} \leq N$. Thus $G^{(n+m)} = (G^{(n)})^{(m)} \leq N^{(m)} = 1$. Theorem 9 shows that G is solvable, which completes the proof.

Some additional conditions under which finite groups are solvable are the following:

Theorem 11. Let G be a finite group.

- (1) (Burnside) If $|G| = p^a q^b$ for some primes p and q , then G is solvable.
- (2) (Philip Hall) If for every prime p dividing $|G|$ we factor the order of G as $|G| = p^a m$ where $(p, m) = 1$, and G has a subgroup of order m , then G is solvable (i.e., if for all primes p , G has a subgroup whose index equals the order of a Sylow p -subgroup, then G is solvable — such subgroups are called Sylow p -complements).
- (3) (Feit–Thompson) If $|G|$ is odd then G is solvable.
- (4) (Thompson) If for every pair of elements $x, y \in G$, $\langle x, y \rangle$ is a solvable group, then G is solvable.

We shall prove Burnside's Theorem in Chapter 19 and deduce Philip Hall's generalization of it. As mentioned in Section 3.5, the proof of the Feit–Thompson Theorem takes 255 pages. Thompson's Theorem was first proved as a consequence of a 475 page paper (that in turn relies ultimately on the Feit–Thompson Theorem).

A Proof of the Fundamental Theorem of Finite Abelian Groups

We sketch a group-theoretic proof of the result that every finite abelian group is a direct product of cyclic groups (i.e., Parts 1 and 2 of Theorem 5, Section 5.2) — the Classification of Finitely Generated Abelian Groups (Theorem 3, Section 5.2) will be derived as a consequence of a more general theorem in Chapter 12.

By Corollary 4 it suffices to prove that for p a prime, any abelian p -group is a direct product of cyclic groups (the divisibility condition in Theorem 5.5 is trivially achieved by reordering factors). Let A be an abelian p -group. We proceed by induction on $|A|$.

If E is an elementary abelian p -group (i.e., $x^p = 1$ for all $x \in E$), we first prove the following result:

for any $x \in E$, there exists $M \leq E$ with $E = M \times \langle x \rangle$.

If $x = 1$, let $M = E$. Otherwise let M be a subgroup of E of maximal order subject to the condition that x not be an element of M . If M is not of index p in E , let $\bar{E} = E/M$. Then \bar{E} is elementary abelian and there exists $\bar{y} \in \bar{E} - \{\bar{x}\}$. Since \bar{y} has order p , we also have $\bar{x} \notin \langle \bar{y} \rangle$. The complete preimage of $\langle \bar{y} \rangle$ in E is a subgroup of E that does not contain x and whose order is larger than the order of M , contrary to the choice of M . This proves $|E : M| = p$, hence

$$E = M\langle x \rangle \quad \text{and} \quad M \cap \langle x \rangle = 1.$$

By the recognition theorem for direct products, Theorem 5.9, $E = M \times \langle x \rangle$, as asserted.

Now let $\varphi : A \rightarrow A$ be defined by $\varphi(x) = x^p$ (see Exercise 7, Section 5.2). Then φ is a homomorphism since A is abelian. Denote the kernel of φ by K and denote the image of φ by H . By definition $K = \{x \in A \mid x^p = 1\}$ and H is the subgroup of A consisting of p^{th} powers. Note that both K and A/H are elementary abelian. By the First Isomorphism Theorem

$$|A : H| = |K|.$$

By induction,

$$\begin{aligned} H &= \langle h_1 \rangle \times \cdots \times \langle h_r \rangle \\ &\cong Z_{p^{\alpha_1}} \times \cdots \times Z_{p^{\alpha_r}} \quad \alpha_i \geq 1, \quad i = 1, 2, \dots, r. \end{aligned}$$

By definition of φ , there exist elements $g_i \in A$ such that $g_i^p = h_i$, $1 \leq i \leq r$. Let $A_0 = \langle g_1, \dots, g_r \rangle$. It is an exercise to see that

- (a) $A_0 = \langle g_1 \rangle \times \cdots \times \langle g_r \rangle$,
- (b) $A_0/H = \langle g_1 H \rangle \times \cdots \times \langle g_r H \rangle$ is elementary abelian of order p^r , and
- (c) $H \cap K = \langle h_1^{p^{\alpha_1-1}} \rangle \times \cdots \times \langle h_r^{p^{\alpha_r-1}} \rangle$ is elementary abelian of order p^r .

If K is contained in H , then $|K| = |K \cap H| = p^r = |A_0 : H|$. In this case by comparing orders we see that $A_0 = A$ and the theorem is proved. Assume therefore that K is not a subgroup of H and use the bar notation to denote passage to the quotient group A/H . Let $x \in K - H$, so $|\bar{x}| = |x| = p$. By the initial remark of the proof applied to the elementary abelian p -group $E = \bar{A}$, there is a subgroup \bar{M} of \bar{A} such that

$$\bar{A} = \bar{M} \times \langle \bar{x} \rangle.$$

If M is the complete preimage in A of \bar{M} , then since x has order p and $x \notin M$, we have $\langle x \rangle \cap M = 1$. By the recognition theorem for direct products,

$$A = M \times \langle x \rangle.$$

By induction, M is a direct product of cyclic groups, hence so is A . This completes the proof.

The uniqueness of the decomposition of a finite abelian group into a direct product of cyclic groups (Part 3 of Theorem 5.5) can also be proved by induction using the p^{th} -power map (i.e., using Exercise 7, Section 5.2). This is essentially the procedure we follow in Section 12.1 for the uniqueness part of the proof of the Fundamental Theorem of Finitely Generated Abelian Groups.

EXERCISES

1. Prove that $Z_i(G)$ is a characteristic subgroup of G for all i .
2. Prove Parts 2 and 4 of Theorem 1 for G a finite nilpotent group, not necessarily a p -group.
3. If G is finite prove that G is nilpotent if and only if it has a normal subgroup of each order dividing $|G|$, and is cyclic if and only if it has a unique subgroup of each order dividing $|G|$.
4. Prove that a maximal subgroup of a finite nilpotent group has prime index.
5. Prove Parts 2 and 4 of Theorem 1 for G an infinite nilpotent group.
6. Show that if $G/Z(G)$ is nilpotent then G is nilpotent.
7. Prove that subgroups and quotient groups of nilpotent groups are nilpotent (your proof should work for infinite groups). Give an explicit example of a group G which possesses a normal subgroup H such that both H and G/H are nilpotent but G is not nilpotent.
8. Prove that if p is a prime and P is a non-abelian group of order p^3 then $|Z(P)| = p$ and $P/Z(P) \cong Z_p \times Z_p$.
9. Prove that a finite group G is nilpotent if and only if whenever $a, b \in G$ with $(|a|, |b|) = 1$ then $ab = ba$. [Use Part 4 of Theorem 3.]
10. Prove that D_{2^n} is nilpotent if and only if n is a power of 2. [Use Exercise 9.]
11. Give another proof of Proposition 5 under the additional assumption that G is abelian by invoking the Fundamental Theorem of Finite Abelian Groups.
12. Find the upper and lower central series for A_4 and S_4 .
13. Find the upper and lower central series for A_n and S_n , $n \geq 5$.
14. Prove that G^i is a characteristic subgroup of G for all i .
15. Prove that $Z_i(D_{2^n}) = D_{2^n}^{n-1-i}$.
16. Prove that \mathbb{Q} has no maximal subgroups. [Recall Exercise 21, Section 3.2.]
17. Prove that $G^{(i)}$ is a characteristic subgroup of G for all i .
18. Show that if G'/G'' and G''/G''' are both cyclic then $G'' = 1$. [You may assume $G''' = 1$. Then G/G'' acts by conjugation on the cyclic group G'' .]
19. Show that there is no group whose commutator subgroup is isomorphic to S_4 . [Use the preceding exercise.]
20. Let p be a prime, let P be a p -subgroup of the finite group G , let N be a normal subgroup of G whose order is relatively prime to p and let $\overline{G} = G/N$. Prove the following:
 - (a) $N_{\overline{G}}(\overline{P}) = \overline{N_G(P)}$ [Use Frattini's Argument.]
 - (b) $C_{\overline{G}}(\overline{P}) = \overline{C_G(P)}$. [Use part (a).]

For any group G the *Frattini subgroup* of G (denoted by $\Phi(\dot{G})$) is defined to be the intersection of all the maximal subgroups of G (if G has no maximal subgroups, set $\Phi(G) = G$). The next

few exercises deal with this important subgroup.

21. Prove that $\Phi(G)$ is a characteristic subgroup of G .
22. Prove that if $N \trianglelefteq G$ then $\Phi(N) \leq \Phi(G)$. Give an explicit example where this containment does not hold if N is not normal in G .
23. Compute $\Phi(S_3)$, $\Phi(A_4)$, $\Phi(S_4)$, $\Phi(A_5)$ and $\Phi(S_5)$.
24. Say an element x of G is a *nongenerator* if for every proper subgroup H of G , $\langle x, H \rangle$ is also a proper subgroup of G . Prove that $\Phi(G)$ is the set of nongenerators of G (here $|G| > 1$).
25. Let G be a finite group. Prove that $\Phi(G)$ is nilpotent. [Use Frattini's Argument to prove that every Sylow subgroup of $\Phi(G)$ is normal in G .]
26. Let p be a prime, let P be a finite p -group and let $\bar{P} = P/\Phi(P)$.
 - (a) Prove that \bar{P} is an elementary abelian p -group. [Show that $P' \leq \Phi(P)$ and that $x^p \in \Phi(P)$ for all $x \in P$.]
 - (b) Prove that if N is any normal subgroup of P such that P/N is elementary abelian then $\Phi(P) \leq N$. State this (universal) property in terms of homomorphisms and commutative diagrams.
 - (c) Let \bar{P} be elementary abelian of order p^r (by (a)). Deduce from Exercise 24 that if $\bar{x}_1, \bar{x}_2, \dots, \bar{x}_r$ are any basis for the r -dimensional vector space \bar{P} over \mathbb{F}_p , and if x_i is any element of the coset \bar{x}_i , then $P = \langle x_1, x_2, \dots, x_r \rangle$. Show conversely that if y_1, y_2, \dots, y_s is any set of generators for P , then $s \geq r$ (you may assume that every minimal generating set for an r -dimensional vector space has r elements, i.e., every basis has r elements). Deduce *Burnside's Basis Theorem*: a set y_1, \dots, y_s is a minimal generating set for P if and only if $\bar{y}_1, \dots, \bar{y}_s$ is a basis of $\bar{P} = P/\Phi(P)$. Deduce that any minimal generating set for P has r elements.
 - (d) Prove that if $P/\Phi(P)$ is cyclic then P is cyclic. Deduce that if P/P' is cyclic then so is P .
 - (e) Let σ be any automorphism of P of prime order q with $q \neq p$. Show that if σ fixes the coset $x\Phi(P)$ then σ fixes some element of this coset (note that since $\Phi(P)$ is characteristic in P every automorphism of P induces an automorphism of $P/\Phi(P)$). [Use the observation that σ acts a permutation of order 1 or q on the p^a elements in the coset $x\Phi(P)$.]
 - (f) Use parts (e) and (c) to deduce that every nontrivial automorphism of P of order prime to p induces a nontrivial automorphism on $P/\Phi(P)$. Deduce that any group of automorphisms of P which has order prime to p is isomorphic to a subgroup of $\text{Aut}(\bar{P}) = GL_r(\mathbb{F}_p)$.
27. Generalize part (d) of the preceding exercise as follows: let p be a prime, let P be a p -group and let $\bar{P} = P/\Phi(P)$ be elementary abelian of order p^r . Prove that P has exactly $\frac{p^r - 1}{p - 1}$ maximal subgroups. [Since every maximal subgroup of P contains $\Phi(P)$, the maximal subgroups of P are, by the Lattice Isomorphism Theorem, in bijective correspondence with the maximal subgroups of the elementary abelian group \bar{P} . It therefore suffices to show that the number of maximal subgroups of an elementary abelian p -group of order p^r is as stated above. One way of doing this is to use the result that an abelian group is isomorphic to its dual group (cf. Exercise 14 in Section 5.2) so the number of subgroups of *index* p equals the number of subgroups of *order* p .]
28. Prove that if p is a prime and $P = Z_p \times Z_{p^2}$ then $|\Phi(P)| = p$ and $P/\Phi(P) \cong Z_p \times Z_p$. Deduce that P has $p + 1$ maximal subgroups.

29. Prove that if p is a prime and P is a non-abelian group of order p^3 then $\Phi(P) = Z(P)$ and $P/\Phi(P) \cong Z_p \times Z_p$. Deduce that P has $p + 1$ maximal subgroups.
30. Let p be an odd prime, let $P_1 = Z_p \times Z_{p^2}$ and let P_2 be the non-abelian group of order p^3 which has an element of order p^2 . Prove that P_1 and P_2 have the same lattice of subgroups.
31. For any group G a *minimal normal subgroup* is a normal subgroup M of G such that the only normal subgroups of G which are contained in M are 1 and M . Prove that every minimal normal subgroup of a finite solvable group is an elementary abelian p -group for some prime p . [If M is a minimal normal subgroup of G , consider its characteristic subgroups: M' and $\langle x^p \mid x \in M \rangle$.]
32. Prove that every maximal subgroup of a finite solvable group has prime power index. [Let H be a maximal subgroup of G and let M be a minimal normal subgroup of G — cf. the preceding exercise. Apply induction to G/M and consider separately the two cases: $M \leq H$ and $M \not\leq H$.]
33. Let π be any set of primes. A subgroup H of a finite group is called a *Hall π -subgroup* of G if the only primes dividing $|H|$ are in the set π and $|H|$ is relatively prime to $|G : H|$. (Note that if $\pi = \{p\}$, Hall π -subgroups are the same as Sylow p -subgroups. Hall subgroups were introduced in Exercise 10 of Section 3.3). Prove the following generalization of Sylow's Theorem for solvable groups: if G is a finite solvable group then for every set π of primes, G has a Hall π -subgroup and any two Hall π -subgroups (for the same set π) are conjugate in G . [Fix π and proceed by induction on $|G|$, proving both existence and conjugacy at once. Let M be a minimal normal subgroup of G , so M is a p -group for some prime p . If $p \in \pi$, apply induction to G/M . If $p \notin \pi$, reduce to the case $|G| = p^\alpha n$, where $p^\alpha = |M|$ and n is the order of a Hall π -subgroup of G . In this case let N/M be a minimal normal subgroup of G/M , so N/M is a q -group for some prime $q \neq p$. Let $Q \in Syl_q(N)$. If $Q \trianglelefteq G$ argue as before with Q in place of M . If Q is not normal in G , use Frattini's Argument to show $N_G(Q)$ is a Hall π -subgroup of G and establish conjugacy in this case too.]

The following result shows how to produce normal p -subgroups of some groups on which the elements of order prime to p act faithfully by conjugation. Exercise 26(f) then applies to restrict these actions and give some information about the structure of the group.

34. Let p be a prime dividing the order of the finite solvable group G . Assume G has no nontrivial normal subgroups of order prime to p . Let P be the largest normal p -subgroup of G (cf. Exercise 37, Section 4.5). Note that Exercise 31 above shows that $P \neq 1$. Prove that $C_G(P) \leq P$, i.e., $C_G(P) = Z(P)$. [Let $N = C_G(P)$ and use the preceding exercise to show $N = Z(P) \times H$ for some Hall π -subgroup H of N — here π is the set of all prime divisors of $|N|$ except for p . Show $H \trianglelefteq G$ to obtain the desired conclusion: $H = 1$.]
35. Prove that if G is a finite group in which every proper subgroup is nilpotent, then G is solvable. [Show that a minimal counterexample is simple. Let M and N be distinct maximal subgroups chosen with $|M \cap N|$ as large as possible and apply Part 2 of Theorem 3 to show that $M \cap N = 1$. Now apply the methods of Exercise 53 in Section 4.5.]
36. Let p be a prime, let V be a nonzero finite dimensional vector space over the field of p elements and let φ be an element of $GL(V)$ of order a power of p (i.e., V is a nontrivial elementary abelian p -group and φ is an automorphism of V of p -power order). Prove that there is some nonzero element $v \in V$ such that $\varphi(v) = v$, i.e., φ has a nonzero fixed point on V .
37. Let V be a finite dimensional vector space over the field of 2 elements and let φ be an element of $GL(V)$ of order 2. (i.e., V is a nontrivial elementary abelian 2-group and φ is an

automorphism of V of order 2). Prove that the map $v \mapsto v + \varphi(v)$ is a homomorphism from V to itself. Show that every element in the image of this map is fixed by φ . Deduce that the subspace of elements of V which are fixed by φ has dimension $\geq \frac{1}{2}$ (dimension V). (Note that if G is the semidirect product of V with $\langle \varphi \rangle$, where $V \trianglelefteq G$ and φ acts by conjugation on V by sending each $v \in V$ to $\varphi(v)$, then the fixed points of φ on V are $C_V(\varphi)$ and the above map is simply the commutator map: $v \mapsto [v, \varphi]$. In this terminology the problem is to show that $|C_V(\varphi)|^2 \geq |V|$.)

38. Use the preceding exercise to prove that if P is a 2-group which has a cyclic center and M is a subgroup of index 2 in P , then the center of M has rank ≤ 2 . [The group G/M of order 2 acts by conjugation on the \mathbb{F}_2 vector space: $\{z \in Z(M) \mid z^2 = 1\}$ and the fixed points of this action are in the center of P .]

6.2 APPLICATIONS IN GROUPS OF MEDIUM ORDER

The purpose of this section is to work through a number of examples which illustrate many of the techniques we have developed. These examples use Sylow's Theorems extensively and demonstrate how they are applied in the study of finite groups. Motivated by the Hölder Program we address primarily the problem of showing that for certain n every group of order n has a proper, nontrivial normal subgroup (i.e., there are no simple groups of order n). In most cases we shall stop once this has been accomplished. However readers should be aware that in the process of achieving this result we shall already have determined a great deal of information about arbitrary groups of given order n for the n that we consider. This information could be built upon to classify groups of these orders (but in general this requires techniques beyond the simple use of semidirect products to construct groups).

Since for p a prime we have already proved that there are no simple p -groups (other than the cyclic group of order p , Z_p) and since the structure of p -groups can be very complicated (recall the table in Section 5.3), we shall not study the structure of p -groups explicitly. Rather, the theory of p -groups developed in the preceding section will be applied to subgroups of groups of non-prime-power order.

Finally, for certain n (e.g., 60, 168, 360, 504,...) there do exist simple groups of order n so, of course, we cannot force every group of these orders to be nonsimple. As in Section 4.5 we can, in certain cases, prove there is a unique simple group of order n and unravel some of its internal structure (Sylow numbers, etc.). We shall study simple groups of order 168 as an additional test case. Thus the Sylow Theorems will be applied in a number of different contexts to show how groups of a given order may be manipulated.

We shall end this section with some comments on the existence problem for groups, particularly for finite simple groups.

For $n < 10000$ there are 60 odd, non-prime-power numbers for which the congruence conditions of Sylow's Theorems do *not* force at least one of the Sylow subgroups to be normal i.e., n_p can be > 1 for all primes $p \mid n$ (recall that n_p denotes the number of Sylow p -subgroups). For example, no numbers of the form pq , where p and q are distinct primes occur in our list by results of Section 4.5. In contrast, for even numbers < 500 there are already 46 candidates for orders of simple groups (the congruence

conditions allow many more possibilities). Many of our numerical examples arise from these lists of numbers and we often use odd numbers because the Sylow congruence conditions allow fewer values for n_p . The purpose of these examples is to illustrate the use of the results we have proved. Many of these examples can be dealt with by more advanced techniques (for example, the Feit–Thompson Theorem proves that there are *no* simple groups of odd composite order).

As we saw in the case $n = 30$ in Section 4.5, even though Sylow’s Theorem permitted $n_5 = 6$ and $n_3 = 10$, further examination showed that any group of order 30 must have both $n_5 = 1$ and $n_3 = 1$. Thus the congruence part of Sylow’s Theorem is a sufficient but by no means necessary condition for normality of a Sylow subgroup. For many n (e.g., $n = 120$) we can prove that there are no simple groups of order n , so there is a nontrivial normal subgroup but this subgroup may not be a Sylow subgroup. For example, S_5 and $SL_2(\mathbb{F}_5)$ both have order 120. The group S_5 has a unique nontrivial proper normal subgroup of order 60 (A_5) and $SL_2(\mathbb{F}_5)$ has a unique nontrivial proper normal subgroup of order 2 ($Z(SL_2(\mathbb{F}_5)) \cong Z_2$), neither of which is a Sylow subgroup. Our techniques for producing normal subgroups must be flexible enough to cover such diverse possibilities. In this section we shall examine Sylow subgroups for different primes dividing n , intersections of Sylow subgroups, normalizers of p -subgroups and many other less obvious subgroups. The elementary methods we outline are by no means exhaustive, even for groups of “medium” order.

Some Techniques

Before listing some techniques for producing normal subgroups in groups of a given (“medium”) order we note that in all the problems where one deals with groups of order n , for some specific n , it is first necessary to factor n into prime powers and then to compute the permissible values of n_p , for all primes p dividing n . We emphasize the need to be comfortable computing mod p when carrying out the last step. The techniques we describe may be listed as follows:

- (1) Counting elements.
- (2) Exploiting subgroups of small index.
- (3) Permutation representations.
- (4) Playing p -subgroups off against each other for different primes p .
- (5) Studying normalizers of intersections of Sylow p -subgroups.

Counting Elements

Let G be a group of order n , let p be a prime dividing n and let $P \in Syl_p(G)$. If $|P| = p$, then every nonidentity element of P has order p and every element of G of order p lies in some conjugate of P . By Lagrange’s Theorem distinct conjugates of P intersect in the identity, hence in this case the number of elements of G of order p is $n_p(p - 1)$.

If Sylow p -subgroups for different primes p have prime order and we assume none of these is normal, we can sometimes show that the number of elements of prime order is $> |G|$. This contradiction would show that at least one of the n_p ’s must be 1 (i.e., some Sylow subgroup is normal in G).

This is the argument we used (in Section 4.5) to prove that there are no simple

groups of order 30. For another example, suppose $|G| = 105 = 3 \cdot 5 \cdot 7$. If G were simple, we must have $n_3 = 7$, $n_5 = 21$ and $n_7 = 15$. Thus

$$\begin{array}{rcl} \text{the number of elements of order 3 is } 7 \cdot 2 & = & 14 \\ \text{the number of elements of order 5 is } 21 \cdot 4 & = & 84 \\ \text{the number of elements of order 7 is } 15 \cdot 6 & = & 90 \\ \hline \text{the number of elements of prime order is } 188 & > & |G|. \end{array}$$

Sometimes counting elements of prime order does not lead to too many elements. However, there may be so few elements remaining that there must be a normal subgroup involving these elements. This was (in essence) the technique used in Section 4.5 to show that in a group of order 12 either $n_2 = 1$ or $n_3 = 1$. This technique works particularly well when G has a Sylow p -subgroup P of order p such that $N_G(P) = P$. For example, let $|G| = 56$. If G were simple, the only possibility for the number of Sylow 7-subgroups is 8, so

$$\text{the number of elements of order 7 is } 8 \cdot 6 = 48.$$

Thus there are $56 - 48 = 8$ elements remaining in G . Since a Sylow 2-subgroup contains 8 elements (none of which have order 7), there can be at most one Sylow 2-subgroup, hence G has a normal Sylow 2-subgroup.

Exploiting Subgroups of Small Index

Recall that the results of Section 4.2 show that if G has a subgroup H of index k , then there is a homomorphism from G into the symmetric group S_k whose kernel is contained in H . If $k > 1$, this kernel is a proper normal subgroup of G and if we are trying to prove that G is not simple, we may, by way of contradiction, assume that this kernel is the identity. Then, by the First Isomorphism Theorem, G is isomorphic to a subgroup of S_k . In particular, the order of G divides $k!$. This argument shows that if k is the smallest integer with $|G|$ dividing $k!$ for a finite simple group G then G contains no proper subgroups of index less than k . This smallest permissible index k should be calculated at the outset of the study of groups of a given order n . In the examples we consider this is usually quite easy: n will often factor as

$$p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s} \quad \text{with} \quad p_1 < p_2 < \cdots < p_s$$

and α_s is usually equal to 1 or 2 in our examples. In this case the minimal index of a proper subgroup will have to be at least p_s (respectively $2p_s$) and this is often its exact value.

For example, there is no simple group of order 3393, because if $n = 3393 = 3^2 \cdot 13 \cdot 29$, then the minimal index of a proper subgroup is 29 (n does not divide 28! because 29 does not divide 28!). However any simple group of order 3393 must have $n_3 = 13$, so for $P \in \text{Syl}_3(G)$, $N_G(P)$ has index 13, a contradiction.

Permutation Representations

This method is a refinement of the preceding one. As above, if G is a simple group of order n with a proper subgroup of index k , then G is isomorphic to a subgroup of S_k . We may identify G with this subgroup and so assume $G \leq S_k$. Rather than relying only

on Lagrange's Theorem for our contradiction (this was what we did for the preceding technique) we can sometimes show by calculating within S_k that S_k contains no simple subgroup of order n . Two restrictions which may enable one to show such a result are

- (1) if G contains an element or subgroup of a particular order, so must S_k , and
- (2) if $P \in \text{Syl}_p(G)$ and if P is also a Sylow p -subgroup of S_k , then $|N_G(P)|$ must divide $|N_{S_k}(P)|$.

Condition (2) arises frequently when p is a prime, $k = p$ or $p + 1$ and G has a subgroup of index k . In this case p^2 does not divide $k!$, so Sylow p -subgroups of G are also Sylow p -subgroups of S_k . Since now Sylow p -subgroups of S_k are precisely the groups generated by a p -cycle, and distinct Sylow p -subgroups intersect in the identity,

$$\begin{aligned} \text{the no. of Sylow } p\text{-subgroups of } S_k &= \frac{\text{the no. of } p\text{-cycles}}{\text{the no. of } p\text{-cycles in a Sylow } p\text{-subgroup}} \\ &= \frac{k \cdot (k - 1) \cdots (k - p + 1)}{p(p - 1)}. \end{aligned}$$

This number gives the index in S_k of the normalizer of a Sylow p -subgroup of S_k . Thus for $k = p$ or $k = p + 1$

$$|N_{S_k}(P)| = p(p - 1) \quad (k = p \text{ or } k = p + 1)$$

(cf. also the corresponding discussion for centralizers of elements in symmetric groups in Section 4.3 and the last exercises in Section 4.3). This proves, under the above hypotheses, that $|N_G(P)|$ must divide $p(p - 1)$.

For example, if G were a simple group of order $396 = 2^2 \cdot 3^2 \cdot 11$, we must have $n_{11} = 12$, so if $P \in \text{Syl}_{11}(G)$, $|G : N_G(P)| = 12$ and $|N_G(P)| = 33$. Since G has a subgroup of index 12, G is isomorphic to a subgroup of S_{12} . But then (considering G as actually contained in S_{12}) $P \in \text{Syl}_{11}(S_{12})$ and $|N_{S_{12}}(P)| = 110$. Since $N_G(P) \leq N_{S_{12}}(P)$, this would imply $33 \mid 110$, clearly impossible, so we cannot have a simple group of order 396.

We can sometimes squeeze a little bit more out of this method by working in A_k rather than S_k . This slight improvement helps only occasionally and only for groups of even order. It is based on the following observations (the first of which we have made earlier in the text).

Proposition 12.

- (1) If G has no subgroup of index 2 and $G \leq S_k$, then $G \leq A_k$.
- (2) If $P \in \text{Syl}_p(S_k)$ for some odd prime p , then $P \in \text{Syl}_p(A_k)$ and $|N_{A_k}(P)| = \frac{1}{2}|N_{S_k}(P)|$.

Proof: The first assertion follows from the Second Isomorphism Theorem: if G is not contained in A_k , then $A_k < GA_k$ so we must have $GA_k = S_k$. But now

$$2 = |S_k : A_k| = |GA_k : A_k| = |G : G \cap A_k|$$

so G has a subgroup, $G \cap A_k$, of index 2.

To prove (2) note that if $P \in Syl_p(S_k)$, for some odd prime p , by (1) (or order considerations) $P \leq A_k$, hence $P \in Syl_p(A_k)$ as well. By Frattini's Argument (Proposition 6)

$$S_k = N_{S_k}(P)A_k$$

so, in particular, $N_{S_k}(P)$ is not contained in A_k . This forces $N_{S_k}(P) \cap A_k (= N_{A_k}(P))$ to be a subgroup of index 2 in $N_{S_k}(P)$.

For example, there is no simple group of order 264. Suppose G were a simple group of order $264 = 2^3 \cdot 3 \cdot 11$. We must have $n_{11} = 12$. As usual, G would be isomorphic to a subgroup of S_{12} . Since G is simple (hence contains no subgroup of index 2), $G \leq A_{12}$. Let $P \in Syl_{11}(G)$. Since $n_{11} = 12 = |G : N_G(P)|$, we have $|N_G(P)| = 22$. As above,

$$|N_{A_{12}}(P)| = \frac{1}{2}|N_{S_{12}}(P)| = \frac{1}{2}11(11 - 1) = 55;$$

however, 22 does not divide 55, a contradiction to $N_G(P) \leq N_{A_{12}}(P)$.

Finally, we emphasize that we have only barely touched upon the combinatorial information available from certain permutation representations. Whenever possible in the remaining examples we shall illustrate other applications of this technique.

Playing p -Subgroups Off Against Each Other for Different Primes p

Suppose p and q are distinct primes such that every group of order pq is cyclic. This is equivalent to $p \nmid q - 1$, where $p < q$. If G has a Sylow q -subgroup Q of order q and $p \mid |N_G(Q)|$, applying Cauchy's Theorem in $N_G(Q)$ gives a group P of order p normalizing Q (note that P need not be a Sylow p -subgroup of G). Thus PQ is a group and if PQ is abelian, we obtain

$$PQ \leq N_G(P) \quad \text{and so} \quad q \mid |N_G(P)|.$$

(A symmetric argument applies if Sylow p -subgroups of G have order p and q divides the order of a Sylow p -normalizer). This numerical information alone may be sufficient to force $N_G(P) = G$ (i.e., $P \trianglelefteq G$), or at least to force $N_G(P)$ to have index smaller than the minimal index permitted by permutation representations, giving a contradiction by a preceding technique.

For example, there are no simple groups of order 1785. If there were, let G be a simple group of order $1785 = 3 \cdot 5 \cdot 7 \cdot 17$. The only possible value for n_{17} is 35, so if Q is a Sylow 17-subgroup, $|G : N_G(Q)| = 35$. Thus $|N_G(Q)| = 3 \cdot 17$. Let P be a Sylow 3-subgroup of $N_G(Q)$. The group PQ is abelian since 3 does not divide $17 - 1$, so $Q \leq N_G(P)$ and $17 \mid |N_G(P)|$. In this case $P \in Syl_3(G)$. The permissible values of n_3 are 7, 85 and 595; however, since $17 \mid |N_G(P)|$, we cannot have $17 \mid |G : N_G(P)| = n_3$. Thus $n_3 = 7$. But G has no proper subgroup of index < 17 (the minimal index of a proper subgroup is 17 for this order), a contradiction. Alternatively, if $n_3 = 7$, then $|N_G(P)| = 3 \cdot 5 \cdot 17$, and by Sylow's Theorem applied in $N_G(P)$ we have $Q \trianglelefteq N_G(P)$. This contradicts the fact that $|N_G(Q)| = 3 \cdot 17$.

We can refine this method by not requiring P and Q to be of prime order. Namely, if p and q are distinct primes dividing $|G|$ such that $Q \in Syl_q(G)$ and $p \mid |N_G(Q)|$, let $P \in Syl_p(N_G(Q))$. We can then apply Sylow's Theorems in $N_G(Q)$ to see whether

$P \leq N_G(Q)$, and if so, force $N_G(P)$ to be of small index. If P is a Sylow p -subgroup of the whole group G , we can use the congruence part of Sylow's Theorem to put further restrictions on $|N_G(P)|$ (as we did in the preceding example). If P is not a Sylow p -subgroup of G , then by the second part of Sylow's Theorem $P \leq P^* \in \text{Syl}_p(G)$. In this case since $P < P^*$, Theorem 1(4) shows that $P < N_{P^*}(P)$. Thus $N_G(P)$ (which contains $N_{P^*}(P)$) has order divisible by a larger power of p than divides $|P|$ (as well as being divisible by $|Q|$).

For example, there are no simple groups of order 3675. If there were, let G be a simple group of order $3675 = 3 \cdot 5^2 \cdot 7^2$. The only possibility for n_7 is 15, so for $Q \in \text{Syl}_7(G)$, $|G : N_G(Q)| = 15$ and $|N_G(Q)| = 245 = 5 \cdot 7^2$. Let $N = N_G(Q)$ and let $P \in \text{Syl}_5(N)$. By the congruence conditions of Sylow's Theorem applied in N we get $P \trianglelefteq N$. Since $|P| = 5$, P is not itself a Sylow 5-subgroup of G so P is contained in some Sylow 5-subgroup P^* of G . Since P is of index 5 in the 5-group P^* , $P \trianglelefteq P^*$ by Theorem 1, that is $P^* \leq N_G(P)$. This proves

$$\langle N, P^* \rangle \leq N_G(P) \quad \text{so} \quad 7^2 \cdot 5^2 \mid |N_G(P)|.$$

Thus $|G : N_G(P)| \mid 3$, which is impossible since P is not normal and G has no subgroup of index 3.

Studying Normalizers of Intersections of Sylow p -Subgroups

One of the reasons the counting arguments in the first method above do not immediately generalize to Sylow subgroups which are not of prime order is because if $P \in \text{Syl}_p(G)$ for some prime p and $|P| = p^a$, $a \geq 2$, then it need not be the case that distinct conjugates of P intersect in the identity subgroup. If distinct conjugates of P do intersect in the identity, we can again count to find that the number of elements of p -power order is $n_p(|P| - 1)$.

Suppose, however, there exists $R \in \text{Syl}_p(G)$ with $R \neq P$ and $P \cap R \neq 1$. Let $P_0 = P \cap R$. Then $P_0 < P$ and $P_0 < R$, hence by Theorem 1

$$P_0 < N_P(P_0) \quad \text{and} \quad P_0 < N_R(P_0).$$

One can try to use this to prove that the normalizer in G of P_0 is sufficiently large (i.e., of sufficiently small index) to obtain a contradiction by previous methods (note that this normalizer is a proper subgroup since $P_0 \neq 1$).

One special case where this works particularly well is when $|P_0| = p^{a-1}$ i.e., the two Sylow p -subgroups R and P have large intersection. In this case set $N = N_G(P_0)$. Then by the above reasoning (i.e., since P_0 is a maximal subgroup of the p -groups P and R), $P_0 \trianglelefteq P$ and $P_0 \trianglelefteq R$, that is,

N has 2 distinct Sylow p -subgroups: P and R .

In particular, $|N| = p^a k$, where (by Sylow's Theorem) $k \geq p + 1$.

Recapitulating, if Sylow p -subgroups pairwise intersect in the identity, then counting elements of p -power order is possible; otherwise there is some intersection of Sylow p -subgroups whose normalizer is “large.” Since for an arbitrary group order one cannot necessarily tell which of these two phenomena occurs, it may be necessary to split the nonsimplicity argument into two (mutually exclusive) cases and derive a contradiction

in each. This process is especially amenable when the order of a Sylow p -subgroup is p^2 (for example, this line of reasoning was used to count elements of 2-power order in the proof that a simple group of order 60 is isomorphic to A_5 — Proposition 23, Section 4.5).

Before proceeding with an example we state a lemma which gives a sufficient condition to force a nontrivial Sylow intersection.

Lemma 13. In a finite group G if $n_p \not\equiv 1 \pmod{p^2}$, then there are distinct Sylow p -subgroups P and R of G such that $P \cap R$ is of index p in both P and R (hence is normal in each).

Proof: The argument is an easy refinement of the proof of the congruence part of Sylow's Theorem (cf. the exercises at the end of Section 4.5). Let P act by conjugation on the set $Syl_p(G)$. Let $\mathcal{O}_1, \dots, \mathcal{O}_s$ be the orbits under this action with $\mathcal{O}_1 = \{P\}$. If p^2 divides $|P : P \cap R|$ for all Sylow p -subgroups R of G different from P , then each \mathcal{O}_i has size divisible by p^2 , $i = 2, 3, \dots, s$. In this case, since n_p is the sum of the lengths of the orbits we would have $n_p = 1 + kp^2$, contrary to assumption. Thus for some $R \in Syl_p(G)$, $|P : P \cap R| = p$.

For example, there are no simple groups of order 1053. If there were, let G be a simple group of order $1053 = 3^4 \cdot 13$ and let $P \in Syl_3(G)$. We must have $n_3 = 13$. But $13 \not\equiv 1 \pmod{3^2}$ so there exist $P, R \in Syl_3(G)$ such that $|P \cap R| = 3^3$. Let $N = N_G(P \cap R)$, so by the above arguments $P, R \leq N$. Thus $3^4 \mid |N|$ and $|N| > 3^4$. The only possibility is $N = G$, i.e., $P \cap R \trianglelefteq G$, a contradiction.

Simple Groups of Order 168

We now show how many of our techniques can be used to unravel the structure of and then classify certain simple groups by classifying the simple groups of order 168. Because there are no nontrivial normal subgroups in simple groups, this process departs from the methods in Section 5.5, but the overall approach typifies methods used in the study of finite simple groups.

We begin by assuming there is a simple group G of order $168 = 2^3 \cdot 3 \cdot 7$. We first work out many of its properties: the number and structure of its Sylow subgroups, the conjugacy classes, etc. All of these calculations are based only on the order and simplicity of G . We use these results to first prove the uniqueness of G ; and ultimately we prove the existence of the simple group of order 168.

Because $|G|$ does not divide 6! we have

- (1) *G has no proper subgroup of index less than 7,*

since otherwise the action of G on the cosets of the subgroup would give a (necessarily injective since G is simple) homomorphism from G into some S_n with $n \leq 6$.

The simplicity of G and Sylow's Theorem also immediately imply that

- (2) *$n_7 = 8$, so the normalizer of a Sylow 7-subgroup has order 21. In particular, no element of order 2 normalizes a Sylow 7-subgroup and G has no elements of order 14.*

If G had an element of order 21 then the normalizer of a Sylow 3-subgroup of G would have order divisible by 7. Thus n_3 would be relatively prime to 7. Since then $n_3 \mid 8$ we would have $n_3 = 4$ contrary to (1). This proves:

(3) *G has no elements of order 21.*

By Sylow's Theorem $n_3 = 7$ or 28; we next rule out the former possibility. Assume $n_3 = 7$, let $P \in \text{Syl}_3(G)$ and let T be a Sylow 2-subgroup of the group $N_G(P)$ of order 24. Each Sylow 3-subgroup normalizes some Sylow 7-subgroup of G so P normalizes a Sylow 7-subgroup R of G . For every $t \in T$ we also have that $P = tPt^{-1}$ normalizes tRt^{-1} . The subgroup T acts by conjugation on the set of eight Sylow 7-subgroups of G and since no element of order 2 in G normalizes a Sylow 7-subgroup by (2), it follows that T acts transitively, i.e., every Sylow 7-subgroup of G is one of the tRt^{-1} . Hence P normalizes every Sylow 7-subgroup of G , i.e., P is contained in the intersection of the normalizers of all Sylow 7-subgroups. But this intersection is a proper normal subgroup of G , so it must be trivial. This contradiction proves:

(4) *$n_3 = 28$ and the normalizer of a Sylow 3-subgroup has order 6.*

Since $n_2 = 7$ or 21, we have $n_2 \not\equiv 1 \pmod{8}$, so by Exercise 21 there is a pair of distinct Sylow 2-subgroups that have nontrivial intersection; over all such pairs let T_1 and T_2 be chosen with $U = T_1 \cap T_2$ of maximal order. We next prove

(5) *U is a Klein 4-group and $N_G(U) \cong S_4$.*

Let $N = N_G(U)$. Since $|U| = 2$ or 4 and N permutes the nonidentity elements of U by conjugation, a subgroup of order 7 in N would commute with some element of order 2 in U , contradicting (2). It follows that the order of N is not divisible by 7. By Exercise 13, N has more than one Sylow 2-subgroup, hence $|N| = 2^a \cdot 3$, where $a = 2$ or 3. Let $P \in \text{Syl}_3(N)$. Since P is a Sylow 3-subgroup of G , by (4) the group $N_N(P)$ has order 3 or 6 (with P as its unique subgroup of order 3). Thus by Sylow's Theorem N must have four Sylow 3-subgroups, and these are permuted transitively by N under conjugation. Since any group of order 12 must have either a normal Sylow 2-subgroup or a normal Sylow 3-subgroup (cf. Section 4.5), $|N| = 24$. Let K be the kernel of N acting by conjugation on its four Sylow 3-subgroups, so K is the intersection of the normalizers of the Sylow 3-subgroups of N . If $K = 1$ then $N \cong S_4$ as asserted; so consider when $K \neq 1$. Since $K \leq N_N(P)$, the group K has order dividing 6, and since P does not normalize another Sylow 3-subgroup, P is not contained in K . It follows that $|K| = 2$. But now N/K is a group of order 12 which is seen to have more than one Sylow 2-subgroup and four Sylow 3-subgroups, contrary to the property of groups of order 12 cited earlier. This proves $N \cong S_4$. Since S_4 has a unique nontrivial normal 2-subgroup, V_4 , (5) holds. Since $N \cong S_4$, it follows that N contains a Sylow 2-subgroup of G and also that $N_N(P) \cong S_3$ (so also $N_G(P) \cong S_3$ by (4)). Hence we obtain

(6) *Sylow 2-subgroups of G are isomorphic to D_8 , and*

(7) *the normalizer in G of a Sylow 3-subgroup is isomorphic to S_3 and so G has no elements of order 6.*

By (2) and (7), no element of order 2 commutes with an element of odd prime order. If $T \in Syl_2(G)$, then $T \cong D_8$ by (6), so $Z(T) = \langle z \rangle$ where z is an element of order 2. Then $T \leq C_G(z)$ and $|C_G(z)|$ has no odd prime factors by what was just said, so $C_G(z) = T$. Since any element normalizing T would normalize its center, hence commute with z , it follows that Sylow 2-subgroups of G are self-normalizing. This gives

$$(8) \quad n_2 = 21 \text{ and } C_G(z) = T, \text{ where } T \in Syl_2(G) \text{ and } Z(T) = \langle z \rangle.$$

Since $|C_G(z)| = 8$, the element z in (8) has 21 conjugates. By (6), G has one conjugacy class of elements of order 4, which by (6) and (8) contains 42 elements. By (2) there are 48 elements of order 7, and by (4) there are 56 elements of order 3. These account for all 167 nonidentity elements of G , and so every element of order 2 must be conjugate to z , i.e.,

$$(9) \quad G \text{ has a unique conjugacy class of elements of order 2.}$$

Continuing with the same notation, let $T \in Syl_2(G)$ with $U \leq T$ and let W be the other Klein 4-group in T . It follows from Sylow's Theorem that U and W are not conjugate in G since they are not conjugate in $N_G(T) = T$ (cf. Exercise 50 in Section 4.5). We argue next that

$$(10) \quad N_G(W) \cong S_4.$$

To see this let $W = \langle z, w \rangle$ where, as before, $\langle z \rangle = Z(T)$. Since w is conjugate in G to z , $C_G(w) = T_0$ is another Sylow 2-subgroup of G containing W but different from T . Thus $W = T \cap T_0$. Since U was an arbitrary maximal intersection of Sylow 2-subgroups of G , the argument giving (5) implies (10).

We now record results which we have proved or which are easy consequences of (1) to (10).

Proposition 14. If G is a simple group of order 168, then the following hold:

- (1) $n_2 = 21, n_3 = 7$ and $n_7 = 8$
- (2) Sylow 2-subgroups of G are dihedral, Sylow 3- and 7-subgroups are cyclic
- (3) G is isomorphic to a subgroup of A_7 and G has no subgroup of index ≤ 6
- (4) the conjugacy classes of G are the following: the identity; two classes of elements of order 7 each of which contains 24 elements (represented by any element of order 7 and its inverse); one class of elements of order 3 containing 56 elements; one class of elements of order 4 containing 42 elements; one class of elements of order 2 containing 21 elements
(in particular, every element of G has order a power of a prime)
- (5) if $T \in Syl_2(G)$ and U, W are the two Klein 4-groups in T , then U and W are not conjugate in G and $N_G(U) \cong N_G(W) \cong S_4$
- (6) G has precisely three conjugacy classes of maximal subgroups, two of which are isomorphic to S_4 and one of which is isomorphic to the non-abelian group of order 21.

All of the calculations above were predicated on the assumption that there exists a simple group of order 168. The fact that none of these arguments leads to a contradiction

does not prove the existence of such a group, but rather just gives strong evidence that there *may* be a simple group of this order. We next illustrate how the internal subgroup structure of G gives rise to a geometry on which G acts, and so leads to a proof that a simple group of order 168 is unique, if it exists (which we shall also show).

Continuing the above notation let U_1, \dots, U_7 be the conjugates of U and let W_1, \dots, W_7 be the conjugates of W . Call the U_i *points* and the W_j *lines*. Define an “incidence relation” by specifying that

the point U_i is on the line W_j if and only if U_i normalizes W_j .

Note that U_i normalizes W_j if and only if $U_i W_j \cong D_8$, which in turn occurs if and only if W_j normalizes U_i . In each point or line stabilizer—which is isomorphic to S_4 —there is a unique normal 4-group, V , and precisely three other (nonnormal) 4-groups A_1, A_2, A_3 . The groups $V A_i$ are the three Sylow 2-subgroups of the S_4 . We therefore have:

(11) *each line contains exactly 3 points and each point lies on exactly 3 lines.*

Since any two nonnormal 4-groups in an S_4 generate the S_4 , hence uniquely determine the other two Klein groups in that S_4 , we obtain

(12) *any 2 points on a line uniquely determine the line (and the third point on it).*

Since there are 7 points and 7 lines, elementary counting now shows that

(13) *each pair of points lies on a unique line, and each pair of lines intersects in a unique point.*

(This configuration of points and lines thus satisfies axioms for what is termed a *projective plane*.) It is now straightforward to show that the incidence geometry is uniquely determined and may be represented by the graph in Figure 1, where points are vertices and lines are the six sides and medians of the triangle together with the inscribed circle—see Exercise 27. This incidence geometry is called the *projective plane of order 2* or the *Fano Plane*, and will be denoted by \mathcal{F} . (Generally, a projective plane of “order” N has $N^2 + N + 1$ points, and the same number of lines.) Note that at this point the projective plane \mathcal{F} *does* exist—we have explicitly exhibited points and lines satisfying (11) to (13)—even though the group G is not yet known to exist.

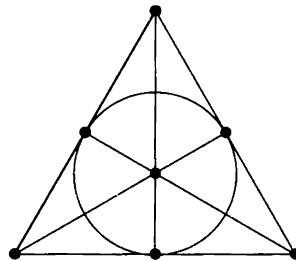


Figure 1

An *automorphism* of this plane is any permutation of points and lines that preserves the incidence relation. For example, any of the six symmetries of the triangle in Figure 1

give automorphisms of \mathcal{F} , but we shall see that \mathcal{F} has many more automorphisms than these.

Each $g \in G$ acts by conjugation on the set of points and lines, and this action preserves the incidence relation. Only the identity element in G fixes all points and so via this action the group G would be isomorphic to a subgroup of the group of $\text{Aut}(\mathcal{F})$, the group of all automorphisms of \mathcal{F} .

Any automorphism of \mathcal{F} that fixes two points on a line as well as a third point not on that line is easily seen to fix all points. Thus any automorphism of \mathcal{F} is uniquely determined by its action on any three noncollinear points. Since one easily computes that there are 168 such triples, \mathcal{F} has at most 168 automorphisms. This proves

if the simple group G exists it is unique and $G \cong \text{Aut}(\mathcal{F})$.

Two steps in the classification process yet remain: to prove that \mathcal{F} does have 168 automorphisms and to prove $\text{Aut}(\mathcal{F})$ is indeed a simple group. Although one can do these graph-theoretically, we adopt an approach following ideas from the theory of “algebraic groups.” Let V be a 3-dimensional vector space over the field of 2 elements, \mathbb{F}_2 , so V is the elementary abelian 2-group $Z_2 \times Z_2 \times Z_2$ of order 8. By Proposition 17 in Section 4.4, $\text{Aut}(V) = GL(V) \cong GL_3(\mathbb{F}_2)$ has order 168. Call the seven 1-dimensional subspaces (i.e., the nontrivial cyclic subgroups) of V *points*, call the seven 2-dimensional subspaces (i.e., the subgroups of order 4) *lines*, and say the point p is *incident to* the line L if $p \subset L$. Then the points and lines are easily seen to satisfy the same axioms (11) to (13) above, hence to represent the Fano Plane. Since $GL(V)$ acts faithfully on these points and lines preserving incidence, $\text{Aut}(\mathcal{F})$ has order at least 168. In light of the established upper bound for $|\text{Aut}(\mathcal{F})|$ this proves

$\text{Aut}(\mathcal{F}) \cong GL(V) \cong GL_3(\mathbb{F}_2)$ and $\text{Aut}(\mathcal{F})$ has order 168.

Finally we prove that $GL(V)$ is a simple group. By way of contradiction assume H is a proper nontrivial normal subgroup of $GL(V)$. Let Ω be the 7 points and let N be the stabilizer in $GL(V)$ of some point in Ω . Since $GL(V)$ acts transitively on Ω , N has index 7. Since the intersection of all conjugates of N fixes all points, this intersection is the identity. Thus $H \not\leq N$, and so $GL(V) = HN$. Since $|H : H \cap N| = |HN : N|$ we have $7 \mid |H|$. Since $GL(V)$ is isomorphic to a subgroup of S_7 and since Sylow 7-subgroups of S_7 have normalizers of order 42, $GL(V)$ does not have a normal Sylow 7-subgroup, so by Sylow’s Theorem $n_7(GL(V)) = 8$. A normal Sylow 7-subgroup of H would be characteristic in H , hence normal in $GL(V)$, so also H does not have a unique Sylow 7-subgroup. Since $n_7(H) \equiv 1 \pmod{7}$ and $n_7(H) \leq n_7(GL(V)) = 8$ we must have $n_7(H) = 8$. This implies $|H|$ is divisible by 8, so $56 \mid |H|$, and since H is proper we must have $|H| = 56$. By usual counting arguments (cf. Exercise 7(b) of Section 5.5) H has a normal, hence characteristic, Sylow 2-subgroup, which is therefore normal in $GL(V)$. But then $GL(V)$ would have a unique Sylow 2-subgroup. Since the set of upper triangular matrices and the set of lower triangular matrices are two subgroups of $GL_3(\mathbb{F}_2)$ each of order 8, we have a contradiction. In summary we have now proven the following theorem.

Theorem 15. Up to isomorphism there is a unique simple group of order 168, $GL_3(\mathbb{F}_2)$, which is also the automorphism group of the projective plane \mathcal{F} .

Note that we might just as well have called the W_j points and the U_i lines. This “duality” between points and lines together with the uniqueness of a simple group of order 168 may be used to prove the existence of an outer automorphism of G that interchanges points and lines i.e., conjugates U to W .

Many families of finite simple groups can be classified by analogous methods. In more general settings geometric structures known as *buildings* play the role of the projective plane (which is a special case of a building of type A_2). In this context the subgroups $N_G(U)$ and $N_G(W)$ are *parabolic subgroups* of G , and U, W are their *unipotent radicals* respectively. In particular, all the simple linear groups (cf. Section 3.4) are characterized by the structure and intersections of their parabolic subgroups, or equivalently, by their action on an associated building.

Remarks on the Existence Problem for Groups

As in other areas of mathematics (such as the theory of differential equations) one may hypothesize the existence of a mathematical system (e.g., solution to an equation) and derive a great deal of information about this proposed system. In general, if after considerable effort no contradiction is reached based on the initial hypothesis one begins to suspect that there actually is a system which does satisfy the conditions hypothesized. However, no amount of consistent data will *prove* existence. Suppose we carried out an analysis of a hypothetical simple group G of order $3^3 \cdot 7 \cdot 13 \cdot 409$ analogous to our analysis of a simple group of order 168 (which we showed to exist). After a certain amount of effort we could show that there are unique possible Sylow numbers:

$$n_3 = 7 \cdot 409 \quad n_7 = 3^2 \cdot 13 \cdot 409 \quad n_{13} = 3^2 \cdot 7 \cdot 409 \quad n_{409} = 3^2 \cdot 7 \cdot 13.$$

We could further show that such a G would have no elements of order pq , p and q distinct primes, no elements of order 9, and that distinct Sylow subgroups would intersect in the identity. We could then count the elements in Sylow p -subgroups for all primes p and we would find that these would total to exactly $|G|$. At this point we would have the complete subgroup structure and class equation for G . We might then guess that there *is* a simple group of this order, but the Feit–Thompson Theorem asserts that there are *no* simple groups of odd composite order. (Note, however, that the configuration for a possible simple group of order $3^3 \cdot 7 \cdot 13 \cdot 409$ is among the cases that must be dealt with in the *proof* of the Feit–Thompson Theorem, so quoting this result in this instance is actually circular. We prove no simple group of this order exists in Section 19.3; see also Exercise 29.) The point is that even though we have as much data in this case as we had in the order 168 situation (i.e., Proposition 14), we cannot prove existence without some new techniques.

When we are dealing with nonsimple groups we have at least one method of building larger groups from smaller ones: semidirect products. Even though this method is fairly restrictive it conveys the notion that nonsimple groups may be built up from smaller groups in some constructive fashion. This process breaks down completely for simple groups; and so this demarcation of techniques reinforces our appreciation for the Hölder

Program: determining the simple groups, and finding how these groups are put together to form larger groups.

The study of simple groups, as illustrated in the preceding discussion of groups of order 168, uses many of the same tools as the study of nonsimple groups (to unravel their subgroup structures, etc.) but also requires other techniques for their construction. As we mentioned at the end of that discussion, these often involve algebraic or geometric methods which construct simple groups as automorphisms of mathematical structures that have intrinsic interest, and thereby link group theory to other areas of mathematics and science in fascinating ways. Thus while we have come a long way in the analysis of finite groups, there are a number of different areas in this branch of mathematics on which we have just touched.

The analysis of infinite groups generally involves quite different methods, and in the next section we introduce some of these.

EXERCISES

Counting elements:

1. Prove that for fixed $P \in Syl_p(G)$ if $P \cap R = 1$ for all $R \in Syl_p(G) - \{P\}$, then $P_1 \cap P_2 = 1$ whenever P_1 and P_2 are distinct Sylow p -subgroups of G . Deduce in this case that the number of nonidentity elements of p -power order in G is $(|P| - 1)|G : N_G(P)|$.
2. In the group $S_3 \times S_3$ exhibit a pair of Sylow 2-subgroups that intersect in the identity and exhibit another pair that intersect in a group of order 2.
3. Prove that if $|G| = 380$ then G is not simple. [Just count elements of odd prime order.]
4. Prove that there are no simple groups of order 80, 351, 3875 or 5313.
5. Let G be a solvable group of order pm , where p is a prime not dividing m , and let $P \in Syl_p(G)$. If $N_G(P) = P$, prove that G has a normal subgroup of order m . Where was the solvability of G needed in the proof? (This result is true for nonsolvable groups as well — it is a special case of *Burnside's N/C-Theorem*.)

Exploiting subgroups of small index:

6. Prove that there are no simple groups of order 2205, 4125, 5103, 6545 or 6435.

Permutation representations:

7. Prove that there are no simple groups of order 1755 or 5265. [Use Sylow 3-subgroups to show $G \leq S_{13}$ and look at the normalizer of a Sylow 13-subgroup.]
8. Prove that there are no simple groups of order 792 or 918.
9. Prove that there are no simple groups of order 336.

Playing p -subgroups off against each other:

10. Prove that there are no simple groups of order 4095, 4389, 5313 or 6669.
11. Prove that there are no simple groups of order 4851 or 5145.
12. Prove that there are no simple groups of order 9555. [Let $Q \in Syl_{13}(G)$ and let $P \in Syl_7(N_G(Q))$. Argue that $Q \trianglelefteq N_G(P)$ — why is this a contradiction?]

Normalizers of Sylow intersections:

13. Let G be a group with more than one Sylow p -subgroup. Over all pairs of distinct Sylow p -subgroups let P and Q be chosen so that $|P \cap Q|$ is maximal. Show that $N_G(P \cap Q)$

has more than one Sylow p -subgroup and that any two distinct Sylow p -subgroups of $N_G(P \cap Q)$ intersect in the subgroup $P \cap Q$. (Thus $|N_G(P \cap Q)|$ is divisible by $p \cdot |P \cap Q|$ and by some prime other than p . Note that Sylow p -subgroups of $N_G(P \cap Q)$ need not be Sylow in G .)

- 14.** Prove that there are no simple groups of order 144, 525, 2025 or 3159.

General exercises:

- 15.** Classify groups of order 105.
- 16.** Prove that there are no non-abelian simple groups of odd order < 10000 .
- 17.** (a) Prove that there is no simple group of order 420.
 (b) Prove that there are no simple groups of even order < 500 except for orders 2, 60, 168 and 360.
- 18.** Prove that if G is a group of order 36 then G has either a normal Sylow 2-subgroup or a normal Sylow 3-subgroup.
- 19.** Show that a group of order 12 with no subgroup of order 6 is isomorphic to A_4 .
- 20.** Show that a group of order 24 with no element of order 6 is isomorphic to S_4 .
- 21.** Generalize Lemma 13 by proving that if $n_p \not\equiv 1 \pmod{p^k}$ then there are distinct Sylow p -subgroups P and R of G such that $P \cap R$ is of index $\leq p^{k-1}$ in both P and R .
- 22.** Suppose over all pairs of distinct Sylow p -subgroups of G , P and R are chosen with $|P \cap R|$ maximal. Prove that $N_G(P \cap R)$ is not a p -group.
- 23.** Let A and B be normal subsets of a Sylow p -subgroup P of G . Prove that if A and B are conjugate in G then they are conjugate in $N_G(P)$.
- 24.** Let G be a group of order pqr where p, q and r are primes with $p < q < r$. Prove that a Sylow r -subgroup of G is normal.
- 25.** Let G be a simple group of order p^2qr where p, q and r are primes. Prove that $|G| = 60$.
- 26.** Prove or construct a counterexample to the assertion: if G is a group of order 168 with more than one Sylow 7-subgroup then G is simple.
- 27.** Show that if \mathcal{F} is any set of points and lines satisfying properties (11) to (13) in the subsection on simple groups of order 168 then the graph of incidences for \mathcal{F} is uniquely determined and is the same as Figure 1 (up to relabeling points and lines). [Take a line and any point not on this line. Depict the line as the base of an equilateral triangle and the point as the vertex of this triangle not on the base. Use the axioms to show that the incidences of the remaining points and lines are then uniquely determined as in Figure 1.]
- 28.** Let G be a simple group of order $3^3 \cdot 7 \cdot 13 \cdot 409$. Compute all permissible values of n_p for each $p \in \{3, 7, 13, 409\}$ and reduce to the case where there is a unique possible value for each n_p .
- 29.** Given the information on the Sylow numbers for a hypothetical simple group of order $3^3 \cdot 7 \cdot 13 \cdot 409$, prove that there is no such group. [Work with the permutation representation of degree 819.]
- 30.** Suppose G is a simple group of order 720. Find as many properties of G as you can (Sylow numbers, isomorphism type of Sylow subgroups, conjugacy classes, etc.). Is there such a group?

6.3 A WORD ON FREE GROUPS

In this section we introduce the basic theory of so-called free groups. This will enable us to make precise the notions of generators and relations which were used in earlier chapters. The results of this section rely only on the basic theory of homomorphisms.

The basic idea of a free group $F(S)$ generated by a set S is that there are no relations satisfied by any of the elements in S (S is “free” of relations). For example, if S is the set $\{a, b\}$ then the elements of the free group on the two generators a and b are of the form $a, aa, ab, abab, bab, \dots$, called *words* in a and b , together with the inverses of these elements, and all these elements are considered distinct. If we group like terms together, then we obtain elements of the familiar form $a, b^{-3}, aba^{-1}b^2$ etc. Such elements are multiplied by concatenating their words (for example, the product of aba and $b^{-1}a^3b$ would simply be $abab^{-1}a^3b$). It is natural at the outset (even before we know S is contained in some group) to simply *define* $F(S)$ to be the set of all words in S , where two such expressions are multiplied in $F(S)$ by concatenating them. Although in essence this is what we do, it is necessary to be more formal in order to prove that this concatenation operation is well defined and associative. After all, even the familiar notation a^n for the product $a \cdot a \cdots a$ (n terms) is permissible only because we know that this product is independent of the way it is bracketed (cf. the generalized associative law in Section 1.1). The formal construction of $F(S)$ is carried out below for an arbitrary set S .

One important property reflecting the fact that there are no relations that must be satisfied by the generators in S is that any *map* from the *set* S to a group G can be uniquely extended to a *homomorphism* from the *group* $F(S)$ to G (basically since we have specified where the generators must go and the images of all the other elements are uniquely determined by the homomorphism property — the fact that there are no relations to worry about means that we can specify the images of the generators *arbitrarily*). This is frequently referred to as the *universal* property of the free group and in fact characterizes the group $F(S)$.

The notion of “freeness” occurs in many algebraic systems and it may already be familiar (using a different terminology) from elementary vector space theory. When the algebraic systems are vector spaces, $F(S)$ is simply the vector space which has S as a basis. Every vector in this space is a unique linear combination of the elements of S (the analogue of a “word”). Any set map from the basis S to another vector space V extends uniquely to a linear transformation (i.e., vector space homomorphism) from $F(S)$ to V .

Before beginning the construction of $F(S)$ we mention that one often sees the universal property described in the language of commutative diagrams. In this form it reads (for groups) as follows: given any set map φ from the set S to a group G there is a unique homomorphism $\Phi : F(S) \rightarrow G$ such that $\Phi|_S = \varphi$ i.e., such that the following diagram commutes:

$$\begin{array}{ccc} S & \xrightarrow{\text{inclusion}} & F(S) \\ & \searrow \varphi & \downarrow \Phi \\ & & G \end{array}$$

As mentioned above, the only difficulty with the construction of $F(S)$ is the verification that the concatenation operation on the words in $F(S)$ is well defined and associative. To prove the associative property for multiplication of words we return to the most basic level where all the exponents in the words of S are ± 1 .

We first introduce inverses for elements of S and an identity.

Let S^{-1} be any set disjoint from S such that there is a bijection from S to S^{-1} . For each $s \in S$ denote its corresponding element in S^{-1} by s^{-1} and similarly for each $t \in S^{-1}$ let the corresponding element of S be denoted by t^{-1} (so $(s^{-1})^{-1} = s$). Take a singleton set not contained in $S \cup S^{-1}$ and call it $\{1\}$. Let $1^{-1} = 1$ and for any $x \in S \cup S^{-1} \cup \{1\}$ let $x^1 = x$.

Next we describe the elements of the free group on the set S . A *word* on S is by definition a sequence

$$(s_1, s_2, s_3, \dots) \quad \text{where } s_i \in S \cup S^{-1} \cup \{1\} \text{ and } s_i = 1 \text{ for all } i \text{ sufficiently large}$$

(that is, for each sequence there is an N such that $s_i = 1$ for all $i \geq N$). Thus we can think of a word as a finite product of elements of S and their inverses (where repetitions are allowed). Next, in order to assure uniqueness of expressions we consider only words which have no obvious “cancellations” between adjacent terms (such as $baa^{-1}b = bb$). The word (s_1, s_2, s_3, \dots) is said to be *reduced* if

- (1) $s_{i+1} \neq s_i^{-1}$ for all i with $s_i \neq 1$, and
- (2) if $s_k = 1$ for some k , then $s_i = 1$ for all $i \geq k$.

The reduced word $(1, 1, 1, \dots)$ is called the *empty word* and is denoted by 1 . We now simplify the notation by writing the reduced word $(s_1^{\epsilon_1}, s_2^{\epsilon_2}, \dots, s_n^{\epsilon_n}, 1, 1, 1, \dots)$, $s_i \in S$, $\epsilon_i = \pm 1$, as $s_1^{\epsilon_1} s_2^{\epsilon_2} \dots s_n^{\epsilon_n}$. Note that by definition, reduced words $r_1^{\delta_1} r_2^{\delta_2} \dots r_m^{\delta_m}$ and $s_1^{\epsilon_1} s_2^{\epsilon_2} \dots s_n^{\epsilon_n}$ are equal if and only if $n = m$ and $\delta_i = \epsilon_i$, $1 \leq i \leq n$. Let $F(S)$ be the set of reduced words on S and embed S into $F(S)$ by

$$s \mapsto (s, 1, 1, 1, \dots).$$

Under this set injection we identify S with its image and henceforth consider S as a subset of $F(S)$. Note that if $S = \emptyset$, $F(S) = \{1\}$.

We are now in a position to introduce the binary operation on $F(S)$. The principal technical difficulty is to ensure that the product of two reduced words is again a *reduced* word. Although the definition appears to be complicated it is simply the formal rule for “successive cancellation” of juxtaposed terms which are inverses of each other (e.g., $ab^{-1}a$ times $a^{-1}ba$ should reduce to aa). Let $r_1^{\delta_1} r_2^{\delta_2} \dots r_m^{\delta_m}$ and $s_1^{\epsilon_1} s_2^{\epsilon_2} \dots s_n^{\epsilon_n}$ be reduced words and assume first that $m \leq n$. Let k be the smallest integer in the range $1 \leq k \leq m + 1$ such that $s_k^{\epsilon_k} \neq r_{m-k+1}^{-\delta_{m-k+1}}$. Then the product of these reduced words is defined to be:

$$(r_1^{\delta_1} r_2^{\delta_2} \dots r_m^{\delta_m})(s_1^{\epsilon_1} s_2^{\epsilon_2} \dots s_n^{\epsilon_n}) = \begin{cases} r_1^{\delta_1} \dots r_{m-k+1}^{\delta_{m-k+1}} s_k^{\epsilon_k} \dots s_n^{\epsilon_n}, & \text{if } k \leq m \\ s_{m+1}^{\epsilon_{m+1}} \dots s_n^{\epsilon_n}, & \text{if } k = m+1 \leq n \\ 1, & \text{if } k = m+1 \text{ and } m = n. \end{cases}$$

The product is defined similarly when $m \geq n$, so in either case it results in a reduced word.

Theorem 16. $F(S)$ is a group under the binary operation defined above.

Proof: One easily checks that 1 is an identity and that the inverse of the reduced word $s_1^{\epsilon_1} s_2^{\epsilon_2} \dots s_n^{\epsilon_n}$ is the reduced word $s_n^{-\epsilon_n} s_{n-1}^{-\epsilon_{n-1}} \dots s_1^{-\epsilon_1}$. The difficult part of the proof is the verification of the associative law. This can be done by induction on the “length” of the words involved and considering various cases or one can proceed as follows: For each $s \in S \cup S^{-1} \cup \{1\}$ define $\sigma_s : F(S) \rightarrow F(S)$ by

$$\sigma_s(s_1^{\epsilon_1} s_2^{\epsilon_2} \dots s_n^{\epsilon_n}) = \begin{cases} s \cdot s_1^{\epsilon_1} s_2^{\epsilon_2} \dots s_n^{\epsilon_n}, & \text{if } s_1^{\epsilon_1} \neq s^{-1} \\ s_2^{\epsilon_2} s_3^{\epsilon_3} \dots s_n^{\epsilon_n}, & \text{if } s_1^{\epsilon_1} = s^{-1}. \end{cases}$$

Since $\sigma_{s^{-1}} \circ \sigma_s$ is the identity map of $F(S) \rightarrow F(S)$, σ_s is a permutation of $F(S)$. Let $A(F)$ be the subgroup of the symmetric group on the set $F(S)$ which is generated by $\{\sigma_s \mid s \in S\}$. It is easy to see that the map

$$s_1^{\epsilon_1} s_2^{\epsilon_2} \dots s_n^{\epsilon_n} \mapsto \sigma_{s_1}^{\epsilon_1} \circ \sigma_{s_2}^{\epsilon_2} \circ \dots \circ \sigma_{s_n}^{\epsilon_n}$$

is a (set) bijection between $F(S)$ and $A(S)$ which respects their binary operations. Since $A(S)$ is a group, hence associative, so is $F(S)$.

The universal property of free groups now follows easily.

Theorem 17. Let G be a group, S a set and $\varphi : S \rightarrow G$ a set map. Then there is a unique group homomorphism $\Phi : F(S) \rightarrow G$ such that the following diagram commutes:

$$\begin{array}{ccc} S & \xrightarrow{\text{inclusion}} & F(S) \\ & \searrow \varphi & \downarrow \Phi \\ & & G \end{array}$$

Proof: Such a map Φ must satisfy $\Phi(s_1^{\epsilon_1} s_2^{\epsilon_2} \dots s_n^{\epsilon_n}) = \varphi(s_1)^{\epsilon_1} \varphi(s_2)^{\epsilon_2} \dots \varphi(s_n)^{\epsilon_n}$ if it is to be a homomorphism (which proves uniqueness), and it is straightforward to check that this map is in fact a homomorphism (which proves existence).

Corollary 18. $F(S)$ is unique up to a unique isomorphism which is the identity map on the set S .

Proof: This follows from the universal property. Suppose $F(S)$ and $F'(S)$ are two free groups generated by S . Since S is contained in both $F(S)$ and $F'(S)$, we have natural injections $S \hookrightarrow F'(S)$ and $S \hookrightarrow F(S)$. By the universal property in the theorem, it follows that we have unique associated group homomorphisms $\Phi : F(S) \rightarrow F'(S)$ and $\Phi' : F'(S) \rightarrow F(S)$ which are both the identity on S . The composite $\Phi' \Phi$ is a homomorphism from $F(S)$ to $F(S)$ which is the identity on S , so by the uniqueness statement in the theorem, it must be the identity map. Similarly $\Phi' \Phi'$ is the identity, so Φ is an isomorphism (with inverse Φ'), which proves the corollary.

Definition. The group $F(S)$ is called the *free group* on the set S . A group F is a *free group* if there is some set S such that $F = F(S)$ — in this case we call S a set of *free generators* (or a *free basis*) of F . The cardinality of S is called the *rank* of the free group.

One can now simplify expressions in a free group by using exponential notation, so we write a^3b^{-2} instead of the formal reduced word $aaab^{-1}b^{-1}$. Expressions like aba , however, cannot be simplified in the free group on $\{a, b\}$. We mention one important theorem in this area.

Theorem 19. (Schreier) Subgroups of a free group are free.

This is not trivial to prove and we do not include a proof. There is a nice proof of this result using covering spaces (cf. *Trees* by J.-P. Serre, Springer-Verlag, 1980).

Presentations

Let G be any group. Then G is a homomorphic image of a free group: take $S = G$ and φ as the identity map from G to G ; then Theorem 16 produces a (surjective) homomorphism from $F(G)$ onto G . More generally, if S is any subset of G such that $G = \langle S \rangle$, then again there is a unique surjective homomorphism from $F(S)$ onto G which is the identity on S . (Note that we can now independently formulate the notion that a subset *generates* a group by noting that $G = \langle S \rangle$ if and only if the map $\pi : F(S) \rightarrow G$ which extends the identity map of S to G is surjective.)

Definition. Let S be a subset of a group G such that $G = \langle S \rangle$.

- (1) A *presentation* for G is a pair (S, R) , where R is a set of words in $F(S)$ such that the normal closure of $\langle R \rangle$ in $F(S)$ (the smallest normal subgroup containing $\langle R \rangle$) equals the kernel of the homomorphism $\pi : F(S) \rightarrow G$ (where π extends the identity map from S to G). The elements of S are called *generators* and those of R are called *relations* of G .
- (2) We say G is *finitely generated* if there is a presentation (S, R) such that S is a finite set and we say G is *finitely presented* if there is a presentation (S, R) with both S and R finite sets.

Note that if (S, R) is a presentation, the kernel of the map $F(S) \rightarrow G$ is not $\langle R \rangle$ itself but rather the (much larger) group generated by R and *all conjugates* of elements in R . Note that even for a fixed set S a group will have many different presentations (we can always throw redundant relations into R , for example). If G is finitely presented with $S = \{s_1, s_2, \dots, s_n\}$ and $R = \{w_1, w_2, \dots, w_k\}$, we write (as we have in preceding chapters):

$$G = \langle s_1, s_2, \dots, s_n \mid w_1 = w_2 = \dots = w_k = 1 \rangle$$

and if w is the word $w_1 w_2^{-1}$, we shall write $w_1 = w_2$ instead of $w = 1$.

Examples

- (1) Every finite group is finitely presented. To see this let $G = \{g_1, \dots, g_n\}$ be a finite group. Let $S = G$ and let $\pi : F(S) \rightarrow G$ be the homomorphism extending the identity map of S . Let R_0 be the set of words $g_i g_j g_k^{-1}$, where $i, j, k = 1, \dots, n$ and $g_i g_j = g_k$ in G . Clearly $R_0 \leq \ker \pi$. If N is the normal closure of R_0 in $F(S)$ and $\tilde{G} = F(S)/N$, then G is a homomorphic image of \tilde{G} (i.e., π factors through N). Moreover, the set of elements $\{\tilde{g}_i \mid i = 1, \dots, n\}$ is closed under multiplication. Since this set generates \tilde{G} , it must equal \tilde{G} . Thus $|\tilde{G}| = |G|$ and so $N = \ker \pi$ and (S, R_0) is a presentation of G .

This illustrates a sufficient condition for (S, R) to be a presentation for a given finite group G :

(i) S must be a generating set for G , and

(ii) any group generated by S satisfying the relations in R must have order $\leq |G|$.

- (2) Abelian groups can be presented easily. For instance

$$\begin{aligned}\mathbb{Z} &\cong F(\{a\}) = \langle a \rangle, \\ \mathbb{Z} \times \mathbb{Z} &\cong \langle a, b \mid [a, b] = 1 \rangle, \\ \mathbb{Z}_n \times \mathbb{Z}_m &\cong \langle a, b \mid a^n = b^m = [a, b] = 1 \rangle.\end{aligned}$$

(Recall $[a, b] = a^{-1}b^{-1}ab$).

- (3) Some familiar non-abelian groups introduced in earlier chapters have simple presentations:

$$\begin{aligned}D_{2n} &= \langle r, s \mid r^n = s^2 = 1, s^{-1}rs = r^{-1} \rangle \\ Q_8 &= \langle i, j \mid i^4 = 1, j^2 = i^2, j^{-1}ij = i^{-1} \rangle.\end{aligned}$$

To check, for example, the presentation for D_{2n} note that the relations in the presentation $\langle r, s \mid r^n = s^2 = 1, s^{-1}rs = r^{-1} \rangle$ imply that this group has a normal subgroup (generated by r) of order $\leq n$ whose quotient is generated by s (which has order ≤ 2). Thus any group with these generators and relations has order at most $2n$. Since we already know of the existence of the group D_{2n} of order $2n$ satisfying these conditions, the abstract presentation must equal D_{2n} .

- (4) As mentioned in Section 1.2, in general it is extremely difficult even to determine if a given set of generators and relations is or is not the identity group (let alone determine whether it is some other nontrivial finite group). For example, in the following two presentations the first group is an *infinite* group and the second is the *identity* group (cf. *Trees*, Chapter 1):

$$\begin{aligned}\langle x_1, x_2, x_3, x_4 \mid x_2x_1x_2^{-1} &= x_1^2, x_3x_2x_3^{-1} = x_2^2, x_4x_3x_4^{-1} = x_3^2, x_1x_4x_1^{-1} = x_4^2 \rangle \\ \langle x_1, x_2, x_3, \mid x_2x_1x_2^{-1} &= x_1^2, x_3x_2x_3^{-1} = x_2^2, x_1x_3x_1^{-1} = x_3^2 \rangle.\end{aligned}$$

- (5) It is easy to see that S_n is generated by the transpositions $(1\ 2), (2\ 3), \dots, (n-1\ n)$, and that these satisfy the relations

$$((i\ i+1)(i+1\ i+2))^3 = 1 \quad \text{and} \quad [(i\ i+1), (j\ j+1)] = 1, \quad \text{whenever } |i - j| \geq 2$$

(here $|i - j|$ denotes the absolute value of the integer $i - j$). One can prove by induction on n that these form a presentation of S_n :

$$\begin{aligned}S_n &\cong \langle t_1, \dots, t_{n-1} \mid t_i^2 = 1, (t_i t_{i+1})^3 = 1, \text{ and } [t_i, t_j] = 1 \\ &\quad \text{whenever } |i - j| \geq 2, 1 \leq i, j \leq n-1 \rangle.\end{aligned}$$

As mentioned in Section 1.6 we can use presentations of a group to find homomorphisms between groups or to find automorphisms of a group. We did this in classifying groups of order 6, for example, when we proved that any non-abelian group of order 6 was generated by an element of order 3 and an element of order 2 inverting it; thus there is a homomorphism from S_3 onto any non-abelian group of order 6 (hence an isomorphism, by computing orders). More generally, suppose G is presented by, say, generators a, b with relations r_1, \dots, r_k . If a', b' are any elements of a group H satisfying these relations, there is a homomorphism from G into H . Namely, if $\pi : F(\{a, b\}) \rightarrow G$ is the presentation homomorphism, we can define $\pi' : F(\{a, b\}) \rightarrow H$ by $\pi'(a) = a'$ and $\pi'(b) = b'$. Then $\ker \pi \leq \ker \pi'$ so π' factors through $\ker \pi$ and we obtain

$$G \cong F(\{a, b\})/\ker \pi \longrightarrow H.$$

In, particular, if $\langle a', b' \rangle = H = G$, this homomorphism is an automorphism of G . Conversely, any automorphism must send a set of generators to another set of generators satisfying the same relations. For example, $D_8 = \langle a, b \mid a^2 = b^4 = 1, aba = b^{-1} \rangle$ and any pair a', b' of elements, where a' is a noncentral element of order 2 and b' is of order 4, satisfies the same relations. Since there are four noncentral elements of order 2 and two elements of order 4, D_8 has 8 automorphisms.

Similarly, any pair of elements of order 4 in Q_8 which are not equal or inverses of each other necessarily generate Q_8 and satisfy the relations given in Example 3 above. It is easy to check that there are 24 such pairs, so

$$|\text{Aut}(Q_8)| = 24.$$

Free objects can be constructed in (many, but not all) other categories. For instance, a *monoid* is a set together with a binary operation satisfying all of the group axioms except the axiom specifying the existence of inverses. Free objects in the category of monoids play a fundamental role in theoretical computer science where they model the behavior of machines (Turing machines, etc.). We shall encounter free algebras (i.e., polynomial algebras) and free modules in later chapters.

EXERCISES

- Let F_1 and F_2 be free groups of finite rank. Prove that $F_1 \cong F_2$ if and only if they have the same rank. What facts do you need in order to extend your proof to infinite ranks (where the result is also true)?
- Prove that if $|S| > 1$ then $F(S)$ is non-abelian.
- Prove that the commutator subgroup of the free group on 2 generators is not finitely generated (in particular, subgroups of finitely generated groups need not be finitely generated).
- Prove that every nonidentity element of a free group is of infinite order.
- Establish a finite presentation for A_4 using 2 generators.
- Establish a finite presentation for S_4 using 2 generators.
- Prove that the following is a presentation for the quaternion group of order 8:

$$Q_8 = \langle a, b \mid a^2 = b^2, a^{-1}ba = b^{-1} \rangle.$$

- Use presentations to find the orders of the automorphism groups of the groups $Z_2 \times Z_4$ and $Z_4 \times Z_4$.

9. Prove that $\text{Aut}(Q_8) \cong S_4$.
10. This exercise exhibits an automorphism of S_6 that is not inner (hence, together with Exercise 19 in Section 4.4 it shows that $|\text{Aut}(S_6) : \text{Inn}(S_6)| = 2$). Let $t'_1 = (1\ 2)(3\ 4)(5\ 6)$, $t'_2 = (1\ 4)(2\ 5)(3\ 6)$, $t'_3 = (1\ 3)(2\ 4)(5\ 6)$, $t'_4 = (1\ 2)(3\ 6)(4\ 5)$, and $t'_5 = (1\ 4)(2\ 3)(5\ 6)$. Show that t'_1, \dots, t'_5 satisfy the following relations:

$$(t'_i)^2 = 1 \text{ for all } i,$$

$$(t'_i t'_j)^2 = 1 \text{ for all } i \text{ and } j \text{ with } |i - j| \geq 2, \text{ and}$$

$$(t'_i t'_{i+1})^3 = 1 \text{ for all } i \in \{1, 2, 3, 4\}.$$

Deduce that $S_6 = \langle t'_1, \dots, t'_5 \rangle$ and that the map

$$(1\ 2) \mapsto t'_1, \quad (2\ 3) \mapsto t'_2, \quad (3\ 4) \mapsto t'_3, \quad (4\ 5) \mapsto t'_4, \quad (5\ 6) \mapsto t'_5$$

extends to an automorphism of S_6 (which is clearly not inner since it does not send transpositions to transpositions). [Use the presentation for S_6 described in Example 5.]

11. Let S be a set. The group with presentation (S, R) , where $R = \{[s, t] \mid s, t \in S\}$ is called the *free abelian* group on S — denote it by $A(S)$. Prove that $A(S)$ has the following universal property: if G is any abelian group and $\varphi : S \rightarrow G$ is any set map, then there is a unique group homomorphism $\Phi : A(S) \rightarrow G$ such that $\Phi|_S = \varphi$. Deduce that if A is a free abelian group on a set of cardinality n then

$$A \cong \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z} \quad (n \text{ factors}).$$

12. Let S be a set and let c be a positive integer. Formulate the notion of a *free nilpotent group* on S of nilpotence class c and prove it has the appropriate universal property with respect to nilpotent groups of class $\leq c$.
13. Prove that there cannot be a nilpotent group N generated by two elements with the property that *every* nilpotent group which is generated by two elements is a homomorphic image of N (i.e., the specification of the class c in the preceding problem was necessary).

Part II

RING THEORY

The theory of groups is concerned with general properties of certain objects having an algebraic structure defined by a single binary operation. The study of rings is concerned with objects possessing two binary operations (called addition and multiplication) related by the distributive laws. We first study analogues for the basic points of development in the structure theory of groups. In particular, we introduce subrings, quotient rings, ideals (which are the analogues of normal subgroups) and ring homomorphisms. We then focus on questions about general rings which arise naturally from the presence of two binary operations. Questions concerning multiplicative inverses lead to the notion of fields and eventually to the construction of some specific fields such as finite fields. The study of the arithmetic (divisibility, greatest common divisors, etc.) of rings such as the familiar ring of integers, \mathbb{Z} , leads to the notion of primes and unique factorizations in Chapter 8. The results of Chapters 7 and 8 are then applied to rings of polynomials in Chapter 9.

The basic theory of rings developed in Part II is the cornerstone for the remaining four parts of the book. The theory of ring actions (modules) comprises Part III of the book. There we shall see how the structure of rings is reflected in the structure of the objects on which they act and this will enable us to prove some powerful classification theorems. The structure theory of rings, in particular of polynomial rings, forms the basis in Part IV for the theory of fields and polynomial equations over fields. There the rich interplay among ring theory, field theory and group theory leads to many beautiful results on the structure of fields and the theory of roots of polynomials. Part V continues the study of rings and applications of ring theory to such topics as geometry and the theory of extensions. In Part VI the study of certain specific kinds of rings (group rings) and the objects (modules) on which they act again gives deep classification theorems whose consequences are then exploited to provide new results and insights into finite groups.

CHAPTER 7

Introduction to Rings

7.1 BASIC DEFINITIONS AND EXAMPLES

Definition.

(1) A *ring* R is a set together with two binary operations $+$ and \times (called addition and multiplication) satisfying the following axioms:

- (i) $(R, +)$ is an *abelian* group,
- (ii) \times is associative : $(a \times b) \times c = a \times (b \times c)$ for all $a, b, c \in R$,
- (iii) the *distributive laws* hold in R : for all $a, b, c \in R$

$$(a + b) \times c = (a \times c) + (b \times c) \quad \text{and} \quad a \times (b + c) = (a \times b) + (a \times c).$$

(2) The ring R is *commutative* if multiplication is commutative.

(3) The ring R is said to have an *identity* (or *contain a 1*) if there is an element $1 \in R$ with

$$1 \times a = a \times 1 = a \quad \text{for all } a \in R.$$

We shall usually write simply ab rather than $a \times b$ for $a, b \in R$. The additive identity of R will always be denoted by 0 and the additive inverse of the ring element a will be denoted by $-a$.

The condition that R be a group under addition is a fairly natural one, but it may seem artificial to require that this group be *abelian*. One motivation for this is that if the ring R has a 1 , the commutativity under addition is *forced* by the distributive laws. To see this, compute the product $(1+1)(a+b)$ in two different ways, using the distributive laws (but not assuming that addition is commutative). One obtains

$$(1+1)(a+b) = 1(a+b) + 1(a+b) = 1a + 1b + 1a + 1b = a + b + a + b$$

and

$$(1+1)(a+b) = (1+1)a + (1+1)b = 1a + 1a + 1b + 1b = a + a + b + b.$$

Since R is a group under addition, this implies $b+a = a+b$, i.e., that R under addition is necessarily commutative.

Fields are one of the most important examples of rings. Note that their definition below is just another formulation of the one given in Section 1.4.

Definition. A ring R with identity 1 , where $1 \neq 0$, is called a *division ring* (or *skew field*) if every nonzero element $a \in R$ has a multiplicative inverse, i.e., there exists $b \in R$ such that $ab = ba = 1$. A commutative division ring is called a *field*.

More examples of rings follow.

Examples

- (1) The simplest examples of rings are the *trivial rings* obtained by taking R to be any commutative group (denoting the group operation by $+$) and defining the multiplication \times on R by $a \times b = 0$ for all $a, b \in R$. It is easy to see that this multiplication defines a commutative ring. In particular, if $R = \{0\}$ is the trivial group, the resulting ring R is called the *zero ring*, denoted $R = 0$. Except for the zero ring, a trivial ring does not contain an identity ($R = 0$ is the only ring where $1 = 0$; we shall often exclude this ring by imposing the condition $1 \neq 0$). Although trivial rings have two binary operations, multiplication adds no new structure to the additive group and the theory of rings gives no information which could not already be obtained from (abelian) group theory.
- (2) The ring of integers, \mathbb{Z} , under the usual operations of addition and multiplication is a commutative ring with identity (the integer 1). The ring axioms (as with the additive group axioms) follow from the basic axioms for the system of natural numbers. Note that under *multiplication* $\mathbb{Z} - \{0\}$ is *not* a group (in fact, there are very few multiplicative inverses to elements in this ring). We shall come back to the question of these inverses shortly.
- (3) Similarly, the rational numbers, \mathbb{Q} , the real numbers, \mathbb{R} , and the complex numbers, \mathbb{C} , are commutative rings with identity (in fact they are fields). The ring axioms for each of these follow ultimately from the ring axioms for \mathbb{Z} . We shall verify this when we construct \mathbb{Q} from \mathbb{Z} (Section 7.5) and \mathbb{C} from \mathbb{R} (Example 1, Section 13.1); both of these constructions will be special cases of more general processes. The construction of \mathbb{R} from \mathbb{Q} (and subsequent verification of the ring axioms) is carried out in basic analysis texts.
- (4) The quotient group $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring with identity (the element $\bar{1}$) under the operations of addition and multiplication of residue classes (frequently referred to as “modular arithmetic”). We saw that the additive abelian group axioms followed from the general principles of the theory of quotient groups (indeed this was the prototypical quotient group). We shall shortly prove that the remaining ring axioms (in particular, the fact that multiplication of residue classes is well defined) follow analogously from the general theory of quotient rings.

In all of the examples so far the rings have been commutative. Historically, one of the first noncommutative rings was discovered in 1843 by Sir William Rowan Hamilton (1805–1865). This ring, which is a division ring, was extremely influential in the subsequent development of mathematics and it continues to play an important role in certain areas of mathematics and physics.

(5) (The (*real*) *Hamilton Quaternions*) Let \mathbb{H} be the collection of elements of the form $a + bi + cj + dk$ where $a, b, c, d \in \mathbb{R}$ are real numbers (loosely, “polynomials in $1, i, j, k$ with real coefficients”) where addition is defined “componentwise” by

$$(a+bi+cj+dk) + (a'+b'i+c'j+d'k) = (a+a') + (b+b')i + (c+c')j + (d+d')k$$

and multiplication is defined by expanding $(a + bi + cj + dk)(a' + b'i + c'j + d'k)$ using the distributive law (being careful about the order of terms) and simplifying

using the relations

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j$$

(where the real number coefficients commute with i , j and k). For example,

$$\begin{aligned}(1+i+2j)(j+k) &= 1(j+k) + i(j+k) + 2j(j+k) = j + k + ij + ik + 2j^2 + 2jk \\&= j + k + k + (-j) + 2(-1) + 2(i) = -2 + 2i + 2k.\end{aligned}$$

The fact that \mathbb{H} is a ring may be proved by a straightforward, albeit lengthy, check of the axioms (associativity of multiplication is particularly tedious). The Hamilton Quaternions are a noncommutative ring with identity ($1 = 1+0i+0j+0k$). Similarly, one can define the ring of *rational* Hamilton Quaternions by taking a, b, c, d to be rational numbers above. Both the real and rational Hamilton Quaternions are *division rings*, where inverses of nonzero elements are given by

$$(a + bi + cj + dk)^{-1} = \frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2}.$$

- (6) One important class of rings is obtained by considering rings of functions. Let X be any nonempty set and let A be any ring. The collection, R , of all (set) functions $f : X \rightarrow A$ is a ring under the usual definition of pointwise addition and multiplication of functions: $(f + g)(x) = f(x) + g(x)$ and $(fg)(x) = f(x)g(x)$. Each ring axiom for R follows directly from the corresponding axiom for A . The ring R is commutative if and only if A is commutative and R has a 1 if and only if A has a 1 (in which case the 1 of R is necessarily the constant function 1 on X).

If X and A have more structure, we may form other rings of functions which respect those structures. For instance, if A is the ring of real numbers \mathbb{R} and X is the closed interval $[0, 1]$ in \mathbb{R} we may form the ring of all *continuous* functions from $[0, 1]$ to \mathbb{R} (here we need basic limit theorems to guarantee that sums and products of continuous functions are continuous) — this is a commutative ring with 1.

- (7) An example of a ring which does not have an identity is the ring $2\mathbb{Z}$ of even integers under usual addition and multiplication of integers (the sum and product of even integers is an even integer).

Another example which arises naturally in analysis is constructed as follows. A function $f : \mathbb{R} \rightarrow \mathbb{R}$ is said to have *compact support* if there are real numbers a, b (depending on f) such that $f(x) = 0$ for all $x \notin [a, b]$ (i.e., f is zero outside some bounded interval). The set of all functions $f : \mathbb{R} \rightarrow \mathbb{R}$ with compact support is a commutative ring without identity (since an identity could not have compact support). Similarly, the set of all continuous functions $f : \mathbb{R} \rightarrow \mathbb{R}$ with compact support is a commutative ring without identity.

In the next section we give three important ways of constructing “larger” rings from a given ring (analogous to Example 6 above) and thus greatly expand our list of examples. Before doing so we mention some basic properties of arbitrary rings. The ring \mathbb{Z} is a good example to keep in mind, although this ring has a good deal more algebraic structure than a general ring (for example, it is commutative and has an identity). Nonetheless, its basic arithmetic holds for general rings as the following result shows.

Proposition 1. Let R be a ring. Then

- (1) $0a = a0 = 0$ for all $a \in R$.
- (2) $(-a)b = a(-b) = -(ab)$ for all $a, b \in R$ (recall $-a$ is the additive inverse of a).
- (3) $(-a)(-b) = ab$ for all $a, b \in R$.
- (4) if R has an identity 1, then the identity is unique and $-a = (-1)a$.

Proof: These all follow from the distributive laws and cancellation in the additive group R . For example, (1) follows from $0a = (0 + 0)a = 0a + 0a$. The equality $(-a)b = -(ab)$ in (2) follows from $ab + (-a)b = (a + (-a))b = 0b = 0$. The rest follow similarly and are left to the reader.

This proposition shows that because of the distributive laws the additive and multiplicative structures of a ring behave well with respect to one another, just as in the familiar example of the integers.

Unlike the integers, however, general rings may possess many elements that have multiplicative inverses or may have nonzero elements a and b whose product is zero. These two properties of elements, which relate to the multiplicative structure of a ring, are given special names.

Definition. Let R be a ring.

- (1) A nonzero element a of R is called a *zero divisor* if there is a nonzero element b in R such that either $ab = 0$ or $ba = 0$.
- (2) Assume R has an identity $1 \neq 0$. An element u of R is called a *unit* in R if there is some v in R such that $uv = vu = 1$. The set of units in R is denoted R^\times .

It is easy to see that the units in a ring R form a group under multiplication so R^\times will be referred to as the *group of units* of R . In this terminology a *field is a commutative ring F with identity $1 \neq 0$ in which every nonzero element is a unit*, i.e., $F^\times = F - \{0\}$.

Observe that a *zero divisor can never be a unit*. Suppose for example that a is a unit in R and that $ab = 0$ for some nonzero b in R . Then $va = 1$ for some $v \in R$, so $b = 1b = (va)b = v(ab) = v0 = 0$, a contradiction. Similarly, if $ba = 0$ for some nonzero b then a cannot be a unit.

This shows in particular that fields contain no zero divisors.

Examples

- (1) The ring \mathbb{Z} of integers has no zero divisors and its only units are ± 1 , i.e., $\mathbb{Z}^\times = \{\pm 1\}$. Note that every nonzero integer has an inverse in the *larger ring \mathbb{Q}* , so the property of being a unit depends on the ring in which an element is viewed.
- (2) Let n be an integer ≥ 2 . In the ring $\mathbb{Z}/n\mathbb{Z}$ the elements \bar{u} for which u and n are relatively prime are units (we shall prove this in the next chapter). Thus our use of the notation $(\mathbb{Z}/n\mathbb{Z})^\times$ is consistent with the definition of the group of units in an arbitrary ring.

If, on the other hand, a is a nonzero integer and a is not relatively prime to n then we show that \bar{a} is a zero divisor in $\mathbb{Z}/n\mathbb{Z}$. To see this let d be the g.c.d. of a and n and let $b = \frac{n}{d}$. By assumption $d > 1$ so $0 < b < n$, i.e., $\bar{b} \neq \bar{0}$. But by construction n

divides ab , that is, $\overline{ab} = \bar{0}$ in $\mathbb{Z}/n\mathbb{Z}$. This shows that *every nonzero element of $\mathbb{Z}/n\mathbb{Z}$ is either a unit or a zero divisor*. Furthermore, every nonzero element is a unit if and only if every integer a in the range $0 < a < n$ is relatively prime to n . This happens if and only if n is a prime, i.e., $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is a prime.

- (3) If R is the ring of all functions from the closed interval $[0,1]$ to \mathbb{R} then the units of R are the functions that are not zero at any point (for such f its inverse is the function $\frac{1}{f}$). If f is not a unit and not zero then f is a zero divisor because if we define

$$g(x) = \begin{cases} 0, & \text{if } f(x) \neq 0 \\ 1, & \text{if } f(x) = 0 \end{cases}$$

then g is not the zero function but $f(x)g(x) = 0$ for all x .

- (4) If R is the ring of all *continuous* functions from the closed interval $[0,1]$ to \mathbb{R} then the units of R are still the functions that are not zero at any point, but now there are functions that are neither units nor zero divisors. For instance, $f(x) = x - \frac{1}{2}$ has only one zero (at $x = \frac{1}{2}$) so f is not a unit. On the other hand, if $gf = 0$ then g must be zero for all $x \neq \frac{1}{2}$, and the only *continuous* function with this property is the zero function. Hence f is neither a unit nor a zero divisor. Similarly, no function with only a finite (or countable) number of zeros on $[0,1]$ is a zero divisor. This ring also contains many zero divisors. For instance let

$$f(x) = \begin{cases} 0, & 0 \leq x \leq \frac{1}{2} \\ x - \frac{1}{2}, & \frac{1}{2} \leq x \leq 1 \end{cases}$$

and let $g(x) = f(1-x)$. Then f and g are nonzero continuous functions whose product is the zero function.

- (5) Let D be a rational number that is not a perfect square in \mathbb{Q} and define

$$\mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D} \mid a, b \in \mathbb{Q}\}$$

as a subset of \mathbb{C} . This set is clearly closed under subtraction, and the identity $(a + b\sqrt{D})(c + d\sqrt{D}) = (ac + bdD) + (ad + bc)\sqrt{D}$ shows that it is also closed under multiplication. Hence $\mathbb{Q}(\sqrt{D})$ is a subring of \mathbb{C} (even a subring of \mathbb{R} if $D > 0$), so in particular is a commutative ring with identity. It is easy to show that the assumption that D is not a square implies that every element of $\mathbb{Q}(\sqrt{D})$ may be written uniquely in the form $a + b\sqrt{D}$. This assumption also implies that if a and b are not both 0 then $a^2 - Db^2$ is nonzero, and since $(a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2$ it follows that if $a + b\sqrt{D} \neq 0$ (i.e., one of a or b is nonzero) then $\frac{a - b\sqrt{D}}{a^2 - Db^2}$ is the inverse of $a + b\sqrt{D}$ in $\mathbb{Q}(\sqrt{D})$. This shows that every nonzero element in this commutative ring is a unit, i.e., $\mathbb{Q}(\sqrt{D})$ is a field (called a *quadratic field*, cf. Section 13.2).

The rational number D may be written $D = f^2 D'$ for some rational number f and a unique integer D' where D' is not divisible by the square of any integer greater than 1, i.e., D' is either -1 or ± 1 times the product of distinct primes in \mathbb{Z} (for example, $8/5 = (2/5)^2 \cdot 10$). Call D' the *squarefree part* of D . Then $\sqrt{D} = f\sqrt{D'}$, and so $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{D'})$. Thus *there is no loss in assuming that D is a squarefree integer (i.e., $f = 1$) in the definition of the quadratic field $\mathbb{Q}(\sqrt{D})$* .

Rings having some of the same characteristics as the integers \mathbb{Z} are given a name:

Definition. A commutative ring with identity $1 \neq 0$ is called an *integral domain* if it has no zero divisors.

The absence of zero divisors in integral domains give these rings a cancellation property:

Proposition 2. Assume a, b and c are elements of any ring with a not a zero divisor. If $ab = ac$, then either $a = 0$ or $b = c$ (i.e., if $a \neq 0$ we can cancel the a 's). In particular, if a, b, c are any elements in an integral domain and $ab = ac$, then either $a = 0$ or $b = c$.

Proof: If $ab = ac$ then $a(b - c) = 0$ so either $a = 0$ or $b - c = 0$. The second statement follows from the first and the definition of an integral domain.

Corollary 3. Any finite integral domain is a field.

Proof: Let R be a finite integral domain and let a be a nonzero element of R . By the cancellation law the map $x \mapsto ax$ is an injective function. Since R is finite this map is also surjective. In particular, there is some $b \in R$ such that $ab = 1$, i.e., a is a unit in R . Since a was an arbitrary nonzero element, R is a field.

A remarkable result of Wedderburn is that a finite division ring is necessarily commutative, i.e., is a field. A proof of this theorem is outlined in the exercises at the end of Section 13.6.

In Section 5 we study the relation between zero divisors and units in greater detail. We shall see that every nonzero element of a commutative ring that is not a zero divisor has a multiplicative inverse in some larger ring. This gives another perspective on the cancellation law in Proposition 2.

Having defined the notion of a ring, there is a natural notion of a subring.

Definition. A *subring* of the ring R is a subgroup of R that is closed under multiplication.

In other words, a subset S of a ring R is a subring if the operations of addition and multiplication in R when restricted to S give S the structure of a ring. To show that a subset of a ring R is a subring it suffices to check that it is *nonempty* and *closed under subtraction and under multiplication*.

Examples

A number of the examples above were also subrings.

- (1) \mathbb{Z} is a subring of \mathbb{Q} and \mathbb{Q} is a subring of \mathbb{R} . The property “is a subring of” is clearly transitive.
- (2) $2\mathbb{Z}$ is a subring of \mathbb{Z} , as is $n\mathbb{Z}$ for any integer n . The ring $\mathbb{Z}/n\mathbb{Z}$ is not a subring (or a subgroup) of \mathbb{Z} for any $n \geq 2$.

- (3) The ring of all continuous functions from \mathbb{R} to \mathbb{R} is a subring of the ring of all functions from \mathbb{R} to \mathbb{R} . The ring of all differentiable functions from \mathbb{R} to \mathbb{R} is a subring of both of these.
- (4) $S = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k$, the *integral Quaternions*, form a subring of either the real or the rational Quaternions — it is easy to check that multiplying two such quaternions together gives another quaternion with integer coefficients. This ring (which is not a division ring) can be used to give proofs for a number of results in number theory.
- (5) If R is a subring of a field F that contains the identity of F then R is an integral domain. The converse of this is also true, namely any integral domain is contained in a field (cf. Section 5).

Example: (Quadratic Integer Rings)

Let D be a squarefree integer. It is immediate from the addition and multiplication that the subset $\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\}$ forms a subring of the quadratic field $\mathbb{Q}(\sqrt{D})$ defined earlier. If $D \equiv 1 \pmod{4}$ then the slightly larger subset

$$\mathbb{Z}\left[\frac{1 + \sqrt{D}}{2}\right] = \{a + b\frac{1 + \sqrt{D}}{2} \mid a, b \in \mathbb{Z}\}$$

is also a subring: closure under addition is immediate and $(a + b\frac{1 + \sqrt{D}}{2})(c + d\frac{1 + \sqrt{D}}{2}) = (ac + bd\frac{D-1}{4}) + (ad + bc + bd)\frac{1 + \sqrt{D}}{2}$ together with the congruence on D shows closure under multiplication.

Define

$$\mathcal{O} = \mathcal{O}_{\mathbb{Q}(\sqrt{D})} = \mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\},$$

where

$$\omega = \begin{cases} \sqrt{D}, & \text{if } D \equiv 2, 3 \pmod{4} \\ \frac{1 + \sqrt{D}}{2}, & \text{if } D \equiv 1 \pmod{4}. \end{cases}$$

called the *ring of integers* in the quadratic field $\mathbb{Q}(\sqrt{D})$. The terminology comes from the fact that the elements of the subring \mathcal{O} of the field $\mathbb{Q}(\sqrt{D})$ have many properties analogous to those of the subring of integers \mathbb{Z} in the field of rational numbers \mathbb{Q} (and are the *integral closure* of \mathbb{Z} in $\mathbb{Q}(\sqrt{D})$ as explained in Section 15.3).

In the special case when $D = -1$ we obtain the ring $\mathbb{Z}[i]$ of *Gaussian integers*, which are the complex numbers $a + bi \in \mathbb{C}$ with a and b both *integers*. These numbers were originally introduced by Gauss around 1800 in order to state the biquadratic reciprocity law which deals with the beautiful relations that exist among fourth powers modulo primes. We shall shortly see another useful application of the algebraic structure of this ring to number theoretic questions.

Define the *field norm* $N : \mathbb{Q}(\sqrt{D}) \rightarrow \mathbb{Q}$ by

$$N(a + b\sqrt{D}) = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2 \in \mathbb{Q},$$

which, as previously mentioned, is nonzero if $a + b\sqrt{D} \neq 0$. This norm gives a measure of “size” in the field $\mathbb{Q}(\sqrt{D})$. For instance when $D = -1$ the norm of $a + bi$ is $a^2 + b^2$, which is the square of the length of this complex number considered as a vector in the complex plane. We shall use the field norm in this and subsequent examples to establish many properties of the rings \mathcal{O} .

It is easy to check that N is *multiplicative*, i.e., that $N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in \mathbb{Q}(\sqrt{D})$. On the subring \mathcal{O} it is also easy to see that the field norm is given by

$$N(a + b\omega) = (a + b\omega)(a + b\bar{\omega}) = \begin{cases} a^2 - Db^2, & \text{if } D \equiv 2, 3 \pmod{4} \\ a^2 + ab + \frac{1-D}{4}b^2, & \text{if } D \equiv 1 \pmod{4} \end{cases}$$

where

$$\bar{\omega} = \begin{cases} -\sqrt{D}, & \text{if } D \equiv 2, 3 \pmod{4} \\ \frac{1-\sqrt{D}}{2}, & \text{if } D \equiv 1 \pmod{4}. \end{cases}$$

It follows that $N(\alpha)$ is in fact an *integer* for every $\alpha \in \mathcal{O}$.

We may use this norm to characterize the units in \mathcal{O} . If $\alpha \in \mathcal{O}$ has field norm $N(\alpha) = \pm 1$, the previous formula shows that $(a + b\omega)^{-1} = \pm(a + b\bar{\omega})$, which is again an element of \mathcal{O} and so α is a unit in \mathcal{O} . Suppose conversely that α is a unit in \mathcal{O} , say $\alpha\beta = 1$ for some $\beta \in \mathcal{O}$. Then the multiplicative property of the field norm implies that $N(\alpha)N(\beta) = N(\alpha\beta) = N(1) = 1$. Since both $N(\alpha)$ and $N(\beta)$ are integers, each must be ± 1 . Hence,

the element α is a unit in \mathcal{O} if and only if $N(\alpha) = \pm 1$.

In particular the determination of the integer solutions to the equation $x^2 - Dy^2 = \pm 1$ (called *Pell's equation* in elementary number theory) is essentially equivalent to the determination of the units in the ring \mathcal{O} .

When $D = -1$, the units in the Gaussian integers $\mathbb{Z}[i]$ are the elements $a + bi$ with $a^2 + b^2 = \pm 1$, $a, b \in \mathbb{Z}$, so the group of units consists of $\{\pm 1, \pm i\}$. When $D = -3$, the units in $\mathbb{Z}[(1 + \sqrt{-3})/2]$ are determined by the integers a, b with $a^2 + ab + b^2 = \pm 1$, i.e., with $(2a + b)^2 + 3b^2 = \pm 4$, from which it is easy to see that the group of units is a group of order 6 given by $\{\pm 1, \pm \rho, \pm \rho^2\}$ where $\rho = (-1 + \sqrt{-3})/2$. For any other $D < 0$ it is similarly straightforward to see that the only units are $\{\pm 1\}$.

By contrast, when $D > 0$ it can be shown that the group of units \mathcal{O}^\times is always infinite. For example, it is easy to check that $1 + \sqrt{2}$ is a unit in the ring $\mathcal{O} = \mathbb{Z}[\sqrt{2}]$ (with field norm -1) and that $\{\pm(1 + \sqrt{2})^n \mid n \in \mathbb{Z}\}$, is an infinite set of distinct units (in fact the full group of units in this case, but this is harder to prove).

EXERCISES

Let R be a ring with 1.

1. Show that $(-1)^2 = 1$ in R .
2. Prove that if u is a unit in R then so is $-u$.
3. Let R be a ring with identity and let S be a subring of R containing the identity. Prove that if u is a unit in S then u is a unit in R . Show by example that the converse is false.
4. Prove that the intersection of any nonempty collection of subrings of a ring is also a subring.
5. Decide which of the following (a) – (f) are subrings of \mathbb{Q} .
 - (a) the set of all rational numbers with odd denominators (when written in lowest terms)
 - (b) the set of all rational numbers with even denominators (when written in lowest terms)
 - (c) the set of nonnegative rational numbers
 - (d) the set of squares of rational numbers
 - (e) the set of all rational numbers with odd numerators (when written in lowest terms)

- (f) the set of all rational numbers with even numerators (when written in lowest terms).
6. Decide which of the following are subrings of the ring of all functions from the closed interval $[0,1]$ to \mathbb{R} :
- the set of all functions $f(x)$ such that $f(q) = 0$ for all $q \in \mathbb{Q} \cap [0, 1]$
 - the set of all polynomial functions
 - the set of all functions which have only a finite number of zeros, together with the zero function
 - the set of all functions which have an infinite number of zeros
 - the set of all functions f such that $\lim_{x \rightarrow 1^-} f(x) = 0$
 - the set of all rational linear combinations of the functions $\sin nx$ and $\cos mx$, where $m, n \in \{0, 1, 2, \dots\}$.
7. The *center* of a ring R is $\{z \in R \mid zr = rz \text{ for all } r \in R\}$ (i.e., is the set of all elements which commute with every element of R). Prove that the center of a ring is a subring that contains the identity. Prove that the center of a division ring is a field.
8. Describe the center of the real Hamilton Quaternions \mathbb{H} . Prove that $\{a + bi \mid a, b \in \mathbb{R}\}$ is a subring of \mathbb{H} which is a field but is not contained in the center of \mathbb{H} .
9. For a fixed element $a \in R$ define $C(a) = \{r \in R \mid ra = ar\}$. Prove that $C(a)$ is a subring of R containing a . Prove that the center of R is the intersection of the subrings $C(a)$ over all $a \in R$.
10. Prove that if D is a division ring then $C(a)$ is a division ring for all $a \in D$ (cf. the preceding exercise).
11. Prove that if R is an integral domain and $x^2 = 1$ for some $x \in R$ then $x = \pm 1$.
12. Prove that any subring of a field which contains the identity is an integral domain.
13. An element x in R is called *nilpotent* if $x^m = 0$ for some $m \in \mathbb{Z}^+$.
 - Show that if $n = a^k b$ for some integers a and b then \overline{ab} is a nilpotent element of $\mathbb{Z}/n\mathbb{Z}$.
 - If $a \in \mathbb{Z}$ is an integer, show that the element $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ is nilpotent if and only if every prime divisor of n is also a divisor of a . In particular, determine the nilpotent elements of $\mathbb{Z}/72\mathbb{Z}$ explicitly.
 - Let R be the ring of functions from a nonempty set X to a field F . Prove that R contains no nonzero nilpotent elements.
14. Let x be a nilpotent element of the commutative ring R (cf. the preceding exercise).
 - Prove that x is either zero or a zero divisor.
 - Prove that rx is nilpotent for all $r \in R$.
 - Prove that $1 + x$ is a unit in R .
 - Deduce that the sum of a nilpotent element and a unit is a unit.
15. A ring R is called a *Boolean ring* if $a^2 = a$ for all $a \in R$. Prove that every Boolean ring is commutative.
16. Prove that the only Boolean ring that is an integral domain is $\mathbb{Z}/2\mathbb{Z}$.
17. Let R and S be rings. Prove that the direct product $R \times S$ is a ring under componentwise addition and multiplication. Prove that $R \times S$ is commutative if and only if both R and S are commutative. Prove that $R \times S$ has an identity if and only if both R and S have identities.
18. Prove that $\{(r, r) \mid r \in R\}$ is a subring of $R \times R$.
19. Let I be any nonempty index set and let R_i be a ring for each $i \in I$. Prove that the direct

- product $\prod_{i \in I} R_i$ is a ring under componentwise addition and multiplication.
20. Let R be the collection of sequences (a_1, a_2, a_3, \dots) of integers a_1, a_2, a_3, \dots where all but finitely many of the a_i are 0 (called the *direct sum* of infinitely many copies of \mathbb{Z}). Prove that R is a ring under componentwise addition and multiplication which does not have an identity.
21. Let X be any nonempty set and let $\mathcal{P}(X)$ be the set of all subsets of X (the *power set* of X). Define addition and multiplication on $\mathcal{P}(X)$ by
- $$A + B = (A - B) \cup (B - A) \quad \text{and} \quad A \times B = A \cap B$$
- i.e., addition is symmetric difference and multiplication is intersection.
- (a) Prove that $\mathcal{P}(X)$ is a ring under these operations ($\mathcal{P}(X)$ and its subrings are often referred to as *rings of sets*).
- (b) Prove that this ring is commutative, has an identity and is a Boolean ring.
22. Give an example of an infinite Boolean ring.
23. Let D be a squarefree integer, and let \mathcal{O} be the ring of integers in the quadratic field $\mathbb{Q}(\sqrt{D})$. For any positive integer f prove that the set $\mathcal{O}_f = \mathbb{Z}[f\omega] = \{a + bf\omega \mid a, b \in \mathbb{Z}\}$ is a subring of \mathcal{O} containing the identity. Prove that $[\mathcal{O} : \mathcal{O}_f] = f$ (index as additive abelian groups). Prove conversely that a subring of \mathcal{O} containing the identity and having finite index f in \mathcal{O} (as additive abelian group) is equal to \mathcal{O}_f . (The ring \mathcal{O}_f is called the *order of conductor* f in the field $\mathbb{Q}(\sqrt{D})$. The ring of integers \mathcal{O} is called the *maximal order* in $\mathbb{Q}(\sqrt{D})$.)
24. Show for $D = 3, 5, 6$, and 7 that the group of units \mathcal{O}^\times of the quadratic integer ring \mathcal{O} is infinite by exhibiting an explicit unit of infinite (multiplicative) order in each ring.
25. Let I be the ring of integral Hamilton Quaternions and define
- $$N : I \rightarrow \mathbb{Z} \quad \text{by} \quad N(a + bi + cj + dk) = a^2 + b^2 + c^2 + d^2$$
- (the map N is called a *norm*).
- (a) Prove that $N(\alpha) = \alpha\bar{\alpha}$ for all $\alpha \in I$, where if $\alpha = a + bi + cj + dk$ then $\bar{\alpha} = a - bi - cj - dk$.
- (b) Prove that $N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in I$.
- (c) Prove that an element of I is a unit if and only if it has norm $+1$. Show that I^\times is isomorphic to the quaternion group of order 8. [The inverse in the ring of rational quaternions of a nonzero element α is $\frac{\bar{\alpha}}{N(\alpha)}$.]
26. Let K be a field. A *discrete valuation* on K is a function $v : K^\times \rightarrow \mathbb{Z}$ satisfying
- (i) $v(ab) = v(a) + v(b)$ (i.e., v is a homomorphism from the multiplicative group of nonzero elements of K to \mathbb{Z}),
 - (ii) v is surjective, and
 - (iii) $v(x+y) \geq \min\{v(x), v(y)\}$ for all $x, y \in K^\times$ with $x+y \neq 0$.
- The set $R = \{x \in K^\times \mid v(x) \geq 0\} \cup \{0\}$ is called the *valuation ring* of v .
- (a) Prove that R is a subring of K which contains the identity. (In general, a ring R is called a *discrete valuation ring* if there is some field K and some discrete valuation v on K such that R is the valuation ring of v .)
- (b) Prove that for each nonzero element $x \in K$ either x or x^{-1} is in R .
- (c) Prove that an element x is a unit of R if and only if $v(x) = 0$.
27. A specific example of a discrete valuation ring (cf. the preceding exercise) is obtained

when p is a prime, $K = \mathbb{Q}$ and

$$\nu_p : \mathbb{Q}^\times \rightarrow \mathbb{Z} \quad \text{by} \quad \nu_p\left(\frac{a}{b}\right) = \alpha \quad \text{where } \frac{a}{b} = p^\alpha \frac{c}{d}, \quad p \nmid c \text{ and } p \nmid d.$$

Prove that the corresponding valuation ring R is the ring of all rational numbers whose denominators are relatively prime to p . Describe the units of this valuation ring.

28. Let R be a ring with $1 \neq 0$. A nonzero element a is called a *left zero divisor* in R if there is a nonzero element $x \in R$ such that $ax = 0$. Symmetrically, $b \neq 0$ is a *right zero divisor* if there is a nonzero $y \in R$ such that $yb = 0$ (so a zero divisor is an element which is either a left or a right zero divisor). An element $u \in R$ has a *left inverse* in R if there is some $s \in R$ such that $su = 1$. Symmetrically, v has a *right inverse* if $vt = 1$ for some $t \in R$.
- (a) Prove that u is a unit if and only if it has both a right and a left inverse (i.e., u must have a two-sided inverse).
 - (b) Prove that if u has a right inverse then u is not a right zero divisor.
 - (c) Prove that if u has more than one right inverse then u is a left zero divisor.
 - (d) Prove that if R is a finite ring then every element that has a right inverse is a unit (i.e., has a two-sided inverse).
29. Let A be any commutative ring with identity $1 \neq 0$. Let R be the set of all group homomorphisms of the additive group A to itself with addition defined as pointwise addition of functions and multiplication defined as function composition. Prove that these operations make R into a ring with identity. Prove that the units of R are the group automorphisms of A (cf. Exercise 20, Section 1.6).
30. Let $A = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \dots$ be the direct product of copies of \mathbb{Z} indexed by the positive integers (so A is a ring under componentwise addition and multiplication) and let R be the ring of all group homomorphisms from A to itself as described in the preceding exercise. Let φ be the element of R defined by $\varphi(a_1, a_2, a_3, \dots) = (a_2, a_3, \dots)$. Let ψ be the element of R defined by $\psi(a_1, a_2, a_3, \dots) = (0, a_1, a_2, a_3, \dots)$.
- (a) Prove that $\varphi\psi$ is the identity of R but $\psi\varphi$ is not the identity of R (i.e., ψ is a *right inverse* for φ but not a left inverse).
 - (b) Exhibit infinitely many right inverses for φ .
 - (c) Find a nonzero element π in R such that $\varphi\pi = 0$ but $\pi\varphi \neq 0$.
 - (d) Prove that there is no nonzero element $\lambda \in R$ such that $\lambda\varphi = 0$ (i.e., φ is a left zero divisor but not a right zero divisor).

7.2 EXAMPLES: POLYNOMIAL RINGS, MATRIX RINGS, AND GROUP RINGS

We introduce here three important types of rings: polynomial rings, matrix rings, and group rings. We shall see in the course of the text that these three classes of rings are often related. For example, we shall see in Part VI that the group ring of a group G over the complex numbers \mathbb{C} is a direct product of matrix rings over \mathbb{C} .

These rings also have many important applications, in addition to being interesting in their own right. In Part III we shall use polynomial rings to prove some classification theorems for matrices which, in particular, determine when a matrix is similar to a diagonal matrix. In Part VI we shall use group rings to study group actions and to prove some additional important classification theorems.

Polynomial Rings

Fix a commutative ring R with identity. We define the ring of polynomials in a form which may already be familiar, at least for polynomials with real coefficients. A definition in terms of Cartesian products is given in Appendix I. Let x be an indeterminate. The formal sum

$$a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$$

with $n \geq 0$ and each $a_i \in R$ is called a *polynomial* in x with coefficients a_i in R . If $a_n \neq 0$, then the polynomial is said to be of *degree* n , a_nx^n is called the *leading term*, and a_n is called the *leading coefficient* (where the leading coefficient of the zero polynomial is taken to be 0). The polynomial is *monic* if $a_n = 1$. The set of all such polynomials is called the ring of *polynomials in the variable x with coefficients in R* and will be denoted $R[x]$.

The operations of addition and multiplication which make $R[x]$ into a ring are the same operations familiar from elementary algebra: addition is “componentwise”

$$\begin{aligned}(a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0) + (b_nx^n + b_{n-1}x^{n-1} + \cdots + b_1x + b_0) \\= (a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + \cdots + (a_1 + b_1)x + (a_0 + b_0)\end{aligned}$$

(here a_n or b_n may be zero in order for addition of polynomials of different degrees to be defined). Multiplication is performed by first defining $(ax^i)(bx^j) = abx^{i+j}$ for polynomials with only one nonzero term and then extending to all polynomials by the distributive laws (usually referred to as “expanding out and collecting like terms”):

$$\begin{aligned}(a_0 + a_1x + a_2x^2 + \dots) \times (b_0 + b_1x + b_2x^2 + \dots) \\= a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \dots\end{aligned}$$

(in general, the coefficient of x^k in the product will be $\sum_{i=0}^k a_i b_{k-i}$). These operations make sense since R is a ring so the sums and products of the coefficients are defined. An easy verification proves that $R[x]$ is indeed a ring with these definitions of addition and multiplication.

The ring R appears in $R[x]$ as the *constant polynomials*. Note that by definition of the multiplication, $R[x]$ is a *commutative ring with identity* (the identity 1 from R).

The coefficient ring R above was assumed to be a commutative ring since that is the situation we shall be primarily interested in, but note that the definition of the addition and multiplication in $R[x]$ above would be valid even if R were not commutative or did not have an identity. If the coefficient ring R is the integers \mathbb{Z} (respectively, the rationals \mathbb{Q}) the polynomial ring $\mathbb{Z}[x]$ (respectively, $\mathbb{Q}[x]$) is the ring of polynomials with integer (rational) coefficients familiar from elementary algebra.

Another example is the polynomial ring $\mathbb{Z}/3\mathbb{Z}[x]$ of polynomials in x with coefficients in $\mathbb{Z}/3\mathbb{Z}$. This ring consists of nonnegative powers of x with coefficients 0, 1, and 2 with calculations on the coefficients performed modulo 3. For example, if

$$p(x) = x^2 + 2x + 1 \quad \text{and} \quad q(x) = x^3 + x + 2$$

then

$$p(x) + q(x) = x^3 + x^2$$

and

$$p(x)q(x) = x^5 + 2x^4 + 2x^3 + x^2 + 2x + 2.$$

The ring in which the coefficients are taken makes a substantial difference in the behavior of polynomials. For example, the polynomial $x^2 + 1$ is not a perfect square in the polynomial ring $\mathbb{Z}[x]$, but is a perfect square in the polynomial ring $\mathbb{Z}/2\mathbb{Z}[x]$, since $(x + 1)^2 = x^2 + 2x + 1 = x^2 + 1$ in this ring.

Proposition 4. Let R be an integral domain and let $p(x), q(x)$ be nonzero elements of $R[x]$. Then

- (1) $\deg p(x)q(x) = \deg p(x) + \deg q(x)$,
- (2) the units of $R[x]$ are just the units of R ,
- (3) $R[x]$ is an integral domain.

Proof: If R has no zero divisors then neither does $R[x]$; if $p(x)$ and $q(x)$ are polynomials with leading terms $a_n x^n$ and $b_m x^m$, respectively, then the leading term of $p(x)q(x)$ is $a_n b_m x^{n+m}$, and $a_n b_m \neq 0$. This proves (3) and also verifies (1). If $p(x)$ is a unit, say $p(x)q(x) = 1$ in $R[x]$, then $\deg p(x) + \deg q(x) = 0$, so both $p(x)$ and $q(x)$ are elements of R , hence are units in R since their product is 1. This proves (2).

If the ring R has zero divisors then so does $R[x]$, because $R \subset R[x]$. Also, if $f(x)$ is a zero divisor in $R[x]$ (i.e., $f(x)g(x) = 0$ for some nonzero $g(x) \in R[x]$) then in fact $cf(x) = 0$ for some nonzero $c \in R$ (cf. Exercise 2).

If S is a subring of R then $S[x]$ is a subring of $R[x]$. For instance, $\mathbb{Z}[x]$ is a subring of $\mathbb{Q}[x]$. Some other examples of subrings of $R[x]$ are the set of all polynomials in x^2 (i.e., in which only even powers of x appear) and the set of all polynomials with zero constant term (the latter subring does not have an identity).

Polynomial rings, particularly those over fields, will be studied extensively in Chapter 9.

Matrix Rings

Fix an arbitrary ring R and let n be a positive integer. Let $M_n(R)$ be the set of all $n \times n$ matrices with entries from R . The element (a_{ij}) of $M_n(R)$ is an $n \times n$ square array of elements of R whose entry in row i and column j is $a_{ij} \in R$. The set of matrices becomes a ring under the usual rules by which matrices of real numbers are added and multiplied. Addition is componentwise: the i, j entry of the matrix $(a_{ij}) + (b_{ij})$ is $a_{ij} + b_{ij}$. The i, j entry of the matrix product $(a_{ij}) \times (b_{ij})$ is $\sum_{k=1}^n a_{ik} b_{kj}$ (note that these matrices need to be square in order that multiplication of any two elements be defined). It is a straightforward calculation to check that these operations make $M_n(R)$ into a ring. When R is a field we shall prove that $M_n(R)$ is a ring by less computational means in Part III.

Note that if R is any nontrivial ring (even a commutative one) and $n \geq 2$ then $M_n(R)$ is not commutative: if $ab \neq 0$ in R let A be the matrix with a in position 1,1 and zeros elsewhere and let B be the matrix with b in position 1,2 and zeros elsewhere; then ab is the (nonzero) entry in position 1,2 of AB whereas BA is the zero matrix.

These two matrices also show that $M_n(R)$ has zero divisors for all nonzero rings R whenever $n \geq 2$.

An element (a_{ij}) of $M_n(R)$ is called a *scalar matrix* if for some $a \in R$, $a_{ii} = a$ for all $i \in \{1, \dots, n\}$ and $a_{ij} = 0$ for all $i \neq j$ (i.e., all diagonal entries equal a and all off-diagonal entries are 0). The set of scalar matrices is a subring of $M_n(R)$. This subring is a copy of R (i.e., is “isomorphic” to R): if the matrix A has the element a along the main diagonal and the matrix B has the element b along the main diagonal then the matrix $A + B$ has $a + b$ along the diagonal and AB has ab along the diagonal (and all other entries 0). If R is commutative, the scalar matrices commute with all elements of $M_n(R)$. If R has a 1, then the scalar matrix with 1's down the diagonal (the $n \times n$ *identity matrix*) is the 1 of $M_n(R)$. In this case the units in $M_n(R)$ are the invertible $n \times n$ matrices and the group of units is denoted $GL_n(R)$, the *general linear group* of degree n over R .

If S is a subring of R then $M_n(S)$ is a subring of $M_n(R)$. For instance $M_n(\mathbb{Z})$ is a subring of $M_n(\mathbb{Q})$ and $M_n(2\mathbb{Z})$ is a subring of both of these. Another example of a subring of $M_n(R)$ is the set of *upper triangular* matrices: $\{(a_{ij}) \mid a_{pq} = 0 \text{ whenever } p > q\}$ (the set of matrices all of whose entries below the main diagonal are zero) — one easily checks that the sum and product of upper triangular matrices is upper triangular.

Group Rings

Fix a commutative ring R with identity $1 \neq 0$ and let $G = \{g_1, g_2, \dots, g_n\}$ be any finite group with group operation written multiplicatively. Define the *group ring*, RG , of G with coefficients in R to be the set of all formal sums

$$a_1g_1 + a_2g_2 + \cdots + a_ng_n \quad a_i \in R, \quad 1 \leq i \leq n.$$

If g_1 is the identity of G we shall write a_1g_1 simply as a_1 . Similarly, we shall write the element $1g$ for $g \in G$ simply as g .

Addition is defined “componentwise”

$$\begin{aligned} (a_1g_1 + a_2g_2 + \cdots + a_ng_n) + (b_1g_1 + b_2g_2 + \cdots + b_ng_n) \\ = (a_1 + b_1)g_1 + (a_2 + b_2)g_2 + \cdots + (a_n + b_n)g_n. \end{aligned}$$

Multiplication is performed by first defining $(ag_i)(bg_j) = (ab)g_k$, where the product ab is taken in R and $g_i g_j = g_k$ is the product in the group G . This product is then extended to all formal sums by the distributive laws so that the coefficient of g_k in the product $(a_1g_1 + \cdots + a_ng_n) \times (b_1g_1 + \cdots + b_ng_n)$ is $\sum_{g_i g_j = g_k} a_i b_j$. It is straightforward to check that these operations make RG into a ring (again, commutativity of R is not needed). The associativity of multiplication follows from the associativity of the group operation in G . The ring RG is commutative if and only if G is a commutative group.

Example

Let $G = D_8$ be the dihedral group of order 8 with the usual generators r, s ($r^4 = s^2 = 1$ and $rs = sr^{-1}$) and let $R = \mathbb{Z}$. The elements $\alpha = r + r^2 - 2s$ and $\beta = -3r^2 + rs$ are