ABSTRACT ALGEBRA

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
$G = \langle \ldots \mid \ldots \rangle$	generators and relations (a presentation) for G
$\ker \varphi$, $\operatorname{im} \varphi$	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
$\mathrm{Aut}(G)$	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
$R[x], R[x_1, \ldots, x_n]$	polynomials in x, and in $x_1, \ldots, x_n$ 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
$\varinjlim A_i, \varprojlim A_i$	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)
$\mathrm{tr}(A)$	the trace of the matrix A
$\mathrm{Hom}_R(A, B)$	the R-module homomorphisms from A to B
$\mathrm{End}(M)$	the endomorphism ring of the module M
$\mathrm{Tor}(M)$	the torsion submodule of M
$\mathrm{Ann}(M)$	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
$\mathrm{ch}(F)$	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 polynomal of α over the field F
$\mathrm{Aut}(K)$	the group of automorphisms of a field K
$\mathrm{Aut}(K/F)$	the group of automorphisms of a field K fixing the field F
$\mathrm{Gal}(K/F)$	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
$\mathrm{rad}\, I$	the radical of the ideal I
$\mathrm{Ass}_R(M)$	the associated primes for the module M
$\mathrm{Supp}(M)$	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 $\mathcal{O}_{v,V}$
$\mathrm{Spec}\, R$, $\mathrm{mSpec}\, R$	the prime spectrum, and the maximal spectrum of R
$\mathcal{O}_X$	the structure sheaf of $X = \mathrm{Spec}\, R$
$\mathcal{O}(U)$	the ring of sections on an open set U in $\mathrm{Spec}\, R$
$\mathcal{O}_P$	the stalk of the structure sheaf at P
$\mathrm{Jac}\, R$	the Jacobson radical of the ring R
$\mathrm{Ext}_R^n(A, B)$	the n^{th} cohomology group derived from Hom_R
$\mathrm{Tor}_n^R(A, B)$	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
$\mathrm{Stab}(1 \trianglelefteq A \trianglelefteq G)$	the stability group of the series $1 \trianglelefteq A \trianglelefteq G$
$\|\|\theta\|\|$	the norm of the character θ
$\mathrm{Ind}_H^G(\psi)$	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.

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

Contents

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

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

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) $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$ 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) $\mathbb{R} = \{$ all decimal expansions $\pm d_1 d_2 \ldots d_n . a_1 a_2 a_3 \ldots\}$ 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 $f : A \to B$ 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 $f : A \to B$ and $g : B \to C$, then the composite map $g \circ f : A \to C$ is defined by

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

Let $f : A \to B$.

(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 $g : B \to A$ such that $g \circ f : A \to A$ 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 $h : B \to A$ such that $f \circ h : B \to B$ is the identity map on B.

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

(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 $g : B \to A$ 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 $f : A \to B$ 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 $f : B \to C$, 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 $g : A \to C$ and there is a function $f : B \to C$ 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 $a, b, c \in A$.

A relation is an *equivalence relation* if it is reflexive, symmetric and transitive.

(3) 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) $A = \cup_{i \in I} A_i$, 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) $f : \mathbb{Q} \to \mathbb{Z}$ defined by $f(a/b) = a$.
   (b) $f : \mathbb{Q} \to \mathbb{Q}$ defined by $f(a/b) = a^2/b^2$.
6. Determine whether the function $f : \mathbb{R}^+ \to \mathbb{Z}$ 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 $f : A \to B$ 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 $a \mid b$; 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) $d \mid a$ and $d \mid b$ (so d is a common divisor of a and b), and
   (b) if $e \mid a$ and $e \mid b$, then $e \mid d$ (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) $a \mid l$ and $b \mid l$ (so l is a common multiple of a and b), and
   (b) if $a \mid m$ and $b \mid m$, then $l \mid m$ (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

$$\begin{aligned} a &= q_0 b + r_0 && (0)\\ b &= q_1 r_0 + r_1 && (1)\\ r_0 &= q_2 r_1 + r_2 && (2)\\ r_1 &= q_3 r_2 + r_3 && (3)\\ &\vdots\\ r_{n-2} &= q_n r_{n-1} + r_n && (n)\\ r_{n-1} &= q_{n+1} r_n && (n{+}1) \end{aligned}$$

where r_n is the last nonzero remainder. Such an r_n exists since $|b| > |r_0| > |r_1| > \cdots > |r_n|$ 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:

$$\begin{aligned} 57970 &= (5)10353 + 6205\\ 10353 &= (1)6205 + 4148\\ 6205 &= (1)4148 + 2057\\ 4148 &= (2)2057 + 34\\ 2057 &= (60)34 + 17\\ 34 &= (2)17 \end{aligned}$$

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 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 $p_1, p_2, \ldots, p_s$ and positive integers $\alpha_1, \alpha_2, \ldots, \alpha_s$ such that

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

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

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

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:

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

where $p_1, p_2, \ldots, p_s$ 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

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

(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

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

(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

1. 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) $a = 20, b = 13$.
(b) $a = 69, b = 372$.
(c) $a = 792, b = 275$.
(d) $a = 11391, b = 5673$.
(e) $a = 1761, b = 1567$.
(f) $a = 507885, b = 60808$.

2. 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 $n! = n(n-1)(n-2)\ldots 2 \cdot 1$ (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.,

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

There are precisely n distinct equivalence classes mod n, namely
$$\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}$$
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

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

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

$$\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{11}$$

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 $-7, -19, \ldots$) 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 $\bar{5} + \bar{8} = \overline{13} = \bar{1}$ 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 $\bar{5} + \bar{8} = \overline{(17 - 28)} = \overline{-11} = \bar{1}$ and as we mentioned the result does not depend on the choice of representatives chosen. The product of these two classes is $\bar{a} \cdot \bar{b} = \overline{5 \cdot 8} = \overline{40} = \bar{4}$, 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 $\{0, 1, \ldots, n-1\}$ 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 $\overline{-7} = \overline{53}$ is the multiplicative inverse of $\overline{17}$ 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 $\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}$ (use the Division Algorithm).
3. Prove that if $a = a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_1 10 + a_0$ is any positive integer then $a \equiv a_n + a_{n-1} + \cdots + a_1 + a_0 \pmod{9}$ (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.*

[1] For 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)

[2] See *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 $\star : G \times G \to G$. 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 $a^{-1} = \dfrac{1}{a}$, 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 $\overline{-a}$. 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

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 $a_1, a_2, \ldots, a_n \in G$ the value of $a_1 \star a_2 \star \cdots \star a_n$ 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:

$$\begin{aligned} b^{-1} \star (b \star c) &= b^{-1} \star a^{-1} \\ (b^{-1} \star b) \star c &= b^{-1} \star a^{-1} \\ e \star c &= b^{-1} \star a^{-1} \\ c &= b^{-1} \star a^{-1}, \end{aligned}$$

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 $\bar{6} \neq \bar{0}$, $\bar{6} + \bar{6} = \overline{12} = \bar{3} \neq \bar{0}$, but $\bar{6} + \bar{6} + \bar{6} = \overline{18} = \bar{0}$, 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 $G = \{g_1, g_2, \ldots, g_n\}$ 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.

1. Determine which of the following binary operations are associative:
- **(a)** the operation $\star$ on $\mathbb{Z}$ defined by $a \star b = a - b$
- **(b)** the operation $\star$ on $\mathbb{R}$ defined by $a \star b = a + b + ab$
- **(c)** the operation $\star$ on $\mathbb{Q}$ defined by $a \star b = \dfrac{a+b}{5}$
- **(d)** the operation $\star$ on $\mathbb{Z} \times \mathbb{Z}$ defined by $(a, b) \star (c, d) = (ad + bc, bd)$
- **(e)** the operation $\star$ on $\mathbb{Q} - \{0\}$ defined by $a \star b = \dfrac{a}{b}$.

2. Decide which of the binary operations in the preceding exercise are commutative.

3. Prove that addition of residue classes in $\mathbb{Z}/n\mathbb{Z}$ is associative (you may assume it is well defined).

4. Prove that multiplication of residue classes in $\mathbb{Z}/n\mathbb{Z}$ is associative (you may assume it is well defined).

5. Prove for all $n > 1$ that $\mathbb{Z}/n\mathbb{Z}$ is not a group under multiplication of residue classes.

6. Determine which of the following sets are groups under addition:
- **(a)** the set of rational numbers (including $0 = 0/1$) in lowest terms whose denominators are odd
- **(b)** the set of rational numbers (including $0 = 0/1$) in lowest terms whose denominators are even
- **(c)** the set of rational numbers of absolute value < 1
- **(d)** the set of rational numbers of absolute value ≥ 1 together with 0
- **(e)** the set of rational numbers with denominators equal to 1 or 2
- **(f)** the set of rational numbers with denominators equal to 1, 2 or 3.

7. 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 $(\mathbb{Z}/12\mathbb{Z})^\times$: $\overline{1}$, $\overline{-1}$, $\overline{5}$, $\overline{7}$, $\overline{-7}$, $\overline{13}$.

13. Find the orders of the following elements of the additive group $\mathbb{Z}/36\mathbb{Z}$: $\overline{1}$, $\overline{2}$, $\overline{6}$, $\overline{9}$, $\overline{10}$, $\overline{12}$, $\overline{-1}$, $\overline{-10}$, $\overline{-18}$.

14. Find the orders of the following elements of the multiplicative group $(\mathbb{Z}/36\mathbb{Z})^\times$: $\overline{1}$, $\overline{-1}$, $\overline{5}$, $\overline{13}$, $\overline{-13}$, $\overline{17}$.

15. Prove that $(a_1 a_2 \ldots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \ldots a_1^{-1}$ for all $a_1, a_2, \ldots, a_n \in G$.

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 $1, x, x^2, \ldots, x^{n-1}$ are all distinct. Deduce that $|x| \leq |G|$.

33. Let x be an element of finite order n in G.
(a) Prove that if n is odd then $x^i \neq x^{-i}$ for all $i = 1, 2, \ldots, n-1$.
(b) 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.

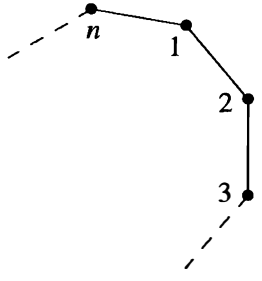
35. If x is an element of finite order n in G, use the Division Algorithm to show that *any* integral power of x equals one of the elements in the set $\{1, x, x^2, \ldots, x^{n-1}\}$ (so these are all the distinct elements of the cyclic subgroup (cf. Exercise 27 above) of G generated by x).

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.

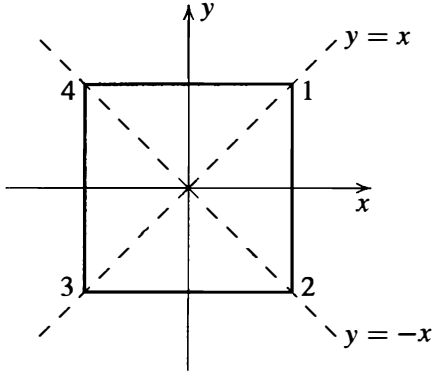


Then each symmetry s can be described uniquely by the corresponding permutation σ of $\{1, 2, 3, \ldots, n\}$ where if the symmetry s puts vertex i in the place where vertex j was originally, then σ is the permutation sending i to j. For instance, if s is a rotation of $2\pi/n$ radians clockwise about 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) $1, r, r^2, \ldots, r^{n-1}$ 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

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

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 $\{1, 2, \ldots, n\}$ 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 $n = 12$,

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

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 $R_1, R_2, \ldots, R_m$ (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

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

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

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

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:

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

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 $y^k x^i$ 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

$$Y = \langle u, v \mid u^4 = v^3 = 1,\ uv = v^2u^2 \rangle. \tag{1.3}$$

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 $\sigma : \Omega \to \Omega$ and $\tau : \Omega \to \Omega$ 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, $\sigma^{-1} : \Omega \to \Omega$ satisfying $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = 1$. Thus, all the group axioms hold for $(S_\Omega, \circ)$. 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 $\Omega = \{1, 2, 3, \ldots, n\}$, 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 $\{1, 2, 3, \ldots, n\}$ 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 $\{1, 2, 3, \ldots, n\}$; $\sigma(2)$ 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 $n \cdot (n-1) \cdot (n-2) \ldots 2 \cdot 1 = n!$ possible injective functions from $\{1, 2, 3, \ldots, n\}$ to itself. Hence there are precisely $n!$ permutations of $\{1, 2, 3, \ldots, n\}$ so there are precisely $n!$ elements in S_n.

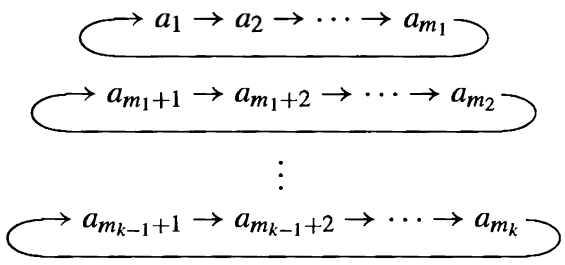
We now describe an efficient notation for writing elements σ of S_n which we shall use throughout the text and which is called the *cycle decomposition*.

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 $(a_1\, a_2\, \ldots\, a_m)$ 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

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

from which the action of σ on any number from 1 to n can easily be read, as follows. For any $x \in \{1, 2, 3, \ldots, n\}$ 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

[1] We 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

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

Cycle Decomposition Algorithm

Method	Example
To start a new cycle pick the smallest element of $\{1, 2, \ldots, n\}$ 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: $(a\,b$	$\sigma(1) = 12 = b$, $12 \neq 1$ 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: $(a\,b\,c$ 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 $\{1, 2, \ldots, n\}$ 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 $(1)(2)\ldots(n)$ 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 $\{1, 2, 3, \ldots, n\}$ and fixes each element of $\{n+1, n+2, \ldots, m\}$. 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 $(1\ 2\ 3) \circ (1\ 2)(3\ 4)$ 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,

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

In particular this shows that

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

Each cycle $(a_1\, a_2 \ldots a_m)$ in a cycle decomposition can be viewed as the permutation which cyclically permutes $a_1, a_2, \ldots, a_m$ 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, $(a_1\, a_2 \ldots a_m)$, permutes $\{a_1, a_2, \ldots, a_m\}$ cyclically, the numbers in the cycle itself can be cyclically permuted without altering the permutation, i.e.,

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

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

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

and let τ be the permutation

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

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 $\Omega = \{1, 2, 3, \ldots\}$ 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 $(a_1\ a_2\ \ldots\ a_m)$, then for all $i \in \{1, 2, \ldots, m\}$, $\sigma^i(a_k) = a_{k+i}$, 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 $\ldots$ 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

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

[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:

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

(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 $|GL_n(F)| = (q^n - 1)(q^n - q)(q^n - q^2) \ldots (q^n - q^{n-1})$.

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 $G = \{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{R},\ a \neq 0,\ c \neq 0\}$.

(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 $H(F) = \{\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in F\}$ — 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:

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

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

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

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

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 $\varphi : G \to H$ such that

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

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 $\varphi : G \to H$ 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 $\exp : \mathbb{R} \to \mathbb{R}^+$ 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 $\varphi : S_\Delta \to S_\Omega$ 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 $\varphi : G \to H$ 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 $S = \{s_1, \ldots, s_m\}$ be the generators. Let H be another group and $\{r_1, \ldots, r_m\}$ 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 $\varphi : G \to H$ 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 $\{r_1, \ldots, r_m\}$, 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

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

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 $\varphi : G \to H$ 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 $n \in \mathbb{Z}$.

2. If $\varphi : G \to H$ 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?

3. If $\varphi : G \to H$ is an isomorphism, prove that G is abelian if and only if H is abelian. If $\varphi : G \to H$ is a homomorphism, what additional conditions on φ (if any) are sufficient to ensure that if G is abelian, then so is H?

4. Prove that the multiplicative groups $\mathbb{R} - \{0\}$ and $\mathbb{C} - \{0\}$ are not isomorphic.

5. Prove that the additive groups $\mathbb{R}$ and $\mathbb{Q}$ are not isomorphic.

6. Prove that the additive groups $\mathbb{Z}$ and $\mathbb{Q}$ are not isomorphic.

7. Prove that D_8 and Q_8 are not isomorphic.

8. Prove that if $n \neq m$, S_n and S_m are not isomorphic.

9. Prove that D_{24} and S_4 are not isomorphic.

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

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

and prove the following:

(a) 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.

(b) φ is a bijection from S_Δ onto S_Ω. [Find a 2-sided inverse for φ.]

(c) 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).

11. Let A and B be groups. Prove that $A \times B \cong B \times A$.

12. Let A, B, and C be groups and let $G = A \times B$ and $H = B \times C$. Prove that $G \times C \cong A \times H$.

13. Let G and H be groups and let $\varphi : G \to H$ 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 $G \cong \varphi(G)$.

14. Let G and H be groups and let $\varphi : G \to H$ 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.

15. Define a map $\pi : \mathbb{R}^2 \to \mathbb{R}$ by $\pi((x, y)) = x$. Prove that π is a homomorphism and find the kernel of π (cf. Exercise 14).

16. Let A and B be groups and let G be their direct product, $A \times B$. Prove that the maps $\pi_1 : G \to A$ and $\pi_2 : G \to B$ defined by $\pi_1((a, b)) = a$ and $\pi_2((a, b)) = b$ are homomorphisms and find their kernels (cf. Exercise 14).

17. 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.

18. 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.

19. 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 $\mathrm{Aut}(G)$ be the set of all isomorphisms from G onto G. Prove that $\mathrm{Aut}(G)$ is a group under function composition (called the *automorphism group* of G and the elements of $\mathrm{Aut}(G)$ 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 $\varphi : D_{2n} \to GL_2(\mathbb{R})$ defined on generators by

$$\varphi(r) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \qquad \text{and} \qquad \varphi(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

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

$$\varphi(i) = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix} \qquad \text{and} \qquad \varphi(j) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

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

$$\sigma_g : A \to A$$
$$\sigma_g(a) = g \cdot a.$$

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 $a \in A$

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

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 $\varphi : G \to S_A$ 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 $a \in A$

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

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 $\varphi : G \to S_A$ 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

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

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 $G \to S_A$ 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

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

for all $\alpha \in \mathbb{R}$, $(r_1, r_2, \ldots, r_n) \in \mathbb{R}^n$, 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 $\{1, 2, \ldots, n\}$ by the way the symmetry α permutes the corresponding vertices. The map of $D_{2n} \times \{1, 2, \ldots, n\}$ onto $\{1, 2, \ldots, n\}$ defined by $(\alpha, i) \to \sigma_\alpha(i)$ defines a group action of D_{2n} on $\{1, 2, \ldots, n\}$. 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*:

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

(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 $G \to S_A$ (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 $\sigma \cdot \{a_1, \ldots, a_k\} = \{\sigma(a_1), \ldots, \sigma(a_k)\}$.
(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

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

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 $\{1, r, r^2, \ldots, r^{n-1}\}$, 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 $x, x^2, x^3, \ldots$ 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) $\{a^n \mid a \in A\}$
(b) $\{a \in A \mid a^n = 1\}$.

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 $H_1 \leq H_2 \leq \cdots$ 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 $s^i r^j \in N_{D_8}(A)$ 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 $y \in G_s$,

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

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

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

This proves G_s is a subgroup[1] 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).

[1]Notice 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

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

(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 $i \in \{1, 2, \ldots, n\}$ 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 $r_1, \ldots, r_4$ are nonnegative integers. For example,

$$12x_1^5x_2^7x_4 - 18x_2^3x_3 + 11x_1^6x_2x_3^3x_4^{23} \qquad (*)$$

is a typical element of R. Each $\sigma \in S_4$ gives a permutation of $\{x_1, \ldots, x_4\}$ 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 $p(x_1, \ldots, x_4)$ 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 $p = p(x_1, \ldots, x_4)$ 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 $x_1, x_2, \ldots, x_n$, 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 $r_1, \ldots, r_n$ are nonnegative integers. For each $\sigma \in S_n$ define a map

$$\sigma : R \to R \qquad \text{by} \qquad \sigma \cdot p(x_1, x_2, \ldots, x_n) = p(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}).$$

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 $1, r, r^2, \ldots, r^{n-1}$ (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,

$$r^n = 1,\ r^{n+1} = r,\ r^{n+2} = r^2, \ldots$$
$$r^{-1} = r^{n-1},\ r^{-2} = r^{n-2}, \ldots \quad \text{etc.}$$

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

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

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 $1, x, x^2, \ldots, x^{n-1}$ 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 $1, x, x^2, \ldots, x^{n-1}$ 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

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

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

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

is well defined and is an isomorphism

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

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

is well defined and is an isomorphism.

Proof: Suppose $\langle x \rangle$ and $\langle y \rangle$ are both cyclic groups of order n. Let $\varphi : \langle x \rangle \to \langle y \rangle$ 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 $\varphi : \mathbb{Z} \to \langle x \rangle$ 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 $|x^a| = \dfrac{n}{(n, a)}$.

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

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

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

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 $a \in \{1, 2, \ldots, n\}$ 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 $\overline{11}$ 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 $1, 2, 3, \ldots$.

(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 $x^d \in K$, $\langle x^d \rangle \leq K$. 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

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

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 $K \leq \langle x^d \rangle$ 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 $d = \dfrac{n}{a}$ 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) $\mathbb{Z}/12\mathbb{Z} = \langle \bar{1} \rangle = \langle \bar{5} \rangle = \langle \bar{7} \rangle = \langle \overline{11} \rangle$ (order 12)
(b) $\langle \bar{2} \rangle = \langle \overline{10} \rangle$ (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:
    (a) $Z_2 \times Z_2$
    (b) $Z_2 \times \mathbb{Z}$
    (c) $\mathbb{Z} \times \mathbb{Z}$.
13. Prove that the following pairs of groups are *not* isomorphic:
    (a) $\mathbb{Z} \times Z_2$ and $\mathbb{Z}$
    (b) $\mathbb{Q} \times Z_2$ 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 $(1 + p)^{p^{n-1}} \equiv 1 (\text{mod } p^n)$ but $(1 + p)^{p^{n-2}} \not\equiv 1 (\text{mod } p^n)$. 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 $(1+2^2)^{2^{n-2}} \equiv 1 (\text{mod } 2^n)$ but $(1+2^2)^{2^{n-3}} \not\equiv 1 (\text{mod } 2^n)$. 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 $x \in G$.

(a) Prove that if $g \in N_G(\langle x \rangle)$ then $gxg^{-1} = x^a$ for some $a \in \mathbb{Z}$.

(b) 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 $gx^kg^{-1} = (gxg^{-1})^k = x^{ak}$ 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^ig^{-1}, $i = 0, 1, \ldots, n-1$ 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

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

(a) 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).

(b) Prove that $\sigma_a = \sigma_b$ if and only if $a \equiv b (\text{mod } n)$.

(c) Prove that *every* automorphism of Z_n is equal to σ_a for some integer a.

(d) Prove that $\sigma_a \circ \sigma_b = \sigma_{ab}$. Deduce that the map $\overline{a} \mapsto \sigma_a$ 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 $A = \{v_1, v_2, \ldots, v_n\}$, then there is a unique smallest subspace of

G which contains A, namely the (linear) span of $v_1, v_2, \ldots, v_n$ and each vector in this span can be written as $k_1v_1 + k_2v_2 + \cdots + k_nv_n$, for some $k_1, \ldots, k_n \in \mathbb{R}$. 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 $\{a_1, a_2, \ldots, a_n\}$ we write $\langle a_1, a_2, \ldots, a_n \rangle$ for the group generated by $a_1, a_2, \ldots, a_n$ instead of $\langle \{a_1, a_2, \ldots, a_n\} \rangle$. 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

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

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 $a = a_1^{\epsilon_1} a_2^{\epsilon_2} \ldots a_n^{\epsilon_n}$ and $b = b_1^{\delta_1} b_2^{\delta_2} \ldots b_m^{\delta_m}$, then

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

(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 $a_1^{\epsilon_1} a_2^{\epsilon_2} \ldots a_n^{\epsilon_n}$, 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

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

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 $\{a_1, a_2, \ldots, a_k\}$ of the abelian group G, one easily checks that

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

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 $a_1^{\alpha_1} a_2^{\alpha_2} \ldots a_k^{\alpha_k}$ is at most $d_1 d_2 \ldots d_k$, that is,

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

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 $abab \ldots ab$ 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:

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

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 $G = \langle g_1, g_2, \ldots, g_n \rangle$, 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^kth 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 $n \in \mathbb{Z}^+$, $\{e^{2\pi it/n} \mid t = 0, 1, \ldots, n-1\}$ 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* if 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 lattice[2] 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

[2]The 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).

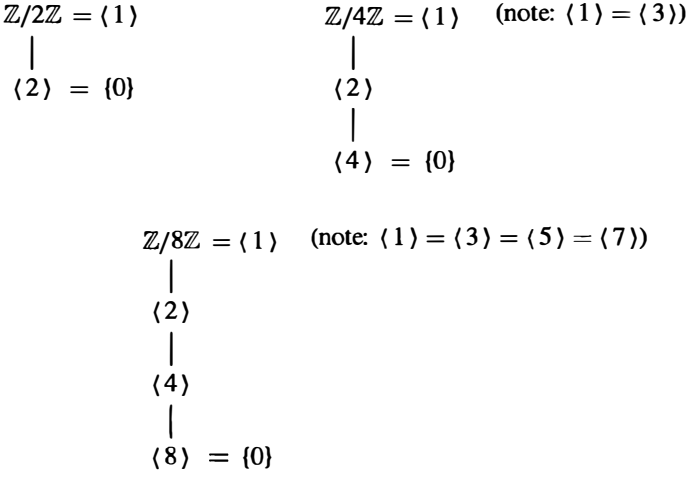
There are some limitations to this process, in particular it cannot be carried out per se for infinite groups. Even for finite groups of relatively small order, lattices can be quite complicated (see the book *Groups of Order* 2^n, $n \leq 6$ by M. Hall and J. Senior, Macmillan, 1964, for some hair-raising 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).

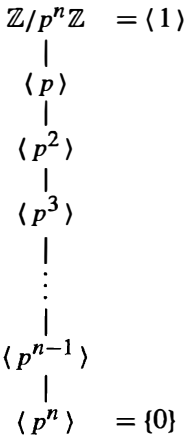
Examples

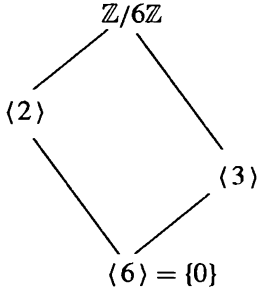
Except for the cyclic groups (Example 1) we have not proved that the following lattices are correct (e.g., contain all subgroups of the given group or have the right joins and intersections). For the moment we shall take these facts as given and, as we build up more theory in the course of the text,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

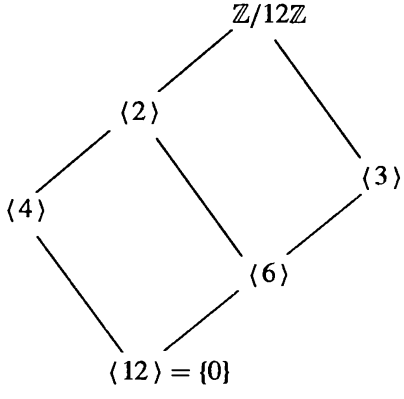
(1) For $G = Z_n \cong \mathbb{Z}/n\mathbb{Z}$, by Theorem 7 the lattice of subgroups of G is the lattice of divisors of n (that is, the divisors of n are written on a page with n at the bottom, 1 at the top and paths upwards from a to b if $b \mid a$). Some specific examples for various values of n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



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



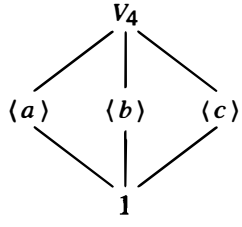




(2) The *Klein 4-group (Viergruppe)*, V_4, is the group of order 4 with multiplication table

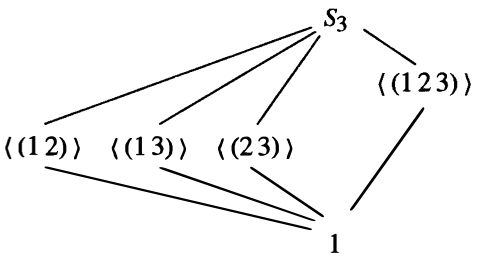
$\cdot$	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

and lattice

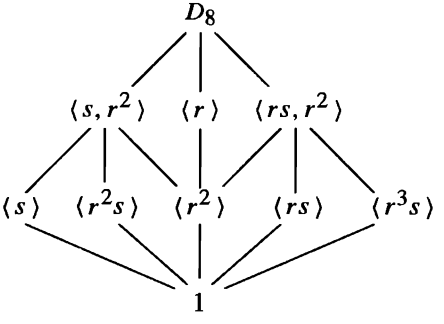


Note that V_4 is abelian and is not isomorphic to Z_4 (why?). We shall see that D_8 has an isomorphic copy of V_4 as a subgroup, so it will not be necessary to check that the associative law holds for the binary operation defined above.

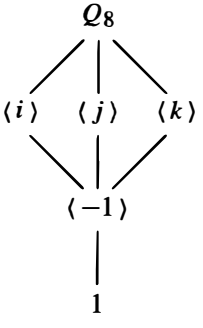
(3) The lattice of S_3 is



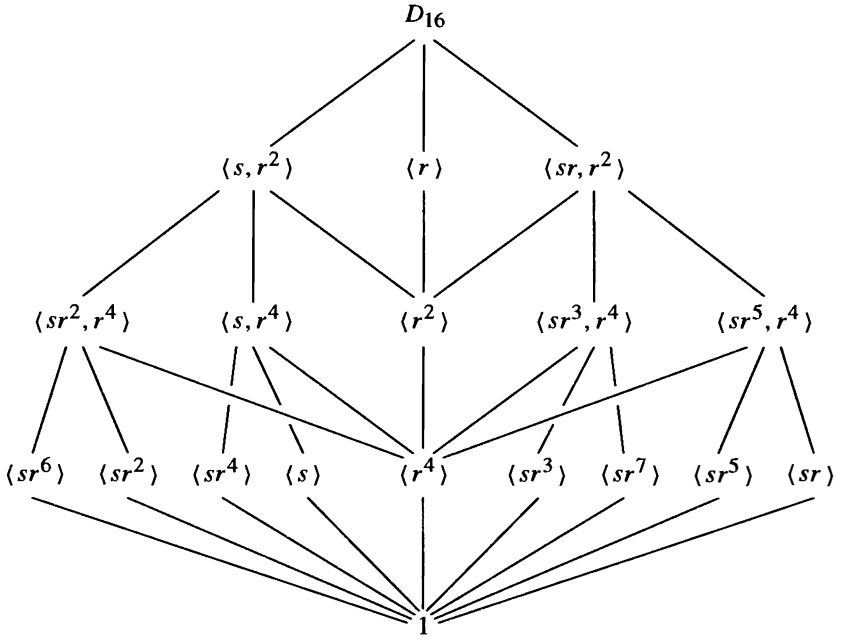
(4) Using our usual notation for $D_8 = \langle r, s \rangle$, the lattice of D_8 is



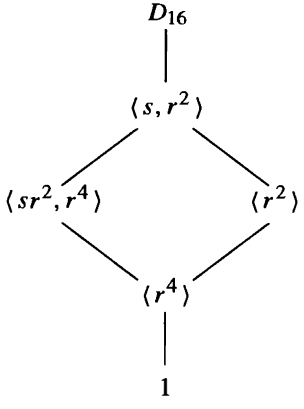
(5) The lattice of subgroups of Q_8 is



(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 $\langle sr^2, r^4 \rangle$ and $\langle r^2 \rangle$ 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

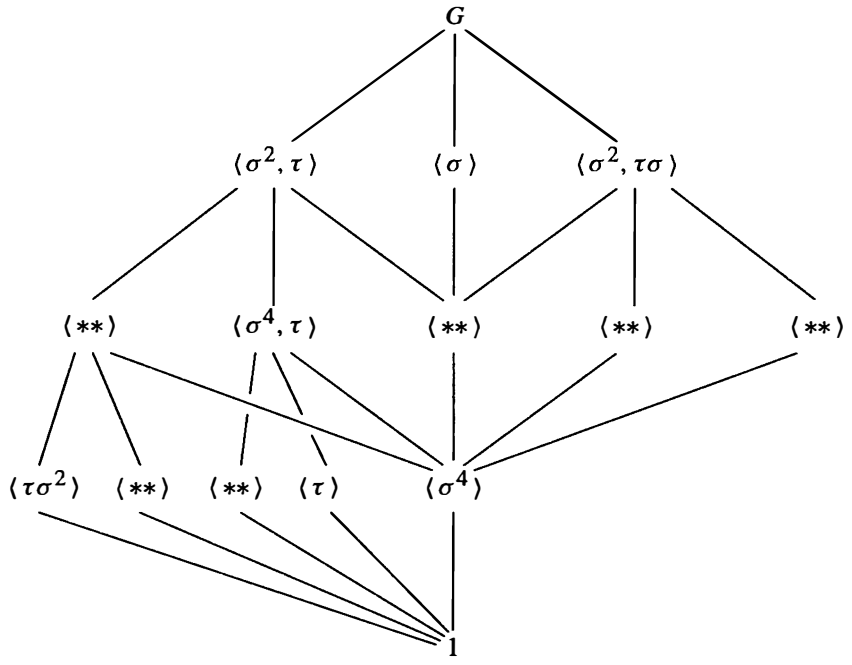
1. Let H and K be subgroups of G. Exhibit all possible sublattices which show only G, 1, H, K and their joins and intersections. What distinguishes the different drawings?
2. In each of (a) to (d) list all subgroups of D_{16} that satisfy the given condition.
   (a) Subgroups that are contained in $\langle sr^2, r^4 \rangle$
   (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.

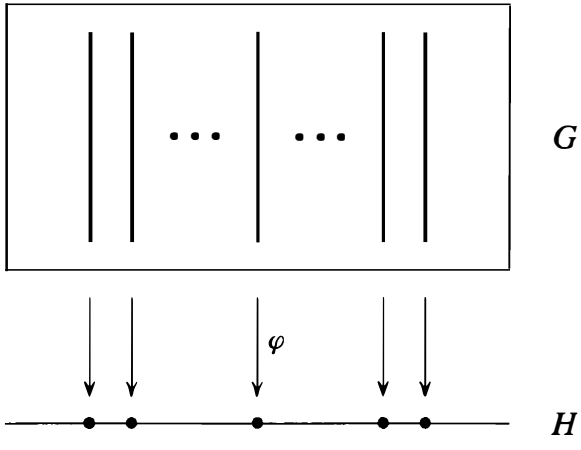


Fig. 1

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., $X_aX_b = X_{ab}$. 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: $(X_aX_b)X_c = (X_{ab})X_c = X_{(ab)c}$ and $X_a(X_bX_c) = X_a(X_{bc}) = X_{a(bc)}$. Since $(ab)c = a(bc)$ in H, $(X_aX_b)X_c = X_a(X_bX_c)$. 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 $H = Z_n = \langle x \rangle$ be the cyclic group of order n and define $\varphi : \mathbb{Z} \to Z_n$ 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 Z_n is multiplication). Note also that φ is surjective. The fiber of φ over x^a is then

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

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

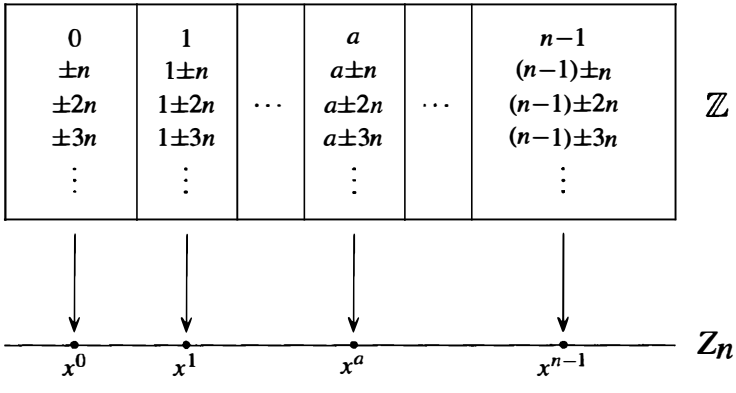


Fig. 2

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 $\varphi : G \to H$ lying above the identity of H is given a name:

Definition. If φ is a homomorphism $\varphi : G \to H$, 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 $\varphi : G \to H$ 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 $\varphi : G \to H$ 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 $\varphi : G \to H$ 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 $u \in X$, $\quad X = \{uk \mid k \in K\}$

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

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

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

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 $\varphi : G \to H$ 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.

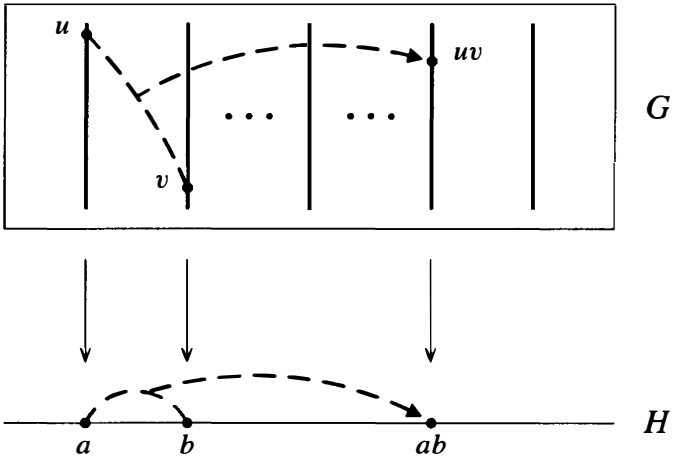


Fig. 3

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 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 $\mathbb{Z}/n\mathbb{Z} \cong Z_n$ of Chapter 2.

(2) If $\varphi : G \to H$ 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 $\varphi : G \to H$ 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 $\varphi : \mathbb{R}^2 \to \mathbb{R}$ 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):

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

Hence Figure 1 in this example becomes

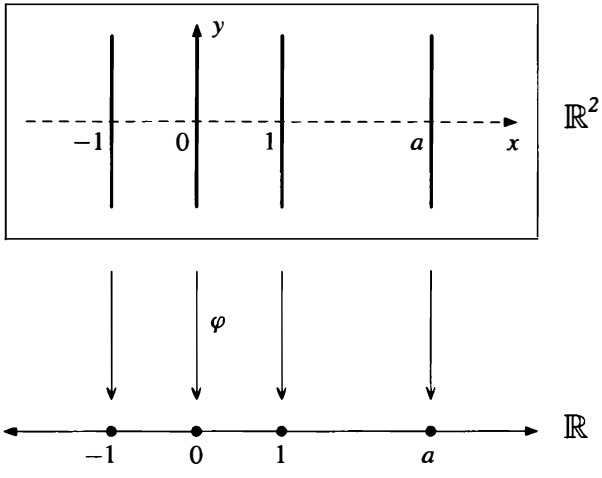


Fig. 4

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 $\varphi : Q_8 \to V_4$ by

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

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 $Q_8/\langle \pm 1 \rangle$ 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

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

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

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

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

$$ut = (vm_1)t = v(m_1 t) \in vN.$$

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 $u, v \in G$,

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

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 $u_1v_1 \in uvN$:

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

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

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

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 $\pi : G \to G/N$ by

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

By definition of the operation in G/N,

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

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 $\pi : G \to G/N$ defined by $\pi(g) = gN$ is called the *natural projection (homomorphism)*[1] of G onto G/N. If $\overline{H} \leq G/N$ is a subgroup of G/N, the *complete preimage* Of $\overline{H}$ in G is the preimage of $\overline{H}$ 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 $\bar{1} \in \overline{H}$. 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,

$$N_G(N) = G.$$

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

[1]The 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 $\pi : G \to H$ 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:

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

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

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

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

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

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

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

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 $\varphi : G \to H$ 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 $\varphi : G \to H$ 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 $\varphi : \mathbb{R}^\times \to \{\pm 1\}$ 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 $\pi : \mathbb{R}^2 \to \mathbb{R}$ by $\pi((x, y)) = x + y$. Prove that π is a surjective homomorphism and describe the kernel and fibers of π geometrically.
8. Let $\varphi : \mathbb{R}^\times \to \mathbb{R}^\times$ 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 $\varphi : \mathbb{C}^\times \to \mathbb{R}^\times$ 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 $\varphi : \mathbb{Z}/8\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ 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 $G = \{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in F,\ ac \neq 0\} \leq GL_2(F)$.

(a) Prove that the map $\varphi : \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto a$ 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 $\psi : \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto (a, c)$ is a surjective homomorphism from G onto $F^\times \times F^\times$. Describe the fibers and kernel of ψ.

(c) Let $H = \{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in F\}$. 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 $\varphi : G \to H$ 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.)

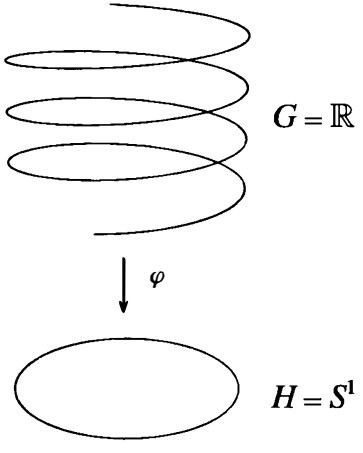


Fig. 5

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 $\overline{G} = \langle \overline{x}, \overline{y} \rangle$. Prove more generally that if $G = \langle S \rangle$ for any subset S of G, then $\overline{G} = \langle \overline{S} \rangle$.

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 $\overline{s}^a\overline{r}^b$, 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 $\overline{s}^a\overline{r}^b$, for some integers a and b as in (b): $\overline{rs}$, $\overline{sr^{-2}s}$, $\overline{s^{-1}r^{-1}sr}$.

(e) Prove that $\overline{H} = \langle \overline{s}, \overline{r}^2 \rangle$ 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 $\overline{\tau}^a\overline{\sigma}^b$, 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 $\overline{\tau}^a\overline{\sigma}^b$, 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 $\overline{u}^a\overline{v}^b$, 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 $\overline{u}^a\overline{v}^b$, 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 $\widetilde{G} = G/\langle \overline{12} \rangle$, where for each integer a we simplify notation by writing $\widetilde{\overline{a}}$ as $\widetilde{a}$.

(a) Show that $\widetilde{G} = \{\widetilde{0}, \widetilde{1}, \ldots, \widetilde{11}\}$.

(b) Find the order of each element of $\widetilde{G}$.

(c) Prove that $\widetilde{G} \cong \mathbb{Z}/12\mathbb{Z}$. (Thus $(\mathbb{Z}/24\mathbb{Z})/(12\mathbb{Z}/24\mathbb{Z}) \cong \mathbb{Z}/12\mathbb{Z}$, 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:

$$G = \langle x, y \mid x^4 = y^4 = 1,\ xy = yx \rangle.$$