

A BOOK OF ABSTRACT ALGEBRA

Second Edition

Charles C. Pinter
Professor of Mathematics
Bucknell University

Dover Publications, Inc., Mineola, New York

Copyright © 1982, 1990 by Charles C. Pinter
All rights reserved.

Bibliographical Note

This Dover edition, first published in 2010, is an unabridged republication of the 1990 second edition of the work originally published in 1982 by the McGraw-Hill Publishing Company, Inc., New York.

Library of Congress Cataloging-in-Publication Data

Pinter, Charles C, 1932–

A book of abstract algebra / Charles C. Pinter. — Dover ed.

p. cm.

Originally published: 2nd ed. New York : McGraw-Hill, 1990.

Includes bibliographical references and index.

ISBN-13: 978-0-486-47417-5

ISBN-10: 0-486-47417-8

1. Algebra, Abstract. I. Title.

QA162.P56 2010

512'.02—dc22

2009026228

Manufactured in the United States by Courier Corporation
47417803

www.doverpublications.com

Preface

- Chapter 1** Why Abstract Algebra?
History of Algebra. New Algebras. Algebraic Structures. Axioms and Axiomatic Algebra. Abstraction in Algebra.
- Chapter 2** Operations
Operations on a Set. Properties of Operations.
- Chapter 3** The Definition of Groups
Groups. Examples of Infinite and Finite Groups. Examples of Abelian and Nonabelian Groups. Group Tables.
Theory of Coding: Maximum-Likelihood Decoding.
- Chapter 4** Elementary Properties of Groups
Uniqueness of Identity and Inverses. Properties of Inverses.
Direct Product of Groups.
- Chapter 5** Subgroups
Definition of Subgroup. Generators and Defining Relations.
Cayley Diagrams. Center of a Group. Group Codes; Hamming Code.
- Chapter 6** Functions
Injective, Surjective, Bijective Function. Composite and Inverse of Functions.
Finite-State Machines. Automata and Their Semigroups.
- Chapter 7** Groups of Permutations
Symmetric Groups. Dihedral Groups.
An Application of Groups to Anthropology.
- Chapter 8** Permutations of a Finite Set
Decomposition of Permutations into Cycles. Transpositions. Even and Odd Permutations. Alternating Groups.
- Chapter 9** Isomorphism
The Concept of Isomorphism in Mathematics. Isomorphic and Nonisomorphic Groups. Cayley's Theorem.

Chapter 10 Order of Group Elements

Powers/Multiples of Group Elements. Laws of Exponents. Properties of the Order of Group Elements.

Chapter 11 Cyclic Groups

Finite and Infinite Cyclic Groups. Isomorphism of Cyclic Groups. Subgroups of Cyclic Groups.

Chapter 12 Partitions and Equivalence Relations

Chapter 13 Counting Cosets

Lagrange's Theorem and Elementary Consequences.

Survey of Groups of Order ≤ 10 .

Number of Conjugate Elements. Group Acting on a Set.

Chapter 14 Homomorphisms

Elementary Properties of Homomorphisms. Normal Subgroups. Kernel and Range.

Inner Direct Products. Conjugate Subgroups.

Chapter 15 Quotient Groups

Quotient Group Construction. Examples and Applications.

The Class Equation. Induction on the Order of a Group.

Chapter 16 The Fundamental Homomorphism Theorem

Fundamental Homomorphism Theorem and Some Consequences.

The Isomorphism Theorems. The Correspondence Theorem. Cauchy's Theorem. Sylow Subgroups. Sylow's Theorem. Decomposition Theorem for Finite Abelian Groups.

Chapter 17 Rings: Definitions and Elementary Properties

Commutative Rings. Unity. Invertibles and Zero-Divisors. Integral Domain. Field.

Chapter 18 Ideals and Homomorphisms

Chapter 19 Quotient Rings

Construction of Quotient Rings. Examples. Fundamental Homomorphism Theorem and Some Consequences. Properties of Prime and Maximal Ideals.

Chapter 20 Integral Domains

Characteristic of an Integral Domain. Properties of the Characteristic. Finite Fields. Construction of the Field of Quotients.

Chapter 21 The Integers

Ordered Integral Domains. Well-ordering. Characterization of $\mathbf{Z}$ Up to Isomorphism. Mathematical Induction. Division Algorithm.

Chapter 22 Factoring into Primes

Ideals of $\mathbb{Z}$. Properties of the GCD. Relatively Prime Integers. Primes. Euclid's Lemma. Unique Factorization.

Chapter 23 Elements of Number Theory (Optional)

Properties of Congruence. Theorems of Fermat and Euler. Solutions of Linear Congruences. Chinese Remainder Theorem.

Wilson's Theorem and Consequences. Quadratic Residues. The Legendre Symbol. Primitive Roots.

Chapter 24 Rings of Polynomials

Motivation and Definitions. Domain of Polynomials over a Field. Division Algorithm.

Polynomials in Several Variables. Fields of Polynomial Quotients.

Chapter 25 Factoring Polynomials

Ideals of $F[x]$. Properties of the GCD. Irreducible Polynomials. Unique factorization.

Euclidean Algorithm.

Chapter 26 Substitution in Polynomials

Roots and Factors. Polynomial Functions. Polynomials over $\mathbb{Q}$. Eisenstein's Irreducibility Criterion. Polynomials over the Reals. Polynomial Interpolation.

Chapter 27 Extensions of Fields

Algebraic and Transcendental Elements. The Minimum Polynomial. Basic Theorem on Field Extensions.

Chapter 28 Vector Spaces

Elementary Properties of Vector Spaces. Linear Independence. Basis. Dimension. Linear Transformations.

Chapter 29 Degrees of Field Extensions

Simple and Iterated Extensions. Degree of an Iterated Extension.

Fields of Algebraic Elements. Algebraic Numbers. Algebraic Closure.

Chapter 30 Ruler and Compass

Constructible Points and Numbers. Impossible Constructions.

Constructible Angles and Polygons.

Chapter 31 Galois Theory: Preamble

Multiple Roots. Root Field. Extension of a Field. Isomorphism.

Roots of Unity. Separable Polynomials. Normal Extensions.

Chapter 32 Galois Theory: The Heart of the Matter

Field Automorphisms. The Galois Group. The Galois Correspondence. Fundamental Theorem of Galois Theory.

Computing Galois Groups.

Chapter 33 Solving Equations by Radicals

Radical Extensions. Abelian Extensions. Solvable Groups. Insolubility of the Quintic.

Appendix A	Review of Set Theory
Appendix B	Review of the Integers
Appendix C	Review of Mathematical Induction
	Answers to Selected Exercises
	Index

* Italic headings indicate topics discussed in the exercise sections.

GROUPS OF PERMUTATIONS

In this chapter we continue our discussion of functions, but we confine our discussions to functions *from a set to itself*. In other words, we consider only functions $f: A \rightarrow A$ whose domain is a set A and whose range is in the same set A .

To begin with, we note that any two functions f and g (from A to A) are *equal* if and only if $f(x) = g(x)$ for every element x in A .

If f and g are functions from A to A , their composite $f \circ g$ is also a function from A to A . We recall that it is the function defined by

$$[f \circ g](x) = f(g(x)) \quad \text{for every } x \text{ in } A \quad (1)$$

It is a very important fact that the *composition of functions is associative*. Thus, if f , g , and h are three functions from A to A , then

$$f \circ (g \circ h) = (f \circ g) \circ h$$

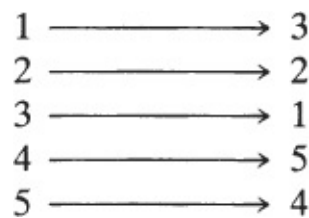
To prove that the functions $f \circ (g \circ h)$ and $(f \circ g) \circ h$ are equal, one must show that for every element x in A ,

$$\{f \circ [g \circ h]\}(x) = \{[f \circ g] \circ h\}(x)$$

We get this by repeated use of [Equation \(1\)](#):

$$\begin{aligned} \{f \circ [g \circ h]\}(x) &= f([g \circ h](x)) = f(g(h(x))) \\ &= [f \circ g](h(x)) = \{[f \circ g] \circ h\}(x) \end{aligned}$$

By a *permutation* of a set A we mean a *bijective function* from A to A , that is, a one-to-one correspondence between A and itself. In elementary algebra we learned to think of a permutation as a *rearrangement* of the elements of a set. Thus, for the set $\{1,2,3,4,5\}$, we may consider the rearrangement which changes $(1,2,3,4,5)$ to $(3,2,1,5,4)$; this rearrangement may be identified with the function



which is obviously a one-to-one correspondence between the set $\{1,2,3,4,5\}$ and itself. It is clear, therefore, that there is no real difference between the new definition of permutation and the old. The new definition, however, is more general in a very useful way since it allows us to speak of permutations of sets A even when A has infinitely many elements.

In [Chapter 6](#) we saw that the composite of any two bijective functions is a bijective function. Thus, *the composite of any two permutations of A is a permutation of A* . It follows that we may regard the operation $\circ$ of composition as *an operation on the set of all the permutations of A* . We have just seen that composition is an associative operation. Is there a neutral element for composition?

For any set A , the *identity function on A* , symbolized by ε_A or simply ε , is the function $x \rightarrow x$ which carries every element of A to itself. That is, it is defined by

$$\varepsilon(x) = x \quad \text{for every element} \quad x \in A$$

It is easy to see that ε is a permutation of A (it is a one-to-one correspondence between A and itself); and if f is any other permutation of A , then

$$f \circ \varepsilon = f \quad \text{and} \quad \varepsilon \circ f = f$$

The first of these equations asserts that $[f \circ \varepsilon](x) = f(x)$ for every element x in A , which is quite obvious, since $[f \circ \varepsilon](x) = f(\varepsilon(x)) = f(x)$. The second equation is proved analogously.

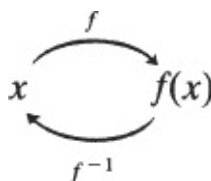
We saw in [Chapter 6](#) that the inverse of any bijective function exists and is a bijective function. Thus, *the inverse of any permutation of A is a permutation of A* . Furthermore, if f is any permutation of A and f^{-1} is its inverse, then

$$f^{-1} \circ f = \varepsilon \quad \text{and} \quad f \circ f^{-1} = \varepsilon$$

The first of these equations asserts that for any element x in A ,

$$[f^{-1} \circ f](x) = \varepsilon(x)$$

that is, $f^{-1}(f(x)) = x$:



This is obviously true, by the definition of the inverse of a function. The second equation is proved analogously.

Let us recapitulate: The operation $\circ$ of composition of functions qualifies as an operation on the set of all the permutations of A . This operation is associative. There is a permutation ε such that $\varepsilon \circ f = f$ and

$f \circ \varepsilon = f$ for any permutation f of A . Finally, for every permutation f of A there is another permutation f^{-1} of A such that $f \circ f^{-1} = \varepsilon$ and $f^{-1} \circ f = \varepsilon$. Thus, *the set of all the permutations of A , with the operation $\circ$ of composition, is a group.*

For any set A , the group of all the permutations of A is called the *symmetric group on A* , and it is represented by the symbol S_A . For any positive integer n , the symmetric group on the set $\{1, 2, 3, \dots, n\}$ is called the *symmetric group on n elements*, and is denoted by S_n .

Let us take a look at S_3 . First, we list all the permutations of the set $\{1, 2, 3\}$:

$$\begin{array}{lll} \varepsilon = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} & \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} & \beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \\ \gamma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} & \delta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} & \kappa = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \end{array}$$

This notation for functions was explained on page 57; for example,

$$\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

is the function such that $\beta(1) = 3$, $\beta(2) = 1$, and $\beta(3) = 2$. A more graphic way of representing the same function would be

$$\beta = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 1 & 2 \end{pmatrix}$$

The operation on elements of S_3 is composition. To find $\alpha \circ \beta$, we note that

$$[\alpha \circ \beta](1) = \alpha(\beta(1)) = \alpha(3) = 2$$

$$[\alpha \circ \beta](2) = \alpha(\beta(2)) = \alpha(1) = 1$$

$$[\alpha \circ \beta](3) = \alpha(\beta(3)) = \alpha(2) = 3$$

Thus

$$\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \gamma$$

Note that in $\alpha \circ \beta$, β is applied first and α next. A graphic way of representing this is

$$\begin{array}{c} \beta = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 1 & 2 \end{pmatrix} \\ \swarrow \quad \searrow \\ \alpha = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 3 & 2 \end{pmatrix} \end{array}$$

The other combinations of elements of S_3 may be computed in the same fashion. The student

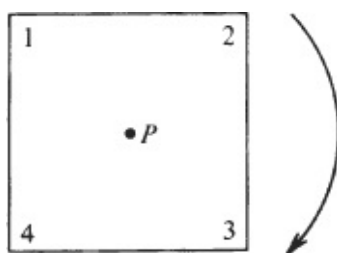
should check the following table, which is the table of the group S_3 :

$\circ$	ε	α	β	γ	δ	κ
ε	ε	α	β	γ	δ	κ
α	α	ε	γ	β	κ	δ
β	β	κ	δ	α	ε	γ
γ	γ	δ	κ	ε	α	β
δ	δ	γ	ε	κ	β	α
κ	κ	β	α	δ	γ	ε

By a *group of permutations* we mean any group S_A or S_n , or any subgroup of one of these groups. Among the most interesting groups of permutations are the groups of symmetries of geometric figures. We will see how such groups arise by considering the *group of symmetries of the square*.

We may think of a symmetry of the square as any way of moving a square to make it coincide with its former position. Every time we do this, vertices will coincide with vertices, so a symmetry is completely described by its effect on the vertices.

Let us number the vertices as in the following diagram:



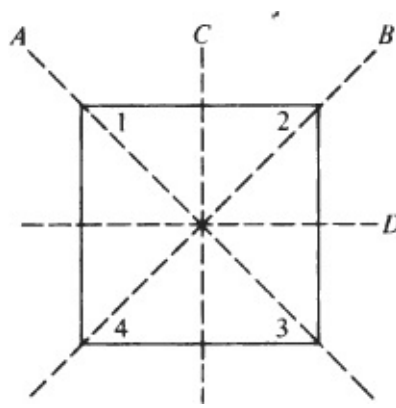
The most obvious symmetries are obtained by rotating the square clockwise about its center P , through angles of 90° , 180° , and 270° , respectively. We indicate each symmetry as a permutation of the vertices; thus a clockwise rotation of 90° yields the symmetry

$$R_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

for this rotation carries vertex 1 to 2, 2 to 3, 3 to 4, and 4 to 1. Rotations of 180° and 270° yield the following symmetries, respectively:

$$R_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \quad \text{and} \quad R_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

The remaining symmetries are flips of the square about its axes A , B , C , and D :



For example, when we flip the square about the axis A , vertices 1 and 3 stay put, but 2 and 4 change places; so we get the symmetry

$$R_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

In the same way, the other flips are

$$R_5 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \quad R_6 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

and

$$R_7 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

One last symmetry is the *identity*

$$R_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

which leaves the square as it was.

The operation on symmetries is composition: $R_i \circ R_j$ is the result of first performing R_j , and then R_i . For example, $R_1 \circ R_4$ is the result of first flipping the square about its axis A , then rotating it clockwise 90° :

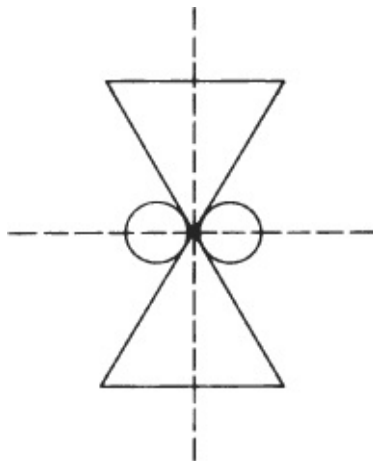
$$\begin{aligned} R_1 \circ R_4 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = R_6 \end{aligned}$$

Thus, the net effect is the same as if the square had been flipped about its axis C .

The eight symmetries of the square form a group under the operation $\circ$ of composition, called the *group of symmetries of the square*.

For every positive integer $n \geq 3$, the regular polygon with n sides has a group of symmetries, symbolized by D_n , which may be found as we did here. These groups are called the *dihedral groups*. For example, the group of the square is D_4 , the group of the pentagon is D_5 , and so on.

Every plane figure which exhibits regularities has a group of symmetries. For example, the following figure, has a group of symmetries consisting of two rotations (180° and 360°) and two flips about the indicated axes. Artificial as well as natural objects often have a surprising number of symmetries.



Far more complicated than the plane symmetries are the symmetries of objects in space. Modern-day crystallography and crystal physics, for example, rely very heavily on knowledge about groups of symmetries of three-dimensional shapes.

Groups of symmetry are widely employed also in the theory of electron structure and of molecular vibrations. In elementary particle physics, such groups have been used to predict the existence of certain elementary particles before they were found experimentally!

Symmetries and their groups arise everywhere in nature: in quantum physics, flower petals, cell division, the work habits of bees in the hive, snowflakes, music, and Romanesque cathedrals.

EXERCISES

A. Computing Elements of S_6

1 Consider the following permutations f , g , and h in S_6 :

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 3 & 5 & 4 & 2 \end{pmatrix} \quad g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 6 & 5 & 4 \end{pmatrix}$$

$$h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 6 & 4 & 5 & 2 \end{pmatrix}$$

Compute the following:

$$f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ & & & & & \end{pmatrix} \quad g^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ & & & & & \end{pmatrix}$$

$$h^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ & & & & & \end{pmatrix}$$

$$f \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ & & & & & \end{pmatrix} \quad g \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ & & & & & \end{pmatrix}$$

2 $f \circ (g \circ h) =$

- 3 $g \circ h^{-1} =$
 4 $h \circ g^{-1} \circ f^{-1} =$
 5 $g \circ g \circ g =$

B. Examples of Groups of Permutations

1 Let G be the subset of S_4 consisting of the permutations

$$\begin{aligned} \varepsilon &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} & f &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \\ g &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} & h &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \end{aligned}$$

Show that G is a group of permutations, and write its table:

$\circ$	ε	f	g	h
ε				
f				
g				
h				

2 List the elements of the cyclic subgroup of S_6 generated by

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 1 & 6 & 5 \end{pmatrix}$$

3 Find a four-element abelian subgroup of S_5 . Write its table.

4 The subgroup of S_5 generated by

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix} \quad g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 5 & 3 \end{pmatrix}$$

has six elements. List them, then write the table of this group:

$\varepsilon = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$	$\circ$	ε	f	g	h	k	l
$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$							
$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 5 & 3 \end{pmatrix}$							
$h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$							
$k = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$							
$l = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$							

C. Groups of Permutations of $\mathbb{R}$

In each of the following, A is a subset of $\mathbb{R}$ and G is a set of permutations of A . Show that G is a subgroup of S_A , and write the table of G .

- 1 A is the set of all $x \in \mathbb{R}$ such that $x \neq 0, 1$. $G = \{\varepsilon, f, g\}$, where $f(x) = 1/(1-x)$ and $g(x) = (x-1)/x$.
- 2 A is the set of all the nonzero real numbers. $G = \{\varepsilon, f, g, h\}$, where $f(x) = 1/x$, $g(x) = -x$, and $h(x) = -1/x$.
- 3 A is the set of all the real numbers $x \neq 0, 1$. $G = \{\varepsilon, f, g, h, k\}$, where $f(x) = 1-x$, $g(x) = 1/x$, $h(x) = 1/(1-x)$, $j(x) = (x-1)/x$, and $k(x) = x/(x-1)$.
- 4 A is the set of all the real numbers $x \neq 0, 1, 2$. G is the subgroup of S_A generated by $f(x) = 2-x$ and $g(x) = 2/x$. (G has eight elements. List them, and write the table of G .)

† D. A Cyclic Group of Permutations

For each integer n , define f_n by $f_n(x) = x + n$.

- 1 Prove: For each integer n , f_n is a permutation of $\mathbb{R}$, that is, $f_n \in S_{\mathbb{R}}$.
- 2 Prove that $f_n \circ f_m = f_{n+m}$ and $f_n^{-1} = f_{-n}$.
- 3 Let $G = \{f_n : n \in \mathbb{Z}\}$. Prove that G is a subgroup of $S_{\mathbb{R}}$.
- 4 Prove that G is cyclic. (Indicate a generator of G .)

† E. A Subgroup of $S_{\mathbb{R}}$

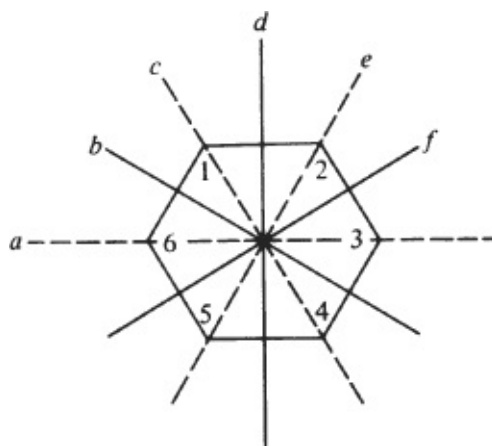
For any pair of real numbers $a \neq 0$ and b , define a function $f_{a,b}$ as follows:

$$f_{a,b}(x) = ax + b$$

- 1 Prove that $f_{a,b}$ is a permutation of $\mathbb{R}$, that is, $f_{a,b} \in S_{\mathbb{R}}$.
- 2 Prove that $f_{a,b} \circ f_{c,d} = f_{ac, ad+b}$.
- 3 Prove that $f_{a,b}^{-1} = f_{1/a, -b/a}$.
- 4 Let $G = \{f_{a,b} : a \in \mathbb{R}, b \in \mathbb{R}, a \neq 0\}$. Show that G is a subgroup of $S_{\mathbb{R}}$.

F. Symmetries of Geometric Figures

- 1 Let G be the group of symmetries of the regular hexagon. List the elements of G (there are 12 of them), then write the table of G .



$$R_0 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} \quad R_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix}$$

$$R_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix} \quad R_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix}$$

etc. . . .

2 Let G be the group of symmetries of the rectangle. List the elements of G (there are four of them), and write the table of G .

3 List the symmetries of the letter **Z** and give the table of this group of symmetries. Do the same for the letters **V** and **H**.

4 List the symmetries of the following shape, and give the table of their group.



(Assume that the three arms are of equal length, and the three central angles are equal.)

G. Symmetries of Polynomials

Consider the polynomial $p = (x_1 - x_2)^2 + (x_3 - x_4)^2$. It is unaltered when the subscripts undergo any of the following permutations:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

For example, the first of these permutations replaces p by

$$(x_2 - x_1)^2 + (x_3 - x_4)^2$$

the second permutation replaces p by $(x_1 - x_2)^2 + (x_4 - x_3)^2$; and so on. The *symmetries of a polynomial* ρ are all the permutations of the subscripts which leave ρ unchanged. They form a group of permutations.

List the symmetries of each of the following polynomials, and write their group table.

- 1 $p = x_1x_2 + x_2x_3$
- 2 $p = (x_1 - x_2)(x_2 - x_3)(x_1 - x_3)$
- 3 $p = x_1x_2 + x_2x_3 + x_1x_3$
- 4 $p = (x_1 - x_2)(x_3 - x_4)$

H. Properties of Permutations of a Set A

- 1 Let A be a set and $a \in A$. Let G be the subset of S_A consisting of all the permutations f of A such that $f(a) = a$. Prove that G is a subgroup of S_A .
- # 2 If f is a permutation of A and $a \in A$, we say that f moves a if $f(a) \neq a$. Let A be an infinite set, and let G be the subset of S_A which consists of all the permutations f of A which move *only a finite number of elements* of A . Prove that G is a subgroup of S_A .
- 3 Let A be a finite set, and B a subset of A . Let G be the subset of S_A consisting of all the permutations f of A such that $f(x) \in B$ for every $x \in B$. Prove that G is a subgroup of S_A .
- 4 Give an example to show that the conclusion of part 3 is not necessarily true if A is an infinite set.

I. Algebra of Kinship Structures (Anthropology)

Anthropologists have used groups of permutations to describe kinship systems in primitive societies. The algebraic model for kinship structures described here is adapted from *An Anatomy of Kinship* by H. C. White. The model is based on the following assumptions, which are widely supported by anthropological research:

- (i) The entire population of the society is divided into *clans*. Every person belongs to one, and only one, clan. Let us call the clans $k_1, k_2, \dots, k_n$.
- (ii) In every clan k_i , all the men must choose their wives from among the women of a specified clan k_j . We symbolize this by writing $w(k_i) = k_j$.
- (iii) Men from two different clans cannot marry women from the same clan. That is, if $k_i \neq k_j$, then $w(k_i) \neq w(k_j)$.
- (iv) All the children of a couple are assigned to some fixed clan. So if a man belongs to clan k_i , all his children belong to a clan which we symbolize by $c(k_i)$.
- (v) Children whose fathers belong to different clans must themselves be in different clans. That is, if $k_i \neq k_j$, then $c(k_i) \neq c(k_j)$.
- (vi) A man cannot marry a woman of his own clan. That is, $w(k_i) \neq k_i$.

Now let $K = \{k_1, k_2, \dots, k_n\}$ be the set of all the distinct clans. By (ii), w is a function from K to K , and by (iv), c is a function from K to K . By (iii), w is an injective function; hence (see [Exercise F2 of Chapter 6](#)) w is a permutation of K . Likewise, by (v), c is a permutation of K .

Let G be the group of permutations generated by c and w ; that is, G consists of c, w, c^{-1}, w^{-1} , and all possible composites which can be formed from these—for example, $c \circ w \circ w \circ c^{-1} \circ w^{-1}$. Clearly the identity function ε is in G since, for example, $\varepsilon = c \circ c^{-1}$. Here are two final assumptions:

- (vii) Every person, in any clan, has a relation in every other clan. This means that for any k_i and k_j in K , there is a permutation α in G such that $\alpha(k_i) = k_j$.

(viii) Rules of kinship apply uniformly to all clans. Thus, for any α and β in G , if $\alpha(k_j) = \beta(k_j)$ for some specific clan k_j , it necessarily follows that $\alpha(k_i) = \beta(k_i)$ for every clan k_i

Prove parts 1–3:

1 Let $\alpha \in G$. If $\alpha(k_i) = k_i$ for any given k_i , then $\alpha = \varepsilon$.

2 Let $\alpha \in G$. There is a positive integer $m \leq n$ such that $\alpha^m = \varepsilon$.

[$\alpha^m = \alpha \circ \alpha \circ \cdots \circ \alpha$ (m factors of α). HINT: Consider $\alpha(k_1)$, $\alpha^2(k_1)$, etc.]

3 The group G consists of exactly n permutations.

Explain parts 4–9.

4 If a person belongs to clan k_i , that person's father belongs to clan $c^{-1}(k_i)$. If a woman belongs to clan k_j , her husband belongs to clan $w^{-1}(k_j)$.

5 If any man is in the same clan as his son, then $c = \varepsilon$. If any woman is in the same clan as her son, then $c = w$.

6 If a person belongs to clan k_i , the son of his mother's sister belongs to clan $c \circ w^{-1} \circ w \circ c^{-1}(k_i)$. Conclude that marriage between matrilineal parallel cousins (marriage between a woman and the son of her mother's sister) is prohibited.

7 Marriage between a man and the daughter of his father's sister is prohibited.

8 If matrilineal cross-cousins may marry (that is, a woman may marry the son of her mother's brother), then $c \circ w = w^{-1} \circ c$.

9 If patrilineal cross-cousins may marry (a woman may marry the son of her father's sister), then c and w^{-1} commute.

PERMUTATIONS OF A FINITE SET

Permutations of finite sets are used in every branch of mathematics—for example, in geometry, in statistics, in elementary algebra—and they have a myriad of applications in science and technology. Because of their practical importance, this chapter will be devoted to the study of a few special properties of permutations of finite sets.

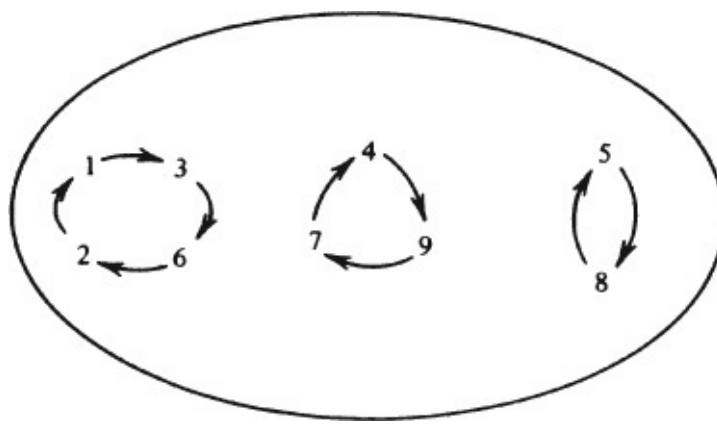
If n is a positive integer, consider a set of n elements. It makes no difference which specific set we consider, just as long as it has n elements; so let us take the set $\{1, 2, \dots, n\}$. We have already seen that the group of all the permutations of this set is called the *symmetric group on n elements* and is denoted by S_n . In the remainder of this chapter, when we say “permutation” we will invariably mean a permutation of the set $\{1, 2, \dots, n\}$ for an arbitrary positive integer n .

One of the most characteristic activities of science (*any* kind of science) is to try to separate complex things into their simplest component parts. This intellectual “divide and conquer” helps us to understand complicated processes and solve difficult problems. The savvy mathematician never misses the chance of doing this whenever the opportunity presents itself. We will see now that every permutation can be decomposed into simple parts called “cycles,” and these cycles are, in a sense, the most basic kind of permutations.

We begin with an example: take, for instance, the permutation

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 1 & 6 & 9 & 8 & 2 & 4 & 5 & 7 \end{pmatrix}$$

and look at how f moves the elements in its domain:



Notice how f decomposes its domain into three separate subsets, so that, in each subset, the elements are permuted cyclically so as to form a closed chain. These closed chains may be considered to be the component parts of the permutation; they are called “cycles.” (This word will be carefully defined in a moment.) Every permutation breaks down, just as this one did, into separate cycles.

Let $a_1, a_2, \dots, a_s$ be distinct elements of the set $\{1, 2, \dots, n\}$. By the *cycle* $(a_1 a_2 \dots a_s)$ we mean the permutation

$$\underbrace{a_1 \rightarrow a_2 \rightarrow a_3 \rightarrow \dots \rightarrow a_{s-1} \rightarrow a_s}_{\text{cycle}}$$

of $\{1, 2, \dots, n\}$ which carries a_1 to a_2 , a_2 to a_3 , ..., a_{s-1} to a_s , and a_s to a_1 , while leaving all the remaining elements of $\{1, 2, \dots, n\}$ fixed.

For instance, in S_6 , the cycle (1426) is the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 3 & 2 & 5 & 1 \end{pmatrix}$$

In S_5 , the cycle (254) is the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 2 & 4 \end{pmatrix}$$

Because cycles are permutations, we may form the *composite* of two cycles in the usual manner. The composite of cycles is generally called their *product* and it is customary to omit the symbol $\circ$. For example, in S_5 ,

$$\begin{aligned} (245)(124) &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 5 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 1 & 2 \end{pmatrix} \end{aligned}$$

Actually, it is very easy to compute the product of two cycles by reasoning in the following manner: Let us continue with the same example,

$$\underbrace{(2 \quad 4 \quad 5)}_{\alpha} \underbrace{(1 \quad 2 \quad 4)}_{\beta}$$

Remember that the permutation on the right is applied first, and the permutation on the left is applied

next. Now,

β carries 1 to 2, and α carries 2 to 4; hence $\alpha\beta$ carries 1 to 4.

β carries 2 to 4, and α carries 4 to 5; hence $\alpha\beta$ carries 2 to 5.

β leaves 3 fixed and so does α ; hence $\alpha\beta$ leaves 3 fixed.

β carries 4 to 1 and α leaves 1 fixed, so $\alpha\beta$ carries 4 to 1.

β leaves 5 fixed and α carries 5 to 2; hence $\alpha\beta$ carries 5 to 2.

If $(a_1 a_2 \dots a_s)$ is a cycle, the integer s is called its *length*; thus, $(a_1 a_2 \dots a_s)$ is a *cycle of length s* . For example, (1532) is a cycle of length 4.

If two cycles have no elements in common they are said to be *disjoint*. For example, (132) and (465) are disjoint cycles, but (132) and (453) are not disjoint. *Disjoint cycles commute*: that is, if $(a_1 \dots a_r)$ and $(b_1 \dots b_s)$ are disjoint, then

$$\underbrace{(a_1 \dots a_r)}_{\alpha} \underbrace{(b_1 \dots b_s)}_{\beta} = \underbrace{(b_1 \dots b_s)}_{\beta} \underbrace{(a_1 \dots a_r)}_{\alpha}$$

It is easy to see why this is true: α moves the a 's but not the b 's, while β moves the b 's but not the a 's. Thus, if β carries b_i to b_j , then $\alpha\beta$ does the same, and so does $\beta\alpha$. Similarly, if α carries a_h to a_k then $\beta\alpha$ does the same, and so does $\alpha\beta$.

We are now ready to prove what was asserted at the beginning of this chapter: Every permutation can be decomposed into cycles—in fact, into *disjoint* cycles. More precisely, we can state the following:

Theorem 1 *Every permutation is either the identity, a single cycle, or a product of disjoint cycles.*

We begin with an example, because the proof uses the same technique as the example. Consider the permutation

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 2 & 1 & 6 \end{pmatrix}$$

and let us write f as a product of disjoint cycles. We begin with 1 and note that

$$1 \xrightarrow{f} 3 \xrightarrow{f} 5 \xrightarrow{f} 1$$

We have come a complete circle and found our first cycle, which is (135) . Next, we take the first number which hasn't yet been used, namely, 2. We see that

$$2 \xrightarrow{f} 4 \xrightarrow{f} 2$$

Again we have come a complete circle and found another cycle, which is (24) . The only remaining number is 6, which leaves fixed. We are done:

$$f = (135)(24)$$

The proof for *any* permutation f follows the same pattern as the example. Let a_1 be the first number in $\{1, \dots, n\}$ such that $f(a_1) \neq a_1$. Let $a_2 = f(a_1)$, $a_3 = f(a_2)$, and so on in succession until we come to our first repetition, that is, until $f(a_k)$ is equal to one of the numbers $a_1, a_2, \dots, a_{k-1}$. Say $f(a_k) = a_i$. If a_i is not

a_1 , we have

$$a_1 \rightarrow a_2 \rightarrow \cdots \rightarrow a_{i-1} \rightarrow \underbrace{a_i \cdots a_k}_{\text{cycle}}$$

so a_i is the image of two elements, a_k and a_{i-1} , which is impossible because f is bijective. Thus, $a_i = a_1$, and therefore $f(a_k) = a_1$. We have come a complete circle and found our first cycle, namely, $(a_1 a_2 \cdots a_k)$.

Next, let b_1 be the first number which has not yet been examined and such that $f(b_1) \neq b_1$. We let $b_2 = f(b_1)$, $b_3 = f(b_2)$, and proceed as before to obtain the next cycle, say $(b_1 \cdots b_t)$. Obviously $(b_1 \cdots b_t)$ is disjoint from $(a_1 \cdots a_k)$. We continue this process until all the numbers in $\{1, \dots, n\}$ have been exhausted. This concludes the proof.

Incidentally, it is easy to see that this product of cycles is unique, except for the order of the factors.

Now our curiosity may prod us to ask: once a permutation has been written as a product of disjoint cycles, *has it been simplified as much as possible?* Or is there some way of simplifying it further?

A cycle of length 2 is called a *transposition*. In other words, a transposition is a cycle (a_i, a_j) which interchanges the two numbers a_i and a_j . It is a fact both remarkable and trivial that every cycle can be expressed as a product of one or more transpositions. In fact,

$$(a_1 a_2 \cdots a_r) = (a_r a_{r-1})(a_r a_{r-2}) \cdots (a_r a_3)(a_r a_2 a_r a_1)$$

which may be verified by direct computation. For example,

$$(12345) = (54)(53)(52)(51)$$

However, there is more than one way to write a given permutation as a product of transpositions. For example, (12345) may also be expressed as a product of transpositions in the following ways:

$$(12345) = (15)(14)(13)(12)$$

$$(12345) = (54)(52)(51)(14)(32)(41)$$

as well as in many other ways.

Thus, every permutation, after it has been decomposed into disjoint cycles, may be broken down further and expressed as a product of transpositions. However, the expression as a product of transpositions is not unique, and even the *number of transpositions* involved is not unique.

Nevertheless, when a permutation π is written as a product of transpositions, *one* property of this expression is unique: the number of transpositions involved is either *always even* or *always odd*. (This fact will be proved in a moment.) For example, we have just seen that (12345) can be written as a product of four transpositions and also as a product of six transpositions; it can be written in many other ways, but always as a product of an *even* number of transpositions. Likewise, (1234) can be decomposed in many ways into transpositions, but always an *odd* number of transpositions.

A permutation is called *even* if it is a product of an even number of transpositions, and *odd* if it is a product of an odd number of transpositions. What we are asserting, therefore, is that every permutation is unambiguously either odd or even.

This may seem like a pretty useless fact—but actually the very opposite is true. A number of great

theorems of mathematics depend for their proof (at that crucial step when the razor of logic makes its decisive cut) on none other but the distinction between even and odd permutations.

We begin by showing that the identity permutation, ε , is an even permutation.

Theorem 2 *No matter how ε is written as a product of transpositions, the number of transpositions is even.*

PROOF: Let $t_1, t_2, \dots, t_m$ be m transpositions, and suppose that

$$\varepsilon = t_1 t_2 \dots t_m \quad (1)$$

We aim to prove that ε can be rewritten as a product of $m - 2$ transpositions. We will then be done: for if ε were equal to a product of an odd number of transpositions, and we were able to rewrite this product repeatedly, each time with two fewer transpositions, then eventually we would get ε equal to a single transposition (ab) , and this is impossible.

Let x be any numeral appearing in one of the transpositions $t_2, \dots, t_m$. Let $t_k = (xa)$, and suppose t_k is the last transposition in Equation (1) (reading from left to right) in which x appears:

$$\varepsilon = t_1 t_2 \dots t_{k-1} \underbrace{t_k}_{=(xa)} \underbrace{t_{k+1} \dots t_m}_{\substack{x \text{ does not} \\ \text{appear here}}}$$

Now, t_{k-1} is a transposition which is either equal to (xa) , or else one or both of its components are different from x and a . This gives four possibilities, which we now treat as four separate cases.

Case I $t_{k-1} = (xa)$.

Then $t_{k-1} t_k = (xa)(xa)$, which is equal to the identity permutation. Thus, $t_{k-1} t_k$ may be removed without changing Equation (1). As a result, ε is a product of $m - 2$ transpositions, as required.

Case II $t_{k-1} = (xb)$ where $b \neq x, a$.

Then $t_{k-1} t_k = (xb)(xa)$

But $(xb)(xa) = (xa)(ab)$

We replace $t_{k-1} t_k$ by $(xa)(ab)$ in Equation (1). As a result, the last occurrence of x is one position further left than it was at the start.

Case III $t_{k-1} = (ca)$, where $c \neq x, a$.

Then $t_{k-1} t_k = (ca)(xa)$

But $(ca)(xa) = (xc)(ca)$

We replace $t_{k-1} t_k$ by $(xa)(bc)$ in Equation (1), as in Case II.

Case IV $t_{k-1} = (bc)$, where $b \neq x, a$ and $c \neq x, a$

Then $t_{k-1} t_k = (bc)(xa)$

But $(bc)(xa) = (xa)(bc)$

We replace $t_{k-1} t_k$ by $(xa)(bc)$ in Equation (1), as in Cases II and III.

In Case I, we are done. In Cases II, III, and IV, we repeat the argument one or more times. Each time, the last appearance of x is one position further left than the time before. This must eventually lead

to Case I. For otherwise, we end up with the last (hence the only) appearance of x being in t_1 . This cannot be: for if $t_1 = (xa)$ and x does not appear in $t_2, \dots, t_m$, then $\varepsilon(x) = a$, which is impossible! ■

(The box ■ is used to mark the ending of a proof.)

Our conclusion is contained in the next theorem.

Theorem 3 *If $\pi \in S_n$, then π cannot be both an odd permutation and an even permutation.*

Suppose π can be written as the product of an even number of transpositions, and differently as the product of an odd number of transpositions. Then the same would be true for π^{-1} . But $\varepsilon = \pi \circ \pi^{-1}$: thus, writing π^{-1} as a product of an even number of transpositions and π as a product of an odd number of transpositions, we get an expression for ε as a product of an odd number of transpositions. This is impossible by [Theorem 2](#).

The set of all the even permutations in S_n is a subgroup of S_n . It is denoted by A_n , and is called the *alternating group* on the set $\{1, 2, \dots, n\}$.

EXERCISES

A. Practice in Multiplying and Factoring Permutations

1 Compute each of the following products in S_9 . (Write your answer as a single permutation.)

(a) $(145)(37)(682)$

(b) $(17)(628)(9354)$

(c) $(71825)(36)(49)$

(d) $(12)(347)$

(e) $(147)(1678)(74132)$

(f) $(6148)(2345)(12493)$

2 Write each of the following permutations in s_9 as a product of disjoint cycles:

(a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 9 & 2 & 5 & 1 & 7 & 6 & 8 & 3 \end{pmatrix}$

(b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 4 & 9 & 2 & 3 & 8 & 1 & 6 & 5 \end{pmatrix}$

(c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 9 & 5 & 3 & 1 & 2 & 4 & 8 & 6 \end{pmatrix}$

(d) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 8 & 7 & 4 & 3 & 6 & 5 & 1 & 2 \end{pmatrix}$

3 Express each of the following as a product of transpositions in S_8 :

(a) (137428)

(b) $(416)(8235)$

(c) $(123)(456)(1574)$

(d) $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 4 & 2 & 8 & 7 & 6 & 5 \end{pmatrix}$

4 If $\alpha = (3714)$, $\beta = (123)$, and $\gamma = (24135)$ in s_7 , express each of the following as a product of disjoint cycles:

(a) $\alpha^{-1} \beta$

(b) $\gamma^{-1} \alpha$

(c) $\alpha^2 \beta$

- (d) $\beta^2\alpha\gamma$
- (e) γ^4
- # (f) $\gamma^3\alpha^{-1}$
- (g) $\beta^{-1}\gamma$
- (h) $\alpha^{-1}\gamma^2\alpha$

(NOTE: $\alpha^2 = \alpha \circ \alpha$, $\gamma^3 = \gamma \circ \gamma \circ \gamma$, etc.)

5 In S_5 , write (12345) in five different ways as a cycle, and in five different ways as a product of transpositions.

6 In S_5 , express each of the following as the square of a cycle (that is, express as α^2 where α is a cycle):

- (a) (132)
- (b) (12345)
- (c) (13)(24)

B. Powers of

If π is any permutation, we write $\pi \circ \pi = \pi^2$, $\pi \circ \pi \circ \pi = \pi^3$, etc. The convenience of this notation is evident.

1 Compute α^{-1} , α^2 , α^3 , α^4 , α^5 where

- (a) $\alpha = (123)$
- (b) $\alpha = (1234)$
- (c) $\alpha = (123456)$.

In the following problems, let α be a cycle of length s , say $\alpha = (\alpha_1\alpha_2 \dots \alpha_s)$.

2 Describe all the *distinct* powers of α . How many are there? Note carefully the connection with addition of integers modulo s (page 27).

3 Find the inverse of α , and show that $\alpha^{-1} = \alpha^s$

Prove each of the following:

4 α^2 is a cycle iff s is odd.

5 If s is odd, α is the square of some cycle of length α . (Find it. HINT: Show $\alpha = \alpha^{s+1}$.)

6 If s is even, say $s = 2t$, then α^2 is the product of two cycles of length t . (Find them.)

7 If s is a multiple of k , say $s = kt$, then α^k is the product of k cycles of length t .

8 If s is a prime number, every power of α is a cycle.

C. Even and Odd Permutations

1 Determine which of the following permutations is even, and which is odd.

- (a) $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 4 & 1 & 5 & 6 & 2 & 3 & 8 \end{pmatrix}$
- (b) (71864)
- (c) (12)(76)(345)
- (d) (1276)(3241)(7812)
- (e) (123)(2345)(1357)

Prove each of the following:

- 2** (a) The product of two even permutations is even.
 (b) The product of two odd permutations is even.
 (c) The product of an even permutation and an odd permutation is odd.
- 3** (a) A cycle of length l is even if l is odd.
 (b) A cycle of length l is odd if l is even.
- 4** (a) If α and β are cycles of length l and m , respectively, then $\alpha\beta$ is even or odd depending on whether $l + m - 2$ is even or odd.
 (b) If $\pi = \beta_1 \dots \beta_r$ where each β_i is a cycle of length l_i , then π is even or odd depending on whether $l_1 + l_2 + \dots + l_r - r$ is even or odd.

D. Disjoint Cycles

In each of the following, let α and β be disjoint cycles, say

$$\alpha = (a_1 a_2 \dots a_s) \quad \text{and} \quad \beta = (b_1 b_2 \dots b_r)$$

Prove parts 1–3:

- 1** For every positive integer n , $(\alpha\beta)^n = \alpha^n \beta^n$.
2 If $\alpha\beta = \varepsilon$, then $\alpha = \varepsilon$ and $\beta = \varepsilon$.
3 If $(\alpha\beta)^t = \varepsilon$, then $\alpha^t = \varepsilon$ and $\beta^t = \varepsilon$ (where t is any positive integer). (Use part 2 in your proof.)
4 Find a transposition γ such that $\alpha\beta\gamma$ is a cycle.
5 Let γ be the same transposition as in the preceding exercise. Show that $\alpha\gamma\beta$ and $\gamma\alpha\beta$ are cycles.
6 Let α and β be cycles of odd length (not disjoint). Prove that if $\alpha^2 = \beta^2$, then $\alpha = \beta$.

† E. Conjugate Cycles

Prove each of the following in S_n :

- 1** Let $\alpha = (a_1, \dots, a_s)$ be a cycle and let π be a permutation in S_n . Then $\pi\alpha\pi^{-1}$ is the cycle $(\pi(a_1), \dots, \pi(a_s))$.

If α is any cycle and π any permutation, $\pi\alpha\pi^{-1}$ is called a *conjugate* of α . In the following parts, let π denote any permutation in S_n .

2 Conclude from part 1: Any two cycles of the same length are conjugates of each other.

- 3** If α and β are disjoint cycles, then $\pi\alpha\pi^{-1}$ and $\pi\beta\pi^{-1}$ are disjoint cycles.
4 Let σ be a product $\alpha_1 \dots \alpha_t$ of t disjoint cycles of lengths $l_1, \dots, l_t$, respectively. Then $\pi\sigma\pi^{-1}$ is also a product of t disjoint cycles of lengths $l_1, \dots, l_t$.
5 Let α_1 and α_2 be cycles of the same length. Let β_1 and β_2 be cycles of the same length. Let α_1 and β_1 be disjoint, and let α_2 and β_2 be disjoint. There is a permutation $\pi \in S_n$ such that $\alpha_1\beta_1 = \pi\alpha_2\beta_2\pi^{-1}$.

† F. Order of Cycles

- 1** Prove in S_n : If $\alpha = (a_1 \dots a_s)$ is a cycle of length s , then $\alpha^s = \varepsilon$, $\alpha^{2s} = \varepsilon$, and $\alpha^{3s} = \varepsilon$. Is $\alpha^k = \varepsilon$ for any positive integer $k < s$? (Explain.)

If α is any permutation, the least positive integer n such that $\alpha^n = \varepsilon$ is called the *order* of α .

2 Prove in S_n : If $\alpha = (\alpha_1 \dots \alpha_s)$ is any cycle of length s , the order of α is s .

3 Find the order of each of the following permutations:

(a) $(12)(345)$

(b) $(12)(3456)$

(c) $(1234)(56789)$

4 What is the order of $\alpha\beta$, if α and β are disjoint cycles of lengths 4 and 6, respectively? (Explain why. Use the fact that disjoint cycles commute.)

5 What is the order of $\alpha\beta$ if α and β are disjoint cycles of lengths r and s , respectively? (Venture a guess, explain, but do not attempt a rigorous proof.)

† G. Even/Odd Permutations in Subgroups of S_n

Prove each of the following in S_n :

1 Let $\alpha_1, \dots, \alpha_r$ be distinct even permutations, and β an odd permutation. Then $\alpha_1\beta, \dots, \alpha_r\beta$ are r *distinct* odd permutations. (See [Exercise C2](#).)

2 If $\beta_1, \dots, \beta_r$ are distinct odd permutations, then $\beta_1\beta_1, \beta_1\beta_2, \dots, \beta_1\beta_r$ are r *distinct* even permutations.

3 In S_n , there are the same number of odd permutations as even permutations. (HINT: Use part 1 to prove that the number of even permutations $\leq$ is the number of odd permutations. Use part 2 to prove the reverse of that inequality.)

4 The set of all the even permutations is a subgroup of S_n . (It is denoted by A_n and is called the *alternating group* on n symbols.)

5 Let H be any subgroup of S_n . H either contains only even permutations, or H contains the same number of odd as even permutations. (Use parts 1 and 2.)

† H. Generators of A_n and S_n

Remember that in any group G , a set S of elements of G is said to *generate* G if every element of G can be expressed as a product of elements in S and inverses of elements in S . (See page 47.)

1 Prove that the set T of all the transpositions in S_n generates S_n .

2 Prove that the set $T_1 = \{(12), (13), \dots, (1n)\}$ generates S_n .

3 Prove that every even permutation is a product of one or more cycles of length 3. [HINT: $(13)(12) = (123)$; $(12)(34) = (321)(134)$.] Conclude that the set U of all cycles of length 3 generates A_n .

4 Prove that the set $U_1 = \{(123), (124), \dots, (12n)\}$ generates A_n . [HINT: $(abc) = (1ca)(1ab)$, $(1ab) = (1b2)(12a)(12b)$, and $(1b2) = (12b)^2$.]

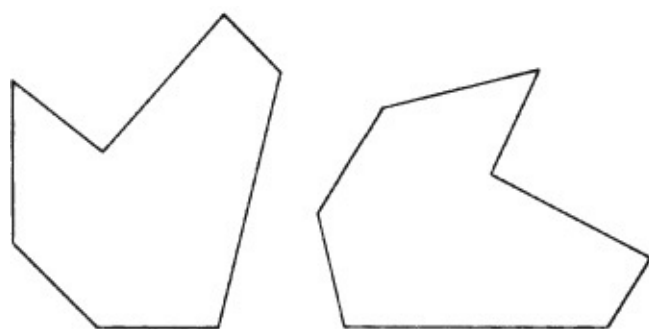
5 The pair of cycles (12) and $(12 \dots n)$ generates S_n . [HINT: $(1 \dots n)(12)(1 \dots n)^{-1} = (23)$; $(12)(23)(12) = (13)$.]

ISOMORPHISM

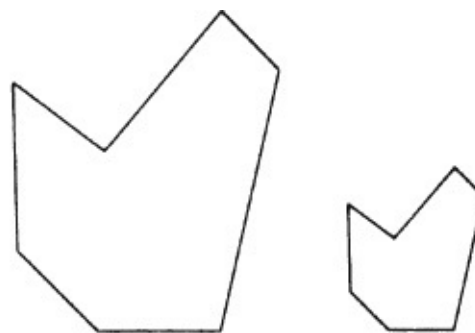
Human perception, as well as the “perception” of so-called intelligent machines, is based on the ability to recognize the same structure in different guises. It is the faculty for discerning, in *different* objects, the same relationships between their parts.

The dictionary tells us that two things are “isomorphic” if they *have the same structure*. The notion of isomorphism—of having the same structure—is central to every branch of mathematics and permeates all of abstract reasoning. It is an expression of the simple fact that objects may be different in substance but identical in form.

In geometry there are several kinds of isomorphism, the simplest being congruence and similarity. Two geometric figures are congruent if there exists a plane motion which makes one figure coincide with the other; they are similar if there exists a transformation of the plane, magnifying or shrinking lengths in a fixed ratio, which (again) makes one figure coincide with the other.



These two figures are congruent



These two figures are similar

We do not even need to venture into mathematics to meet some simple examples of isomorphism. For instance, the two palindromes

M A D A M
A
M A D

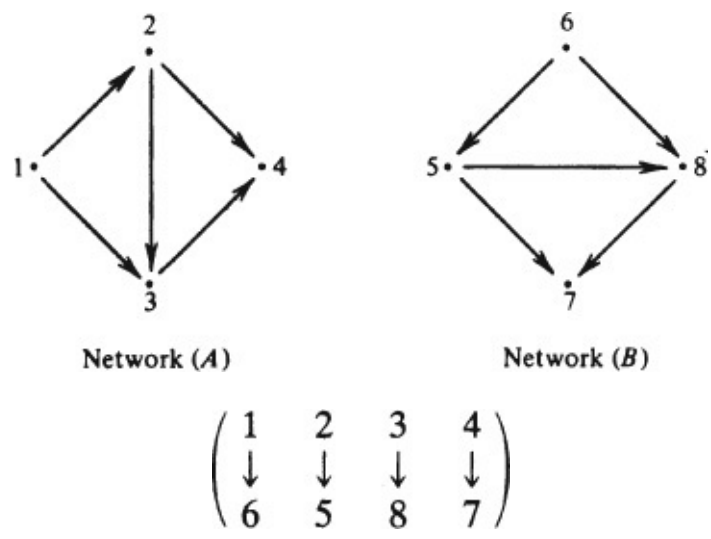
and

R O T O R
O
R O T

are different, but obviously isomorphic; indeed, the first one coincides with the second if we replace M

by R, A by O, and D by T.

Here is an example from applied mathematics: A flow network is a set of points, with arrows joining some of the points. Such networks are used to represent flows of cash or goods, channels of communication, electric circuits, and so on. The flow networks (A) and (B), below, are different, but can be shown to be isomorphic. Indeed, (A) can be made to coincide with (B) if we superimpose point 1 on point 6, point 2 on point 5, point 3 on point 8, and point 4 on point 7. (A) and (B) then coincide in the sense of having the same points joined by arrows in the same direction. Thus, *network (A) is transformed into network (B)* if we replace points 1 by 6, 2 by 5, 3 by 8, and 4 by 7. The one-to-one correspondence which carries out this transformation, namely,



is called an *isomorphism* from network (A) to network (B), for it transforms (A) into (B).

Incidentally, the one-to-one correspondence

$$\left(\begin{array}{ccc} \mathbf{M} & \mathbf{A} & \mathbf{D} \\ \downarrow & \downarrow & \downarrow \\ \mathbf{R} & \mathbf{O} & \mathbf{T} \end{array} \right)$$

is an *isomorphism* between the two palindromes of the preceding example, for it transforms the first palindrome into the second.

Our next and final example is from algebra. Consider the two groups G_1 and G_2 described below:

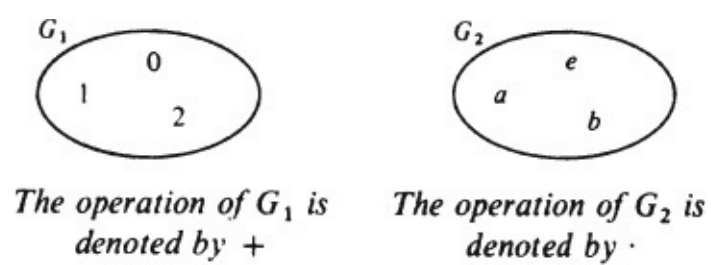


Table of G_1

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Table of G_2

$\cdot$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

G_1 and G_2 are different, but isomorphic. Indeed, if in G_1 we replace 0 by e , 1 by a , and 2 by b , then G_1 coincides with G_2 , the table of G_1 being transformed into the table of G_2 . In other words, the one-to-one correspondence

$$\begin{pmatrix} 0 & 1 & 2 \\ \downarrow & \downarrow & \downarrow \\ e & a & b \end{pmatrix}$$

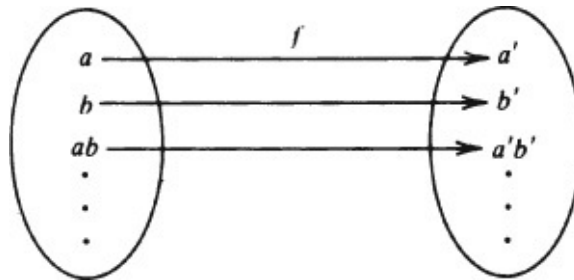
transforms G_1 to G_2 . It is called an *isomorphism* from G_1 to G_2 . Finally, because there exists an isomorphism from G_1 to G_2 , G_1 and G_2 are isomorphic to each other.

In general, by an isomorphism between two groups we mean a one-to-one correspondence between them which transforms one of the groups into the other. If there *exists* an isomorphism from one of the groups to the other, we say they are isomorphic. Let us be more specific:

If G_1 and G_2 are any groups, an *isomorphism* from G_1 to G_2 is a one-to-one correspondence f from G_1 to G_2 with the following property: For every pair of elements a and b in G_1 ,

$$\text{If } f(a) = a' \text{ and } f(b) = b' \text{ then } f(ab) = a'b' \quad (1)$$

In other words, if f matches a with a' and b with b' it *must* match ab with $a'b'$.



It is easy to see that if f has this property it transforms the table of G_1 into the table of G_2 :

G_1	b		G_2	b'
	$\vdots$			$\vdots$
a	$\dots ab$	$\xrightarrow[\text{replace } x \text{ by } f(x)]{\text{For every } x}$	a'	$\dots a'b'$

There is another, equivalent way of looking at this situation: If two groups G_1 and G_2 are isomorphic, we can say the two groups are actually the same, except that the elements of G_1 have *different names* from the elements of G_2 . G_1 becomes exactly G_2 if we *rename* its elements. The function which does the renaming is an isomorphism from G_1 to G_2 . Thus, in our last example, if 0 is

renamed e , 1 is renamed a , and 2 is renamed 6, G_1 becomes exactly G_2 , with the same table. (Note that we have also renamed the operation: it was called $+$ in G_1 and $\cdot$ in G_2 .)

By the way, property (1) may be written more concisely as follows:

$$f(ab) = f(a)f(b) \quad (2)$$

So we may sum up our definition of isomorphism in the following way:

Definition Let G_1 and G_2 be groups. A bijective function $f: G_1 \rightarrow G_2$ with the property that for any two elements a and b in G_1 ,

$$f(ab) = f(a)f(b) \quad (2)$$

is called an **isomorphism** from G_1 to G_2 .

If there exists an isomorphism from G_1 to G_2 , we say that G_1 is **isomorphic** to G_2 .

If there exists an isomorphism f from G_1 to G_2 , in other words, if G_1 is isomorphic to G_2 , we symbolize this fact by writing

$$G_1 \cong G_2$$

to be read, “ G_1 is isomorphic to G_2 .”

How does one recognize if two groups are isomorphic? This is an important question, and not quite so easy to answer as it may appear. There is no way of spontaneously recognizing whether two groups G_1 and G_2 are isomorphic. Rather, the groups must be carefully tested according to the above definition.

G_1 and G_2 are isomorphic if *there exists* an isomorphism from G_1 to G_2 . Therefore, the burden of proof is upon us to *find* an isomorphism from G_1 to G_2 , and show that it *is* an isomorphism. In other words, we must go through the following steps:

1. Make an educated guess, and come up with a function $f: G_1 \rightarrow G_2$ which looks as though it might be an isomorphism.
2. Check that f is *injective* and *surjective* (hence bijective).
3. Check that f satisfies the identity

$$f(ab) = f(a)f(b)$$

Here’s an example: $\mathbb{R}$ is the group of the real numbers with the operation of *addition*. $\mathbb{R}^{\text{pos}}$ is the group of the *positive* real numbers with the operation of *multiplication*. It is an interesting fact that $\mathbb{R}$ and $\mathbb{R}^{\text{pos}}$ are isomorphic. To see this, let us go through the steps outlined above:

1. The educated guess: The exponential function $f(x) = e^x$ is a function from $\mathbb{R}$ to $\mathbb{R}^{\text{pos}}$ which, if we recall its properties, might do the trick.
2. f is injective: Indeed, if $f(a) = f(b)$, that is, $e^a = e^b$, then, taking the natural log on both sides, we get $a = b$.

f is surjective: Indeed, if $y \in \mathbb{R}^{\text{pos}}$, that is, if y is any positive real number, then $y = e^{\ln y} = f(\ln y)$; thus, $y = f(x)$ for $x = \ln y$.

3. It is well known that $e^{a+b} = e^a \cdot e^b$, that is,

$$f(a + b) = f(a) \cdot f(b)$$

Incidentally, note carefully that the operation of $\mathbb{R}$ is $+$, whereas the operation of $\mathbb{R}^{\text{pos}}$ is $\cdot$. That is the reason we have to use $+$ on the left side of the preceding equation, and $\cdot$ on the right side of the equation.

How does one recognize when two groups are not isomorphic? In practice it is usually easier to show that two groups are *not* isomorphic than to show they *are*. Remember that if two groups are isomorphic they are replicas of each other; their elements (and their operation) may be named differently, but in all other respects they are the same and share the same properties. Thus, if a group G_1 has a property which group G_2 does not have (or vice versa), they are not isomorphic! Here are some examples of properties to look out for:

1. Perhaps G_1 is commutative, and G_2 is not.
2. Perhaps G_1 has an element which is its own inverse, and G_2 does not.
3. Perhaps G_1 is generated by two elements, whereas G_2 is not generated by any choice of two of its elements.
4. Perhaps every element of G_1 is the square of an element of G_1 , whereas G_2 does not have this property.

This list is by no means exhaustive; it merely illustrates the kind of things to be on the lookout for. Incidentally, the kind of properties to watch for are properties which do not depend merely on the *names* assigned to individual elements; for instance, in our last example, $0 \in G_1$ and $0 \notin G_2$, but nevertheless G_1 and G_2 are isomorphic.

Finally, let us state the obvious: if G_1 and G_2 cannot be put in one-to-one correspondence (say, G_1 has more elements than G_2), clearly they cannot be isomorphic.

In the early days of modern algebra the word “group” had a different meaning from the meaning it has today. In those days a group always meant a *group of permutations*. The only groups mathematicians used were groups whose elements were permutations of some fixed set and whose operation was composition.

There is something comforting about working with tangible, concrete things, such as groups of permutations of a set. At all times we have a clear picture of what it is we are working with. Later, as the axiomatic method reshaped algebra, a group came to mean *any* set with *any* associative operation having a neutral element and allowing each element an inverse. The new notion of group pleases mathematicians because it is simpler and more lean and sparing than the old notion of groups of permutations; it is also more general because it allows many new things to be groups which are not groups of permutations. However, it is harder to visualize, precisely because so many different things can be groups.

It was therefore a great revelation when, about 100 years ago, Arthur Cayley discovered that *every group is isomorphic to a group of permutations*. Roughly, this means that the groups of permutations are actually all the groups there are! Every group is (or is a carbon copy of) a group of permutations. This great result is a classic theorem of modern algebra. As a bonanza, its proof is not very difficult.

Cayley’s Theorem *Every group is isomorphic to a group of permutations.*

PROOF: Let G be a group; we wish to show that G is isomorphic to a group of permutations. The first question to ask is, “*What* group of permutations? Permutations of *what* set?” (After all, every permutation must be a permutation of some fixed set.) Well, the one set we have at hand is the set G , so we had better fix our attention on *permutations of G* . The way we match up elements of G with permutations of G is quite interesting:

With each element a in G we associate a function $\pi_a : G \rightarrow G$ defined by

$$\pi_a(x) = ax$$

In other words, π_a is the function whose rule may be described by the words “multiply on the left by a ,” We will now show that π_a is a permutation of G :

1. π_a is *injective*: Indeed, if $\pi_a(x_1) = \pi_a(x_2)$, then $ax_1 = ax_2$, so by the cancellation law, $x_1 = x_2$.
2. π_a is *surjective*: For if $y \in G$, then $y = a(a^{-1}y) = \pi_a(a^{-1}y)$. Thus, each y in G is equal to $\pi_a(x)$ for $x = a^{-1}y$.
3. Since π_a is an injective and surjective function from G to G , π_a is a *permutation of G* .

Let us remember that we have a permutation π_a for *each* element a in G ; for example, if b and c are other elements in G , π_b is the permutation “multiply on the left by b ,” π_c is the permutation “multiply on the left by c ,” and so on. In general, let G^* denote the set of *all* the permutations π_a as a ranges over all the elements of G :

$$G^* = \{\pi_a : a \in G\}$$

Observe now that G^* is a set consisting of permutations of G —but not necessarily *all* the permutations of G . In [Chapter 7](#) we used the symbol S_G to designate the group of *all* the permutations of G . We must show now that G^* is a *subgroup* of S_G , for that will prove that G^* is a *group of permutations*.

To prove that G^* is a subgroup of S_G , we must show that G^* is closed with respect to composition, and closed with respect to inverses. That is, we must show that if π_a and π_b are any elements of G^* , their composite $\pi_a \circ \pi_b$ is also in G^* ; and if π_a is any element of G^* , its inverse is in G^* .

First, we claim that if a and b are any elements of G , then

$$\pi_a \circ \pi_b = \pi_{ab} \quad (3)$$

To show that $\pi_a \circ \pi_b$ and π_{ab} are the same, we must show that they have the same effect on every element x : that is, we must prove the identity $[\pi_a \circ \pi_b](x) = \pi_{ab}(x)$. Well, $[\pi_a \circ \pi_b](x) = \pi_a(\pi_b(x)) = \pi_a(bx) = a(bx) = (ab)x = \pi_{ab}(x)$. Thus, $\pi_a \circ \pi_b = \pi_{ab}$; this proves that the composite of any two members π_a and π_b of G^* is another member π_{ab} of G^* . Thus, G^* is *closed with respect to composition*.

It is each to see that π_e is the identity function: indeed,

$$\pi_e(x) = ex = x$$

In other words, π_e is the identity element of S_G .

Finally, by [Equation \(3\)](#),

$$\pi_a \circ \pi_a - 1 = \pi_{aa} - 1 = \pi_e$$

So by [Theorem 2](#) of [Chapter 4](#), the inverse of π_a is $\pi_{a^{-1}}$. This proves that the inverse of any member π_a of G^* is another member $\pi_{a^{-1}}$ of G^* . Thus, G^* is closed with respect to inverses.

Since G^* is closed with respect to composition and inverses, G^* is a subgroup of S_G .

We are now in the final lap of our proof. We have a group of permutations G^* , and it remains only to show that G is isomorphic to G^* . To do this, we must find an isomorphism $f: G \rightarrow G^*$. Let f be the function

$$f(a) = \pi_a$$

In other words, f matches each element a in G with the permutation π_a in G^* . We can quickly show that f is an isomorphism:

1. f is injective: Indeed, if $f(a) = f(b)$ then $\pi_a = \pi_b$. Thus, $\pi_a(e) = \pi_b(e)$, that is, $ae = be$, so, finally, $a = b$.
2. f is surjective: Indeed, every element of G^* is some π_a , and $\pi_a = f(a)$.
3. Lastly, $f(ab) = \pi_{ab} = \pi_a \circ \pi_b = f(a) \circ f(b)$.

Thus, f is an isomorphism, and so $G \cong G^*$. ■

EXERCISES

A. Isomorphism Is an Equivalence Relation among Groups

The following three facts about isomorphism are true for all groups:

- (i) Every group is isomorphic to itself.
- (ii) If $G_1 \cong G_2$, then $G_2 \cong G_1$.
- (iii) If $G_1 \cong G_2$ and $G_2 \cong G_3$, then $G_1 \cong G_3$.

Fact (i) asserts that for any group G , there exists an isomorphism from G to G .

Fact (ii) asserts that, if there is an isomorphism f from G_1 to G_2 , there must be some isomorphism from G_2 to G_1 . Well, the inverse of f is such an isomorphism.

Fact (iii) asserts that, if there are isomorphisms $f: G_1 \rightarrow G_2$ and $g: G_2 \rightarrow G_3$, there must be an isomorphism from G_1 to G_3 . One can easily guess that $g \circ f$ is such an isomorphism. The details of facts (i), (ii), and (iii) are left as exercises.

1 Let G be any group. If $\varepsilon: G \rightarrow G$ is the identity function, $\varepsilon(x) = x$, show that ε is an isomorphism.

2 Let G_1 and G_2 be groups, and $f: G_1 \rightarrow G_2$ an isomorphism. Show that $f^{-1}: G_2 \rightarrow G_1$ is an isomorphism. [HINT: Review the discussion of inverse functions at the end of [Chapter 6](#). Then, for

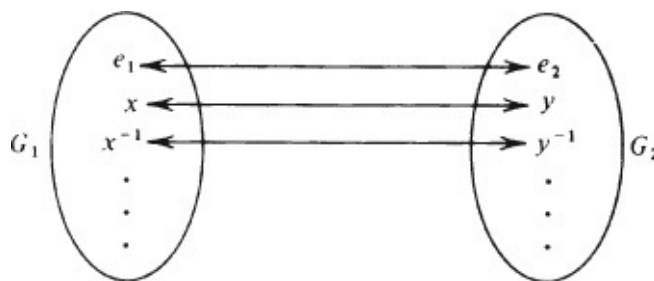
arbitrary elements $c, d \in G_2$, there exist $a, b \in G_1$, such that $c = f(a)$ and $d = f(b)$. Note that $a = f^{-1}(c)$ and $b = f^{-1}(d)$. Show that $f^{-1}(cd) = f^{-1}(c)f^{-1}(d)$.]

3 Let G_1 , G_2 , and G_3 be groups, and let $f: G_1 \rightarrow G_2$ and $g: G_2 \rightarrow G_3$ be isomorphisms. Prove that $g \circ f: G_1 \rightarrow G_3$ is an isomorphism.

B. Elements Which Correspond under an Isomorphism

Recall that an isomorphism f from G_1 to G_2 is a one-to-one correspondence between G_1 and G_2 satisfying $f(ab) = f(a)f(b)$. f matches every element of G_1 with a corresponding element of G_2 . It is important to note that:

- (i) f matches the neutral element of G_1 with the neutral element of G_2 .
- (ii) If f matches an element x in G_1 with y in G_2 , then, necessarily, f matches x^{-1} with y^{-1} . That is, if $x \leftrightarrow y$, then $x^{-1} \leftrightarrow y^{-1}$.
- (iii) f matches a generator of G_1 with a generator of G_2 .



The details of these statements are now left as an exercise. Let G_1 and G_2 be groups, and let $f: G_1 \rightarrow G_2$ be an isomorphism.

1 If e_1 denotes the neutral element of G_1 and e_2 denotes the neutral element of G_2 , prove that $f(e_1) = e_2$. [HINT: In any group, there is exactly one neutral element; show that $f(e_1)$ is the neutral element of G_2 .]

2 Prove that for each element a in G_1 , $f(a^{-1}) = [f(a)]^{-1}$. (HINT: You may use [Theorem 2](#) of [Chapter 4](#).)

3 If G_1 is a cyclic group with generator a , prove that G_2 is also a cyclic group, with generator $f(a)$.

C. Isomorphism of Some Finite Groups

In each of the following, G and H are finite groups. Determine whether or not $G \cong H$. Prove your answer in either case.

To find an isomorphism from G to H will require a little ingenuity. For example, if G and H are cyclic groups, it is clear that we must match a generator a of G with a generator b of H ; that is, $f(a) = b$. Then $f(aa) = bb$, $f(aaa) = bbb$, and so on. If G and H are not cyclic, we have other ways: for example, if G has an element which is its own inverse, it must be matched with an element of H having the same property. Often, the specifics of a problem will suggest an isomorphism, if we keep our eyes open.

To prove that a specific one-to-one correspondence $f: G \rightarrow H$ is an isomorphism, we may check that it transforms the table of G into the table of H .

1 G is the checkerboard game group of [Chapter 3](#), [Exercise D](#). H is the group of the complex numbers $\{i, -i, 1, -1\}$ under multiplication.

- 2 G is the same as in part 1. $H = \mathbb{Z}_4$.
- 3 G is the group P_2 of subsets of a two-element set. (See [Chapter 3, Exercise C](#).) H is as in part 1.
- # 4 G is S_3 , H is the group of matrices described on page 28 of the text.
- 5 G is the coin game group of [Chapter 3, Exercise E](#). H is D_4 , the group of symmetries of the square.
- 6 G is the group of symmetries of the rectangle. H is as in part 1.

D. Separating Groups into Isomorphism Classes

Each of the following is a set of four groups. In each set, determine which groups are isomorphic to which others. Prove your answers, and use [Exercise A3](#) where convenient.

1 $\mathbb{Z}_4$ $\mathbb{Z}_2 \times \mathbb{Z}_2$ P_2 V

[P_2 denotes the group of subsets of a two-element set. (See [Chapter 3, Exercise C](#).) V denotes the group of the four complex numbers $\{i, -i, 1, -1\}$ with respect to multiplication.]

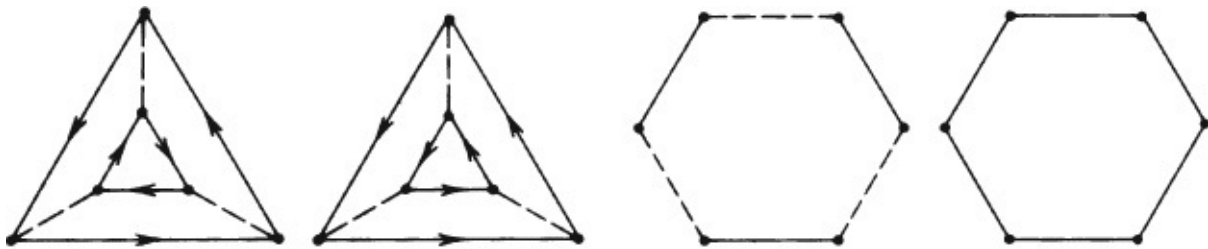
2 S_3 $\mathbb{Z}_6$ $\mathbb{Z}_3 \times \mathbb{Z}_2$ $\mathbb{Z}_7^*$

($\mathbb{Z}_7^*$ denotes the group $\{1, 2, 3, 4, 5, 6\}$ with multiplication modulo 7. The product modulo 7 of a and b is the remainder of ab after division by 7.)

3 $\mathbb{Z}_8$ P_3 $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ D_4

(D_4 is the group of symmetries of the square.)

4 The groups having the following Cayley diagrams:



E. Isomorphism of Infinite Groups

- # 1 Let E designate the group of all the even integers, with respect to addition. Prove that $\mathbb{Z} \cong E$.
- 2 Let G be the group $\{10^n : n \in \mathbb{Z}\}$ with respect to multiplication. Prove that $G \cong \mathbb{Z}$. (Remember that the operation of $\mathbb{Z}$ is addition.)
- 3 Prove that $\mathbb{C} = \mathbb{R} \times \mathbb{R}$.
- 4 We have seen in the text that $\mathbb{R}$ is isomorphic to $\mathbb{R}^{\text{pos}}$. Prove that $\mathbb{R}$ is *not* isomorphic to $\mathbb{R}^*$ (the multiplicative group of the nonzero real numbers). (HINT: Consider the properties of the number -1 in $\mathbb{R}^*$. Does $\mathbb{R}$ have *any* element with those properties?)
- 5 Prove that $\mathbb{Z}$ is not isomorphic to $\mathbb{Q}$.
- 6 We have seen that $\mathbb{R} \cong \mathbb{R}^{\text{pos}}$. However, prove that $\mathbb{Q}$ is *not* isomorphic to $\mathbb{Q}^{\text{pos}}$. ($\mathbb{Q}^{\text{pos}}$ is the multiplicative group of positive rational numbers.)

F. Isomorphism of Groups Given by Generators and Defining Equations

If a group G is generated, say, by a , b , and c , then a set of equations involving a , b , and c is called a set of *defining equations* for G if these equations completely determine the table of G . (See end of [Chapter](#)

5.) If G' is another group, generated by elements a' , b' , and c' satisfying the same defining equations as a , b , and c , then G' has the same table as G (because the tables of G and G' are completely determined by the defining equations, which are the same for G as for G').

Consequently, if we know generators and defining equations for two groups G and G' , and if we are able to match the generators of G with those of G' so that the defining equations are the same, we may conclude that $G \cong G'$.

Prove that the following pairs of groups G , G' are isomorphic.

1 G is the subgroup of S_4 generated by (24) and (1234) ; $G' = \{e, a, b, b^2, b^3, ab, ab^2, ab^3\}$ where $a^2 = e$, $b^4 = e$, and $ba = ab^3$.

2 $G = S_3$; $G' = \{e, a, b, ab, aba, abab\}$ where $a^2 = e$, $b^2 = e$, and $bab = aba$.

3 $G = D_4$; $G' = \{e, a, b, ab, aba, (ab)^2, ba, bab\}$ where $a^2 = b^2 = e$ and $(ab)^4 = e$.

4 $G = \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$; $G' = \{e, a, b, c, ab, ac, bc, abc\}$ where $a^2 = b^2 = c^2 = e$ and $(ab)^2 = (bc)^2 = (ac)^2 = e$.

G. Isomorphic Groups on the Set $\mathbb{R}$

1 G is the set $\{x \in \mathbb{R} : x \neq -1\}$ with the operation $x * y = x + y + xy$. Show that $f(x) = x - 1$ is an isomorphism from $\mathbb{R}^*$ to G . Thus, $\mathbb{R}^* \cong G$.

2 G is the set of the real numbers with the operation $x * y = x + y + 1$. Find an isomorphism $f: \mathbb{R} \rightarrow G$ and show that it is an isomorphism.

3 G is the set of the nonzero real numbers with the operation $x * y = xy/2$. Find an isomorphism from $\mathbb{R}^*$ to G .

4 Show that $f(x, y) = (-1)^y x$ is an isomorphism from $\mathbb{R}^{\text{pos}} \times \mathbf{Z}_2$ to $\mathbb{R}^*$. (REMARK: To combine elements of $\mathbb{R}^{\text{pos}} \times \mathbf{Z}_2$, one multiplies first components, adds second components.) Conclude that $\mathbb{R}^* \cong \mathbb{R}^{\text{pos}} \times \mathbf{Z}_2$.

H. Some General Properties of Isomorphism

1 Let G and H be groups. Prove that $G \times H \cong H \times G$.

2 If $G_1 \cong G_2$ and $H_1 \cong H_2$, then $G_1 \times H_1 \cong G_2 \times H_2$.

3 Let G be any group. Prove that G is abelian iff the function $f(x) = x^{-1}$ is an isomorphism from G to G .

4 Let G be any group, with its operation denoted multiplicatively. Let H be a group with the same set as G and let its operation be defined by $x * y = y \cdot x$ (where $\cdot$ is the operation of G). Prove that $G \cong H$.

5 Let c be a fixed element of G . Let H be a group with the same set as G , and with the operation $x * y = xcy$. Prove that the function $f(x) = c^{-1}x$ is an isomorphism from G to H .

I. Group Automorphisms

If G is a group, an *automorphism* of G is an isomorphism from G to G . We have seen ([Exercise A1](#)) that the identity function $\varepsilon(x) = x$ is an automorphism of G . However, many groups have *other* automorphisms besides this obvious one.

1 Verify that

$$f = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$$

is an automorphism of $\mathbf{z}_6$.

2 Verify that

$$f_1 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 0 & 2 & 4 & 1 & 3 \end{pmatrix} \quad f_2 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 0 & 3 & 1 & 4 & 2 \end{pmatrix}$$

and

$$f_3 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 0 & 4 & 3 & 2 & 1 \end{pmatrix}$$

are all automorphisms of $\mathbf{z}_5$.

3 If G is any group, and a is any element of G , prove that $f(x) = axa^{-1}$ is an automorphism of G .

4 Since each automorphism of G is a bijective function from G to G , it is a *permutation* of G . Prove the set

$$\text{Aut}(G)$$

of all the automorphisms of G is a subgroup of S_G . (Remember that the operation is composition.)

J. Regular Representation of Groups

By Cayley's theorem, every group G is isomorphic to a group G^* of permutations of G . Recall that we match each element a in G with the permutation π_a defined by $\pi_a = ax$, that is, the rule “multiply on the left by a .” We let $G^* = \{\pi_a : a \in G\}$; with the operation $\circ$ of composition it is a group of permutations, called the *left regular representation* of G . (It is called a “representation” of G because it is isomorphic to G .)

Instead of using the permutations π_a , we could just as well have used the permutations ρ_a defined by $\rho_a(x) = xa$, that is, “multiply on the right by a .” The group $G^\rho = \{\rho_a : a \in G\}$ is called the *right regular representation* of G .

If G is commutative, there is no difference between right and left multiplication, so G^* and G^ρ are the same, and are simply called the *regular representation* of G . Also, if the operation of G is denoted by $+$, the permutation corresponding to a is “add a ” instead of “multiply by a .”

Example The regular representation of $\mathbf{z}_3$ consists of the following permutations:

$$\begin{array}{ll} \pi_0 = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 2 \end{pmatrix} & \text{that is, the identity permutation} \\ \pi_1 = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix} & \text{that is, the rule “add 1”} \\ \pi_2 = \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix} & \text{that is, the rule “add 2”} \end{array}$$

The regular representation of $\mathbf{z}_3$ has the following table:

$\circ$	π_0	π_1	π_2
π_0	π_0	π_1	π_2
π_1	π_1	π_2	π_0
π_2	π_2	π_0	π_1

The function

$$f = \begin{pmatrix} 0 & 1 & 2 \\ \pi_0 & \pi_1 & \pi_2 \end{pmatrix}$$

is easily seen to be an isomorphism from $\mathbb{Z}_3$ to its regular representation.

Find the right and left regular representation of each of the following groups, and compute their tables. (If the group is abelian, find its regular representation.)

- 1 P_2 , the group of subsets of a two-element set. (See [Chapter 3](#), [Exercise C](#).)
- 2 $\mathbb{Z}_4$.
- 3 The group G of matrices described on page 28 of the text.

ORDER OF GROUP ELEMENTS

Let G be an arbitrary group, with its operation denoted multiplicatively. *Exponential notation* is a convenient shorthand: for any positive integer n , we will agree to let

$$a^n = \underbrace{a \cdot a \cdots a}_{n \text{ times}}$$

$$a^{-n} = \underbrace{a^{-1} a^{-1} \cdots a^{-1}}_{n \text{ times}}$$

and

$$a^0 = e$$

Take care to observe that we are considering only integer exponents, *not* rational or real exponents. Raising a to a positive power means multiplying a by itself the given number of times. Raising a to a negative power means multiplying a^{-1} by itself the given number of times. Raising a to the power 0 yields the group's identity element.

These are the same conventions used in elementary algebra, and they lead to the same familiar “laws of exponents.”

Theorem 1: Laws of exponents *if G is a group and $a \in G$, the following identities hold for all integers m and n :*

- (i) $a^m a^n = a^{m+n}$
- (ii) $(a^m)^n = a^{mn}$
- (iii) $a^{-n} = (a^{-1})^n = (a^n)^{-1}$

These laws are very easy to prove when m and n are positive integers. Indeed,

$$(i) \quad a^m a^n = \underbrace{aa \cdots a}_{m \text{ times}} \cdot \underbrace{aa \cdots a}_{n \text{ times}} = a^{m+n}$$

$$(ii) \quad (a^m)^n = \underbrace{a^m a^m \cdots a^m}_{n \text{ times}} = \underbrace{aa \cdots a}_{mn \text{ times}} = a^{mn}$$

Next, by definition $a^{-n} = a^{-1} \cdots a^{-1} = (a^{-1})^n$. Finally, since the inverse of a product is the product of the inverses in reverse order,

$$(a^n)^{-1} = (aa \cdots a)^{-1} = a^{-1}a^{-1} \cdots a^{-1} = a^{-n}$$

To prove Theorem 1 completely, we need to check the other cases, where each of the integers m and n is allowed to be zero or negative. This routine case-by-case verification is left to the student as [Exercise A](#) at the end of this chapter.

In order to delve more deeply into the behavior of exponents we must use an elementary but very important property of the integers: From elementary arithmetic we know that we can divide any integer by any positive integer to get an integer quotient and an integer remainder. The remainder is nonnegative and less than the dividend. For example, 25 may be divided by 8, giving a quotient of 3, and leaving a remainder of 1:

$$25 = 8 \times \underbrace{3}_q + \underbrace{1}_r$$

Similarly, -25 may be divided by 8, with a quotient of -4 and a remainder of 7:

$$-25 = 8 \times \underbrace{(-4)}_q + \underbrace{7}_r$$

This important principle is called the division algorithm. In its precise form, it may be stated as follows:

Theorem 2: Division algorithm *if m and n are integers and n is positive, there exist unique integers q and r such that*

$$m = nq + r \quad \text{and} \quad 0 \leq r < n$$

We call q the *quotient*, and r the *remainder*, in the division of m by n .

At this stage we will take the division algorithm to be a *postulate* of the system of the integers. Later, in [Chapter 19](#), we will turn things around, starting with a simpler premise and proving the division algorithm from it.

Let G be a group, and a an element of G . Let us observe that

If there exists a nonzero integer m such that $a^m = e$, then there exists a positive integer n such that $a^n = e$.

Indeed, if $a^m = e$ where m is negative, then $a^{-m} = (a^m)^{-1} = e^{-1} = e$. Thus, $a^{-m} = e$ where $-m$ is positive. This simple observation is crucial in our next definition. Let G be an arbitrary group, and a an element of G :

Definition *If there exists a nonzero integer m such that $a^m = e$, then the **order** of the element a is defined to be the **least positive integer** n such that $a^n = e$.*

*If there does not exist any nonzero integer m such that $a^m = e$, we say that a has order **infinity**.*

Thus, in any group G , every element has an order which is either a positive integer or infinity. If the order of a is a positive integer, we say that a has *finite order*; otherwise, a has *infinite order*. For

example, let us glance at S_3 , whose table appears on page 72. (It is customary to use exponential notation for composition: for instance, $\beta \circ \beta = \beta^2$, $\beta \circ \beta \circ \beta = \beta^3$, and so on.) The order of α is 2, because $\alpha^2 = \varepsilon$ and 2 is the smallest positive integer which satisfies that equation. The order of β is 3, because $\beta^3 = \varepsilon$, and 3 is the lowest positive power of β equal to ε . It is clear, similarly, that γ has order 2, δ has order 3, and κ has order 2. What is the order of ε ?

It is important to note that one speaks of *powers* of a only when the group's operation is called multiplication. When we use additive notation, we speak of *multiples* of a instead of powers of a . The *positive multiples* of a are $a, a + a, a + a + a$, and so on, while the *negative multiples* of a are $-a, (-a) + (-a), (-a) + (-a) + (-a)$, and so on. In $\mathbf{z}_6$, the number 2 has order 3, because $2 + 2 + 2 = 0$, and no smaller multiple of 2 is equal to 0. Similarly, the order of 3 is 2, the order of 4 is 3, and the order of 5 is 6.

In $\mathbf{z}$, the number 2 has infinite order, because no nonzero multiple of 2 is equal to 0. As a matter of fact, in $\mathbf{z}$, every nonzero number has infinite order.

The main fact about the order of elements is given in the next two theorems. In each of the following theorems, G is an arbitrary group and a is any element of G .

Theorem 3: Powers of a , if a has finite order *if the order of a is n , there are exactly n different powers of a , namely,*

$$a^0, a, a^2, a^3, \dots, a^{n-1}$$

What this theorem asserts is that every positive or negative power of a is equal to one of the above, and the above are all different from one another.

Before going on, remember that the order of a is n , hence

$$a^n = e$$

and n is the *smallest* positive integer which satisfies this equation.

PROOF OF THEOREM 3: Let us begin by proving that every power of a is equal to one of the powers $a^0, a^1, a^2, \dots, a^{n-1}$. Let a^m be any power of a . Use the division algorithm to divide m by n :

$$m = nq + r \quad 0 \leq r < n$$

Then $a^m = a^{nq+r} = (a^{nq})a^r = (a^n)^q a^r = e^q a^r = a^r$

Thus, $a^m = a^r$, and r is one of the integers $0, 1, 2, \dots, n-1$.

Next, we will prove that $a^0, a^1, a^2, \dots, a^{n-1}$ are all different. Suppose not; suppose $a^r = a^s$, where r and s are distinct integers between 0 and $n-1$. Either $r < s$ or $s < r$, say $s < r$. Thus $0 \leq s < r < n$, and consequently,

$$0 < r - s < n \quad (1)$$

But $a^r = a^s$; hence

$$a^r (a^s)^{-1} = a^s (a^s)^{-1}$$

Therefore,

$$a^r a^{-s} = e$$

so

$$a^{r-s} = e$$

However, this is impossible, because by [Equation \(1\)](#), $r - s$ is a positive integer less than n , whereas n (the order of a) is the *smallest* positive integer such that $a^n = e$.

This proves that we cannot have $a^r = a^s$ where $r \neq s$. Thus, $a^0, a^1, a^2, \dots, a^{n-1}$ are all different! ■

Theorem 4: Powers of a , if a has infinite order *If a has order infinity, then all the powers of a are different. That is, if r and s are distinct integers, then $a^r \neq a^s$.*

PROOF: Let r and s be integers, and suppose $a^r = a^s$.

Then
$$a^r(a^s)^{-1} = a^s(a^s)^{-1}$$

hence
$$a^{r-s} = e$$

But a has order infinity, and this means that a^m is not equal to e for any integer m except 0. Thus, $r - s = 0$, so $r = s$. ■

This chapter concludes with a technical property of exponents, which is of tremendous importance in applications.

If a is an element of a group, the order of a is the *least positive integer* n such that $a^n = e$. But there are *other* integers, say t , such that $a^t = e$. How are they related to n ? The answer is very simple:

Theorem 5 *Suppose an element a in a group has order n . Then $a^t = e$ iff t is a multiple of n (“ t is a multiple of n ” means that $t = nq$ for some integer q).*

PROOF: If $t = nq$, then $a^t = a^{nq} = (a^n)^q = e^q = e$. Conversely, suppose $a^t = e$. Divide t by n using the division algorithm:

$$t = nq + r \quad 0 \leq r < n$$

Then

$$e = a^t = a^{nq+r} = (a^n)^q a^r = e^q a^r = a^r$$

Thus, $a^r = e$, where $0 \leq r < n$. If $r \neq 0$, then r is a positive integer less than n , whereas n is the *smallest* positive integer such that $a^n = e$. Thus $r = 0$, and therefore $t = nq$. ■

If a is any element of a group, we will denote the order of a by

$$\text{ord}(a)$$

EXERCISES

A. Laws of Exponents

Let G be a group and $a \in G$.

1 Prove that $a^m a^n = a^{m+n}$ in the following cases:

- (a) $m = 0$
- (b) $m < 0$ and $n > 0$
- (c) $m < 0$ and $n < 0$

2 Prove that $(a^m)^n = a^{mn}$ in the following cases:

- (a) $m = 0$
- (b) $n = 0$
- (c) $m < 0$ and $n > 0$
- (d) $m > 0$ and $n < 0$
- (e) $m < 0$ and $n < 0$

3 Prove that $(a^n)^{-1} = a^{-n}$ in the following cases:

- (a) $n = 0$
- (b) $n < 0$

B. Examples of Orders of Elements

1 What is the order of 10 in $\mathbb{Z}_{25}$?

2 What is the order of 6 in $\mathbb{Z}_{16}$?

3 What is the order of

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 3 & 2 & 5 & 4 \end{pmatrix}$$

in S_6

4 What is the order of 1 in $\mathbb{R}^*$? What is the order of 1 in $\mathbb{R}$?

5 If A is the set of all the real numbers $x \neq 0, 1, 2$, what is the order of

$$f(x) = \frac{2}{2-x}$$

in S_A ?

6 Can an element of an *infinite* group have *finite* order? Explain.

7 In $\mathbb{Z}_{24}$, list all the elements (a) of order 2; (b) of order 3; (c) of order 4; (d) of order 6.

C. Elementary Properties of Order

Let a , b , and c be elements of a group G . Prove the following:

- 1 $\text{Ord}(a) = 1$ iff $a = e$.
- 2 If $\text{ord}(a) = n$, then $a^{n-r} = (a^r)^{-1}$.
- 3 If $a^k = e$ where k is odd, then the order of a is odd.
- 4 $\text{Ord}(a) = \text{ord}(bab^{-1})$.
- 5 The order of a^{-1} is the same as the order of a .
- 6 The order of ab is the same as the order of ba . [HINT: if

$$(ba)^n = \underbrace{baba \cdots ba}_x = e$$

then a is the inverse of x . Thus, $ax = e$.]

7 $\text{Ord}(abc) = \text{ord}(cab) = \text{ord}(bca)$.

8 Let $x = a^1 a^2 \cdots a^n$, and let y be a product of the same factors, permuted cyclically. (That is, $y = a_k a_{k+1} \cdots a_n a_1 \cdots a_{k-1}$.)

$\cdots a_n a_1 \cdots a_{k-1}$.) Then $\text{ord}(x) = \text{ord}(y)$.

D. Further Properties of Order

Let a be an element of finite order of a group G . Prove the following:

- 1 If $a^p = e$ where p is a prime number, then a has order p . ($a \neq e$.)
- 2 The order of a^k is a divisor (factor) of the order of a .
- 3 If $\text{ord}(a) = km$, then $\text{ord}(a^k) = m$.
- 4 If $\text{ord}(a) = n$ where n is odd, then $\text{ord}(a^2) = n$.
- 5 If a has order n , and $a^r = a^s$, then n is a factor of $r - s$.
- 6 If a is the *only* element of order k in G , then a is in the center of G . (HINT: Use [Exercise C4](#). Also, see [Chapter 4, Exercise C6](#).)
- 7 If the order of a is not a multiple of r , then the order of a^k is not a multiple of m . (HINT: Use part 2.)
- 8 If $\text{ord}(a) = mk$ and $a^{rk} = e$, then r is a multiple of m .

† E. Relationship between $\text{ord}(ab)$, $\text{ord}(a)$, and $\text{ord}(b)$

Let a and b be elements of a group G . Let $\text{ord}(a) = m$ and $\text{ord}(b) = n$; let $\text{lcm}(m, n)$ denote the least common multiple of m and n . Prove parts 1–5:

- 1 If a and b commute, then $\text{ord}(ab)$ is a divisor of $\text{lcm}(m, n)$.
- 2 If m and n are relatively prime, then no power of a can be equal to any power of b (except for e). (REMARK: Two integers are said to be relatively prime if they have no common factors except ± 1 .) (HINT: Use [Exercise D2](#).)
- 3 If m and n are relatively prime, then the products $a^i b^j$ ($0 \leq i < m$, $0 \leq j < n$) are all distinct.
- 4 Let a and b commute. If m and n are relatively prime, then $\text{ord}(ab) = mn$. (HINT: Use part 2.)
- 5 Let a and b commute. There is an element c in G whose order is $\text{lcm}(m, n)$. (HINT: Use part 4, above, together with [Exercise D3](#). Let $c = a^i b$ where a^i is a certain power of a .)
- 6 Give an example to show that part 1 is not true if a and b do not commute.

Thus, there is no simple relationship between $\text{ord}(ab)$, $\text{ord}(a)$, and $\text{ord}(b)$ if a and b fail to commute.

† F. Orders of Powers of Elements

Let a be an element of order 12 in a group G .

- 1 What is the smallest positive integer k such that $a^{8k} = e$? (HINT: Use Theorem 5 and explain carefully!)
- # 2 What is the order of a^8 ?
- 3 What are the orders of a^9 , a^{10} , a^5 ?
- 4 Which powers of a have the same order as a ? [That is, for what values of k is $\text{ord}(a^k) = 12$?]
- 5 Let a be an element of order m in any group G . What is the order of a^k ? (Look at the preceding examples, and generalize. Do not prove.)
- 6 Let a be an element of order m in any group G . For what values of k is $\text{ord}(a^k) = m$? (Look at the preceding examples. Do not prove.)

† G. Relationship between $\text{ord}(a)$ and $\text{ord}(a^k)$

From elementary arithmetic we know that every integer may be written uniquely as a product of prime numbers. Two integers m and n are said to be *relatively prime* if they have no prime factors in common. (For example, 15 and 8 are relatively prime.) Here is a useful fact: If m and n are relatively prime, and m is a factor of nk , then m is a factor of k . (Indeed, all the prime factors of m are factors of nk but not of n , hence are factors of k .)

Let a be an element of order n in a group G .

1 Prove that if m and n are relatively prime, then a^m has order n . (HINT: If $a^{mk} = e$, use Theorem 5 and explain why n must be a factor of k .)

2 Prove that if a^m has order n , then m and n are relatively prime. [HINT: Assume m and n have a common factor $q > 1$, hence we can write $m = m'q$ and $n = n'q$. Explain why $(a^m)^{n'} = e$, and proceed from there.]

3 Let l be the least common multiple of m and n . Let $l/m = k$. Explain why $(a^m)^k = e$.

4 Prove: If $(a^m)^t = e$, then n is a factor of mt . (Thus, mt is a common multiple of m and n .) Conclude that

$$\underbrace{l}_{=mk} \leq mt$$

5 Use parts 3 and 4 to prove that the order of a^m is $[\text{lcm}(m, n)]/m$.

† H. Relationship between the Order of a and the Order of any k th Root of a

Let a denote an element of a group G .

1 Let a have order 12. Prove that if a has a cube root, say $a = b^3$ for some $b \in G$, then b has order 36. {HINT: Show that $b^{36} = e$; then show that for each factor k of 36, $b^k = e$ is impossible. [Example: If $b^{12} = e$, then $b^{12} = (b^3)^4 = a^4 = e$.] Derive your conclusion from these facts.}

2 Let a have order 6. If a has a fourth root in G , say $a = b^4$, what is the order of b ?

3 Let a have order 10. If a has a sixth root in G , say $a = b^6$, what is the order of b ?

4 Let a have order n , and suppose a has a sixth root in G , say $a = b^k$. Explain why the order of b is a factor of nk .

Let

$$\text{ord}(b) = \frac{nk}{l}$$

5 Prove that n and l are relatively prime. [HINT: Suppose n and l have a common factor $q > 1$. Then $n = qn'$ and $l = ql'$, so

$$\text{ord}(b) = \frac{qn'k}{ql'} = \frac{n'k}{l'}$$

Thus $b^{n'k} = e$. (Why?) Draw your conclusion from these facts.]

Thus, if a has order n and a has a k th root b , then b has order nk/l , where n and l are relatively prime.

6 Let a have order n . Let k be an integer such that every prime factor of k is a factor of n . Prove: If a has a k th root b , then $\text{ord}(b) = nk$.

CHAPTER ELEVEN

CYCLIC GROUPS

If G is a group and $a \in G$, it may happen that *every* element of G is a power of a . In other words, G may consist of all the powers of a , and nothing else:

$$G = \{a^n : n \in \mathbf{z}\}$$

In that case, G is called a *cyclic group*, and a is called its *generator*. We write

$$G = \langle a \rangle$$

and say that G is the cyclic group generated by a .

If $G = \langle a \rangle$ is the cyclic group generated by a , and a has order n , we say that G is a *cyclic group of order n* . We will see in a moment that, in that case, G has exactly n elements. If the generator of G has order infinity, we say that G is a *cyclic group of order infinity*. In that case, we will see that G has infinitely many elements.

The simplest example of a cyclic group is $\mathbf{z}$, which consists of all the multiples of 1. (Remember that in additive notation we speak of “multiples” instead of “powers.”) $\mathbf{z}$ is a cyclic group of order infinity; its generator is 1. Another example of a cyclic group is $\mathbf{z}_6$, which consists of all the multiples of 1, added modulo 6. $\mathbf{z}_6$ is a cyclic group of order 6; 1 is a generator of $\mathbf{z}_6$, but $\mathbf{z}_6$ has another generator too. What is it?

Suppose $\langle a \rangle$ is a cyclic group whose generator a has order n . Since $\langle a \rangle$ is the set of all the powers of a , it follows from [Theorem 3](#) of [Chapter 10](#) that

$$\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$$

If we compare this group with $\mathbf{z}_n$, we notice a remarkable resemblance! For one thing, they are obviously in one-to-one correspondence:

$$\begin{array}{ccccccc} \langle a \rangle = \{ & a^0, & a^1, & a^2, & \dots, & a^{n-1} \} \\ & \updownarrow & \updownarrow & \updownarrow & & \updownarrow \\ \mathbb{Z}_n = \{ & 0, & 1, & 2, & \dots, & n-1 \} \end{array}$$

In other words, the function

$$f(i) = a^i$$

is a one-to-one correspondence from $\mathbb{Z}_n$ to $\langle a \rangle$. But this function has an additional property, namely,

$$f(i+j) = a^{i+j} = a^i a^j = f(i)f(j)$$

Thus, f is an *isomorphism* from $\mathbb{Z}_n$ to $\langle a \rangle$. In conclusion,

$$\mathbb{Z}_n \cong \langle a \rangle$$

Let us review the situation in the case where a has *order infinity*. In this case, by [Theorem 4 of Chapter 10](#),

$$\langle a \rangle = \{ \dots, a^{-2}, a^{-1}, e, a, a^2, \dots \}$$

There is obviously a one-to-one correspondence between this group and $\mathbb{Z}$:

$$\begin{array}{ccccccc} \langle a \rangle = \{ \dots, & a^{-2}, & a^{-1}, & a^0, & a^1, & a^2, & \dots \} \\ & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\ \mathbb{Z} = \{ \dots, & -2, & -1, & 0, & 1, & 2, & \dots \} \end{array}$$

In other words, the function

$$f(i) = a^i$$

is a one-to-one correspondence from $\mathbb{Z}$ to $\langle a \rangle$. As before, f is an isomorphism, and therefore

$$\mathbb{Z} \cong \langle a \rangle$$

What we have just proved is a very important fact about cyclic groups; let us state it as a theorem.

Theorem 1: Isomorphism of cyclic groups

- (i) *For every positive integer n , every cyclic group of order n is isomorphic to $\mathbb{Z}_n$. Thus, any two cyclic groups of order n are isomorphic to each other.*
- (ii) *Every cyclic group of order infinity is isomorphic to $\mathbb{Z}$, and therefore any two cyclic groups of order infinity are isomorphic to each other.*

If G is any group and $a \in G$, it is easy to see that

1. The product of any two powers of a is a power of a ; for $a^m a^n = a^{m+n}$.

2. Furthermore, the inverse of any power of a is a power of a , because $(a^n)^{-1} = a^{-n}$.

3. It therefore follows that the set of all the powers of a is a subgroup of G .

This subgroup is called the *cyclic subgroup of G generated by a* . It is obviously a cyclic group, and therefore we denote it by $\langle a \rangle$. If the element a has order n , then, as we have seen, $\langle a \rangle$ contains the n elements $\{e, a, a^2, \dots, a^{n-1}\}$. If a has order infinity, then $\langle a \rangle = \{\dots, a^{-2}, a^{-1}, e, a, a^2, \dots\}$ and has infinitely many elements.

For example, in $\mathbf{Z}$, $\langle 2 \rangle$ is the cyclic subgroup of $\mathbf{Z}$ which consists of all the multiples of 2. In $\mathbf{Z}_{15}$, $\langle 3 \rangle$ is the cyclic subgroup $\{0, 3, 6, 9, 12\}$ which contains all the multiples of 3. In S_3 , $\langle \beta \rangle = \{e, \beta, \delta\}$, and contains all the powers of β .

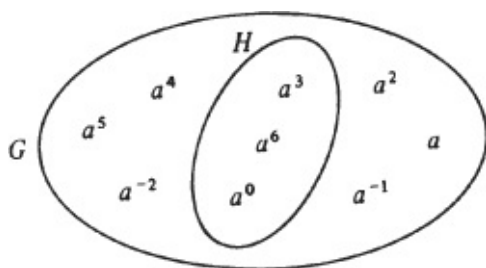
Can a cyclic group, such as $\mathbf{Z}$, have a *subgroup which is not cyclic*? This question is of great importance in our understanding of cyclic groups. Its answer is not obvious, and certainly not self-evident:

Theorem 2 *Every subgroup of a cyclic group is cyclic.*

Let $G = \langle a \rangle$ be a cyclic group, and let H be any subgroup of G . We wish to prove that H is cyclic.

Now, G has a generator a ; and when we say that H is cyclic, what we mean is that H too has a generator (call it b), and H consists of all the powers of b . The gist of this proof, therefore, is to *find* a generator of H , and then check that every element of H is a power of this generator.

Here is the idea: G is the cyclic group generated by a , and H is a subgroup of G . Every element of H is therefore in G , which means that every element of H is some power of a . The generator of H which we are searching for is therefore one of the powers of a —one of the powers of a which happens to be in H ; but which one? Obviously the lowest one! More accurately, the lowest *positive* power of a in H .



And now, carefully, here is the proof:

PROOF: Let m be the smallest positive integer such that $a^m \in H$. We will show that every element of H is a power of a^m , hence a^m is a generator of H .

Let a^t be *any* element of H . Divide t by m using the division algorithm:

$$t = mq + r \quad 0 \leq r < m$$

$$\text{Then} \quad a^t = a^{mq+r} = a^{mq} a^r$$

$$\text{Solving for } a^r, \quad a^r = (a^{mq})^{-1} a^t = (a^m)^{-q} a^t$$

But $a^m \in H$ and $a^t \in H$; thus $(a^m)^{-q} \in H$.

It follows that $a^r \in H$. But $r < m$ and m is the smallest positive integer such that $a^m \in H$. So $r = 0$, and therefore $t = mq$.

We conclude that every element $a^t \in H$ is of the form $a^t = (a^m)^q$, that is, a power of a^m . Thus, H is the cyclic group generated by a^m . ■

This chapter ends with a final comment regarding the different uses of the word “order” in algebra.

Let G be a group; as we have seen, the *order of an element* a in G is the least positive integer n such that

$$\underbrace{aaa \cdots a}_{n \text{ factors}} = e$$

(The order of a is *infinity* if there is no such n .)

Earlier, we defined the *order of the group* G to be the number of elements in G . Remember that the order of G is denoted by $|G|$.

These are two separate and distinct definitions, not to be confused with one another. Nevertheless, there is a connection between them: Let a be an element of order n in a group. By [Chapter 10, Theorem 3](#), there are exactly n different powers of a , hence $\langle a \rangle$ has n elements. Thus,

$$\text{If } \text{ord}(a) = n \text{ then } |\langle a \rangle| = n$$

That is, the order of a cyclic group is the same as the order of its generator.

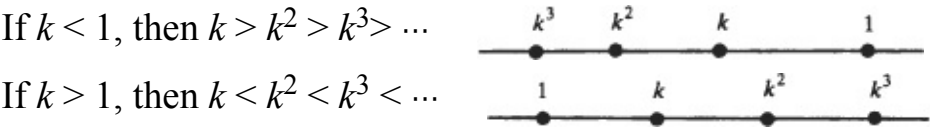
EXERCISES

A. Examples of Cyclic Groups

- 1 List the elements of $\langle 6 \rangle$ in $\mathbb{Z}_{16}$.
- 2 List the elements of $\langle f \rangle$ in S_6 , where

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 3 & 2 & 5 & 4 \end{pmatrix}$$

- 3 Describe the cyclic subgroup $\langle \frac{1}{2} \rangle$ in $\mathbb{R}^*$. Describe the cyclic group $\langle \frac{1}{2} \rangle$ in $\mathbb{R}$.
- 4 If $f(x) = x + 1$, describe the cyclic subgroup $\langle f \rangle$ of $S_{\mathbb{R}}$.
- 5 If $f(x) = x + 1$, describe the cyclic subgroup $\langle f \rangle$ of $\mathcal{F}(\mathbb{R})$.
- 6 Show that -1 , as well as 1 , is a generator of $\mathbb{Z}$. Are there any other generators of $\mathbb{Z}$? Explain! What are the generators of an arbitrary infinite cyclic group $\langle a \rangle$?
- 7 Is $\mathbb{R}^*$ cyclic? Try to prove your answer. HINT: Suppose k is a generator of $\mathbb{R}^*$:



B. Elementary Properties of Cyclic Groups

Prove each of the following:

- # 1 If G is a group of order n , G is cyclic iff G has an element of order n .
- 2 Every cyclic group is abelian.

- 3 If $G = \langle a \rangle$ and $b \in G$, the order of b is a factor of the order of a .
- 4 In any cyclic group of order n , there are elements of order k for every integer k which divides n .
- 5 Let G be an abelian group of order mn , where m and n are relatively prime. If G has an element of order m and an element of order n , G is cyclic. (See [Chapter 10, Exercise E4](#).)
- 6 Let $\langle a \rangle$ be a cyclic group of order n . If n and m are relatively prime, then the function $f(x) = x^m$ is an automorphism of $\langle a \rangle$. (HINT: Use [Exercise B3](#) and [Chapter 10, Theorem 5](#).)

C. Generators of Cyclic Groups

For any positive integer n , let $\phi(n)$ denote the number of positive integers less than n and relatively prime to n . For example, 1, 2, 4, 5, 7, and 8 are relatively prime to 9, so $\phi(9) = 6$. Let a have order n , and prove the following:

- 1 a^r is a generator of $\langle a \rangle$ iff r and n are relatively prime. (HINT: See [Chapter 10, Exercise G2](#).)
- 2 $\langle a \rangle$ has $\phi(n)$ different generators. (Use part 1 in your proof.)
- 3 For any factor m of n , let $C_m = \{x \in \langle a \rangle : x^m = e\}$. C_m is a subgroup of $\langle a \rangle$.
- # 4 C_m has exactly m elements. (HINT: Use [Exercise B4](#).)
- 5 An element x in $\langle a \rangle$ has order m iff x is a generator of C_m .
- 6 There are $\phi(m)$ elements of order m in $\langle a \rangle$. (Use parts 1 and 5.)
- # 7 Let $n = mk$. a^r has order m iff $r = kl$ where l and m are relatively prime. (HINT: See [Chapter 10, Exercise G1](#), 2.)
- 8 If c is any generator of $\langle a \rangle$, then $\{c^r : r \text{ is relatively prime to } n\}$ is the set of all the generators of $\langle a \rangle$.

D. Elementary Properties of Cyclic Subgroups of Groups

Let G be a group and let $a, b \in G$. Prove the following:

- 1 If a is a power of b , say $a = b^k$, then $\langle a \rangle \subseteq \langle b \rangle$.
- 2 Suppose a is a power of b , say $a = b^k$. Then b is equal to a power of a iff $\langle a \rangle = \langle b \rangle$.
- 3 Suppose $a \in \langle b \rangle$. Then $\langle a \rangle = \langle b \rangle$ iff a and b have the same order.
- 4 Let $\text{ord}(a) = n$, and $b = a^k$. Then $\langle a \rangle = \langle b \rangle$ iff n and k are relatively prime.
- 5 Let $\text{ord}(a) = n$, and suppose a has a k th root, say $a = b^k$. Then $\langle a \rangle = \langle b \rangle$ iff k and n are relatively prime.
- 6 Any cyclic group of order mn has a unique subgroup of order n .

E. Direct Products of Cyclic Groups

Let G and H be groups, with $a \in G$ and $b \in H$. Prove parts 1-4:

- 1 If (a, b) is a generator of $G \times H$, then a is a generator of G and b is a generator of H .
- 2 If $G \times H$ is a cyclic group, then G and H are both cyclic.
- 3 The converse of part 2 is false. (Give an example to demonstrate this.)
- 4 Let $\text{ord}(a) = m$ and $\text{ord}(b) = n$. The order of (a, b) in $G \times H$ is the least common multiple of m and n . (HINT: Use [Chapter 10, Theorem 5](#). Nothing else is needed!)

- 5** Conclude from part 4 that if m and n are relatively prime, then (a, b) has order mn .
- 6** Suppose $(c, d) \in G \times H$, where c has order m and d has order n . Prove: If m and n are *not* relatively prime (hence have a common factor $q > 1$), then the order of (c, d) is less than mn .
- 7** Conclude from parts 5 and 6 that $\langle a \rangle \times \langle b \rangle$ is cyclic iff $\text{ord}(a)$ and $\text{ord}(b)$ are relatively prime.
- 8** Let G be an abelian group of order mn , where m and n are relatively prime. Prove: If G has an element a of order m and an element b of order n , then $G \cong \langle a \rangle \times \langle b \rangle$. (HINT: See [Chapter 10, Exercise E1](#), 2.)
- 9** Let $\langle a \rangle$ be a cyclic group of order mn , where m and n are relatively prime, and prove that $\langle a \rangle \cong \langle a^m \rangle \times \langle a^n \rangle$.

† F. k th Roots of Elements in a Cyclic Group

Let $\langle a \rangle$ be a cyclic group of order n . For any integer k , we may ask: which elements in $\langle a \rangle$ have a k th root? The exercises which follow will answer this question.

- 1** Let a have order 10. For what integers k ($0 \leq k \leq 12$), does a have a k th root? For what integers k ($0 \leq k \leq 12$), does a^6 have a k th root?

Let k and n be any integers, and let $\text{gcd}(k, n)$ denote the greatest common divisor of k and n . A linear combination of k and n is any expression $ck + dn$ where c and d are integers. It is a simple fact of number theory (the proof is given on page 219), that an integer m is equal to a linear combination of k and n iff m is a multiple of $\text{gcd}(k, n)$. Use this fact to prove the following, where a is an element of order n in a group G .

- 2** If m is a multiple of $\text{gcd}(k, n)$, then a^m has a k th root in $\langle a \rangle$. [HINT: Compute a^m , and show that $a^m = (a^c)^k$ for some $a^c \in \langle a \rangle$.]

3 If a^m has a k th root in $\langle a \rangle$, then m is a multiple of $\text{gcd}(k, n)$. Thus, a^m has a k th root in $\langle a \rangle$ iff $\text{gcd}(k, n)$ is a factor of m .

- 4** a has a k th root in $\langle a \rangle$ iff k and n are relatively prime.

- 5** Let p be a prime number.

(a) If n is not a multiple of p , then every element in $\langle a \rangle$ has a p th root.

(b) If n is a multiple of p , and a^m has a p th root, then m is a multiple of p .

(Thus, the only elements in $\langle a \rangle$ which have p th roots are e, a^p, a^{2p} , etc.)

- 6** The set of all the elements in $\langle a \rangle$ having a k th root is a subgroup of $\langle a \rangle$. Explain why this subgroup is cyclic, say $\langle a^m \rangle$. What is the value of m ? (Use part 3.)

CHAPTER THIRTEEN

COUNTING COSETS

Just as there are great works in art and music, there are also great creations of mathematics. “Greatness,” in mathematics as in art, is hard to define, but the basic ingredients are clear: a *great* theorem should contribute substantial new information, and it should be *unexpected!*. That is, it should reveal something which common sense would not naturally lead us to expect. The most celebrated theorems of plane geometry, as may be recalled, come as a complete surprise; as the proof unfolds in simple, sure steps and we reach the conclusion—a conclusion we may have been skeptical about, but which is now established beyond a doubt—we feel a certain sense of awe not unlike our reaction to the ironic or tragic twist of a great story.

In this chapter we will consider a result of modern algebra which, by all standards, is a great theorem. It is something we would not likely have foreseen, and which brings new order and simplicity to the relationship between a group and its subgroups.

We begin by adding to our algebraic tool kit a new notion—a conceptual tool of great versatility which will serve us well in all the remaining chapters of this book. It is the concept of a *coset*.

Let G be a group, and H a subgroup of G . For any element a in G , the symbol

$$aH$$

*denotes the set of all products ah , as a remains fixed and h ranges over H . aH is called a **left coset** of H in G .*

In similar fashion

$$Ha$$

*denotes the set of all products ha , as a remains fixed and h ranges over H . Ha is called a **right coset** of H in G .*

In practice, it will make no difference whether we use left cosets or right cosets, just as long as we *remain consistent*. Thus, from here on, whenever we use cosets we will use *right* cosets. To simplify our

sentences, we will say *coset* when we mean “right coset.”

When we deal with cosets in a group G , we must keep in mind that every coset in G is a subset of G . Thus, when we need to prove that two cosets Ha and Hb are equal, we must show that they are *equal sets*. What this means, of course, is that every element $x \in Ha$ is in Hb , and conversely, every element $y \in Hb$ is in Ha . For example, let us prove the following elementary fact:

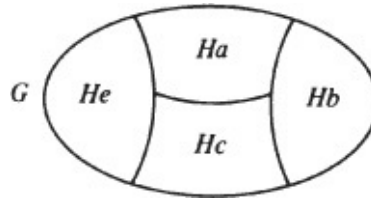
$$\text{If } a \in Hb, \text{ then } Ha = Hb \quad (1)$$

We are given that $a \in Hb$, which means that $a = h_1b$ for some $h_1 \in H$. We need to prove that $Ha = Hb$.

Let $x \in Ha$; this means that $x = h_2a$ for some $h_2 \in H$. But $a = h_1b$, so $x = h_2a = (h_2h_1)b$, and the latter is clearly in Hb . This proves that every $x \in Ha$ is in Hb ; analogously, we may show that every $y \in Hb$ is in Ha , and therefore $Ha = Hb$.

The first major fact about cosets now follows. Let G be a group and let H be a fixed subgroup of G :

Theorem 1 *The family of all the cosets Ha , as a ranges over G , is a partition of G .*



PROOF: First, we must show that any two cosets, say Ha and Hb , are either disjoint or equal. If they are disjoint, we are done. If not, let $x \in Ha \cap Hb$. Because $x \in Ha$, $x = h_1a$ for some $h_1 \in H$. Because $x \in Hb$, $x = h_2b$ for some $h_2 \in H$. Thus, $h_1a = h_2b$, and solving for a , we have

$$a = (h_1^{-1}h_2)b$$

Thus,

$$a \in Hb$$

It follows from Property (1) above that $Ha = Hb$.

Next, we must show that *every* element $c \in G$ is in one of the cosets of H . But this is obvious, because $c = ec$ and $e \in H$; therefore,

$$c = ec \in Hc$$

Thus, the family of all the cosets of H is a partition of G . ■

Before going on, it is worth making a small comment: A given coset, say Hb , may be written in more than one way. By Property (1) if a is any element in Hb , then Hb is the same as Ha . Thus, for example, if a coset of H contains n different elements $a_1, a_2, \dots, a_n$, it may be written in n different ways, namely, $Ha_1, Ha_2, \dots, Ha_n$.

The next important fact about cosets concerns finite groups. Let G be a finite group, and H a subgroup of G . We will show that *all the cosets of H have the same number of elements!* This fact is a consequence of the next theorem.

Theorem 2 *If Ha is any coset of H , there is a one-to-one correspondence from H to Ha .*

PROOF: The most obvious function from H to Ha is the one which, for each $h \in H$, matches h with ha . Thus, let $f: H \rightarrow Ha$ be defined by

$$f(h) = ha$$

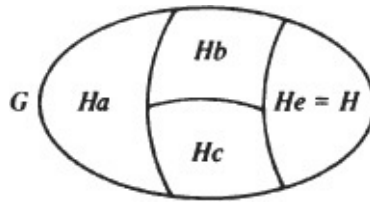
Remember that a remains fixed whereas h varies, and check that f is injective and surjective.

f is injective: Indeed, if $f(h_1) = f(h_2)$, then $h_1a = h_2a$, and therefore $h_1 = h_2$.

f is surjective, because every element of Ha is of the form ha for some $h \in H$, and $ha = f(h)$.

Thus, f is a one-to-one correspondence from H to Ha , as claimed. ■

By Theorem 2, any coset Ha has the same number of elements as H , and therefore all the cosets have the same number of elements!



Let us take a careful look at what we have proved in Theorems 1 and 2. Let G be a finite group and H any subgroup of G . G has been partitioned into cosets of H , and all the cosets of H have the same number of elements (which is the same as the number of elements in H). Thus, *the number of elements in G is equal to the number of elements in H , multiplied by the number of distinct cosets of H* . This statement is known as Lagrange's theorem. (Remember that the number of elements in a group is called the group's *order*.)

Theorem 3: Lagrange's theorem *Let G be a finite group, and H any subgroup of G . The order of G is a multiple of the order of H .*

In other words, the order of any subgroup of a group G is a divisor of the order of G .

For example, if G has 15 elements, its proper subgroups may have either 3 or 5 elements. If G has 7 elements, it has *no* proper subgroups, for 7 has no factors other than 1 and 7. This last example may be generalized:

Let G be a group with a *prime* number p of elements. If $a \in G$ where $a \neq e$, then the order of a is some integer $m \neq 1$. But then the cyclic group $\langle a \rangle$ has m elements. By Lagrange's theorem, m must be a factor of p . But p is a prime number, and therefore $m = p$. It follows that $\langle a \rangle$ has p elements, and is therefore all of G ! Conclusion:

Theorem 4 *If G is a group with a prime number p of elements, then G is a cyclic group. Furthermore, any element $a \neq e$ in G is a generator of G .*

Theorem 4, which is merely a consequence of Lagrange's theorem, is quite remarkable in itself. What it says is that *there is (up to isomorphism) only one group of any given prime order p* . For example, the only group (up to isomorphism) of order 7 is $\mathbf{Z}_7$, the only group of order 11 is $\mathbf{Z}_{11}$, and so on! So we now have complete information about all the groups whose order is a prime number.

By the way, if a is any element of a group G , the order of a is the same as the order of the cyclic

subgroup $\langle a \rangle$, and by Lagrange's theorem this number is a divisor of the order of G . Thus,

Theorem 5 *The order of any element of a finite group divides the order of the group.*

Finally, if G is a group and H is a subgroup of G , the *index of H in G* is the number of cosets of H in G . We denote it by $(G:H)$. Since the number of elements in G is equal to the number of elements in H , multiplied by the number of cosets of H in G ,

$$(G:H) = \frac{\text{order of } G}{\text{order of } H}$$

EXERCISES

A. Examples of Cosets in Finite Groups

In each of the following, H is a subgroup of G . In parts 1–5 list the cosets of H . For each coset, list the elements of the coset.

Example $G = \mathbf{z}_4$, $H = \{0, 2\}$.

(REMARK: If the operation of G is denoted by $+$, it is customary to write $H + x$ for a coset, rather than Hx .) The cosets of H in this example are

$$H = H + 0 = H + 2 = \{0, 2\} \quad \text{and} \quad H + 1 = H + 3 = \{1, 3\}$$

- 1 $G = S_3$, $H = \{\varepsilon, \beta, \delta\}$.
- 2 $G = S_3$, $H = \{\varepsilon, \alpha\}$.
- 3 $G = \mathbf{z}_{15}$, $H = \langle 5 \rangle$.
- 4 $G = D_4$, $H = \{R_0, R_4\}$. (For D_4 , see page 73.)
- 5 $G = S_4$, $H = A_4$. (For A_4 , see page 86.)
- 6 Indicate the order and index of each of the subgroups in parts 1 to 5.

B. Examples of Cosets in Infinite Groups

Describe the cosets of the subgroups described in parts 1–5:

- 1 The subgroup $\langle 3 \rangle$ of $\mathbf{z}$.
- 2 The subgroup $\mathbf{z}$ of $\mathbf{R}$.
- 3 The subgroup $H = \{2^n: n \in \mathbf{z}\}$ of $\mathbf{R}^*$.
- 4 The subgroup $\langle \frac{1}{2} \rangle$ of $\mathbf{R}^*$; the subgroup $\langle \frac{1}{2} \rangle$ of $\mathbf{R}$.
- 5 The subgroup $H = \{(x, y): x = y\}$ of $(\mathbf{R} \times \mathbf{R})$.
- 6 For any positive integer m , what is the index of $\langle m \rangle$ in $\mathbf{z}$?
- 7 Find a subgroup of $\mathbf{R}^*$ whose index is equal to 2.

C. Elementary Consequences of Lagrange's Theorem

Let G be a finite group. Prove the following:

- 1 If G has order n , then $x^n = e$ for every x in G .
- 2 Let G have order pq , where p and q are primes. Either G is cyclic, or every element $x \neq e$ in G has

order p or q .

3 Let G have order 4. Either G is cyclic, or every element of G is its own inverse. Conclude that every group of order 4 is abelian.

4 If G has an element of order p and an element of order q , where p and q are distinct primes, then the order of G is a multiple of pq .

5 If G has an element of order k and an element of order m , then $|G|$ is a multiple of $\text{lcm}(k, m)$, where $\text{lcm}(k, m)$ is the least common multiple of k and m .

6 Let p be a prime number. In any finite group, the number of elements of order p is a multiple of $p - 1$.

D. Further Elementary Consequences of Lagrange's Theorem

Let G be a finite group, and let H and K be subgroups of G . Prove the following:

1 Suppose $H \subseteq K$ (therefore H is a subgroup of K). Then $(G:H) = (G:K)(K:H)$.

2 The order of $H \cap K$ is a common divisor of the order of H and the order of K .

3 Let H have order m and K have order n , where m and n are relatively prime. Then $H \cap K = \{e\}$.

4 Suppose H and K are not equal, and both have order the same prime number p . Then $H \cap K = \{e\}$.

5 Suppose H has index p and K has index q , where p and q are distinct primes. Then the index of $H \cap K$ is a multiple of pq .

6 If G is an abelian group of order n , and m is an integer such that m and n are relatively prime, then the function $f(x) = x^m$ is an automorphism of G .

E. Elementary Properties of Cosets

Let G be a group, and H a subgroup of G . Let a and b denote elements of G . Prove the following:

1 $Ha = Hb$ iff $ab^{-1} \in H$.

2 $Ha = H$ iff $a \in H$.

3 If $aH = Ha$ and $bH = Hb$, then $(ab)H = H(ab)$.

4 If $aH = Ha$, then $a^{-1}H = Ha^{-1}$.

5 If $(ab)H = (ac)H$, then $bH = cH$.

6 The number of right cosets of H is equal to the number of left cosets of H .

7 If J is a subgroup of G such that $J = H \cap K$, then for any $a \in G$, $Ja = Ha \cap Ka$. Conclude that if H and K are of finite index in G , then their intersection $H \cap K$ is also of finite index in G .

Theorem 5 of this chapter has a useful converse, which is the following:

Cauchy's theorem *If G is a finite group, and p is a prime divisor of $|G|$, then G has an element of order p .*

For example, a group of order 30 must have elements of orders 2, 3, and 5. Cauchy's theorem has an elementary proof, which may be found on page 340.

In the next few exercise sets, we will survey all possible groups whose order is ≤ 10 . By **Theorem 4** of this chapter, if G is a group with a prime number p of elements, then $G \cong \mathbb{Z}_p$. This takes care of all groups of orders 2, 3, 5, and 7. In Exercise G6 of **Chapter 15**, it will be shown that if G is a group with p^2 elements (where p is a prime), then $G \cong \mathbb{Z}_{p^2}$ or $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$. This will take care of all groups of orders 4 and 9. The remaining cases are examined in the next three exercise sets.

† F. Survey of All Six-Element Groups

Let G be any group of order 6. By Cauchy's theorem, G has an element a of order 2 and an element b of order 3. By Chapter 10, Exercise E3, the elements

$$e, a, b, b^2, ab, ab^2$$

are all distinct; and since G has only six elements, these are all the elements in G . Thus, ba is one of the elements e, a, b, b^2, ab , or ab^2 .

1 Prove that ba cannot be equal to either e, a, b , or b^2 . Thus, $ba = ab$ or $ba = ab^2$.

Either of these two equations completely determines the table of G . (See the discussion at the end of Chapter 5.)

2 If $ba = ab$, prove that $G \cong \mathbf{z}_6$.

3 If $ba = ab^2$, prove that $G \cong S_3$.

It follows that $\mathbf{z}_6$ and S_3 are (up to isomorphism), the only possible groups of order 6.

† G. Survey of All 10-Element Groups

Let G be any group of order 10.

1 Reason as in Exercise F to show that $G = \{e, a, b, b^2, b^3, b^4, ab, ab^2, ab^3, ab^4\}$, where a has order 2 and b has order 5.

2 Prove that ba cannot be equal to e, a, b, b^2, b^3 , or b^4 .

3 Prove that if $ba = ab$, then $G \cong \mathbf{z}_{10}$.

4 If $ba = ab^2$, prove that $ba^2 = a^2b^4$, and conclude that $b = b^4$. This is impossible because b has order 5; hence $ba \neq ab^2$. (HINT: The equation $ba = ab^2$ tells us that we may move a factor a from the right to the left of a factor b , but in so doing, we must square b . To prove an equation such as the preceding one, move all factors a to the left of all factors b .)

5 If $ba = ab^3$, prove that $ba^2 = a^2b^9 = a^2b^4$, and conclude that $b = b^4$. This is impossible (why?); hence $ba \neq ab^3$.

6 Prove that if $ba = ab^4$, then $G \cong D_5$ (where D_5 is the group of symmetries of the pentagon).

Thus, the only possible groups of order 10 (up to isomorphism), are $\mathbf{z}_{10}$ and D_5 .

† H. Survey of All Eight-Element Groups

Let G be any group of order 8. If G has an element of order 8, then $G \cong \mathbf{z}_8$. Let us assume now that G has no element of order 8; hence all the elements $\neq e$ in G have order 2 or 4.

1 If every $x \neq e$ in G has order 2, let a, b, c be three such elements. Prove that $G = \{e, a, b, c, ab, bc, ac, abc\}$. Conclude that $G \cong \mathbf{z}_2 \times \mathbf{z}_2 \times \mathbf{z}_2$.

In the remainder of this exercise set, assume G has an element a of order 4. Let $H = \langle a \rangle = \{e, a, a^2, a^3\}$. If $b \in G$ is not in H , then the coset $Hb = \{b, ab, a^2b, a^3b\}$. By Lagrange's theorem, G is the union of $He = H$ and Hb ; hence

$$G = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$$

2 Assume there is in Hb an element of order 2. (Let b be this element.) If $ba = a^2b$, prove that $b^2a = a^4b^2$, hence $a = a^4$, which is impossible. (Why?) Conclude that either $ba = ab$ or $ba = a^3b$.

3 Let b be as in part 2. Prove that if $ba = ab$, then $G \cong \mathbf{Z}_4 \times \mathbf{Z}_2$.

4 Let b be as in part 2. Prove that if $ba = a^3b$, then $G \cong D_4$.

5 Now assume the hypothesis in part 2 is false. Then b, ab, a^2b , and a^3b all have order 4. Prove that $b^2 = a^2$. (HINT: What is the order of b^2 ? What element in G has the same order?)

6 Prove: If $ba = ab$, then $(a^3b)^2 = e$, contrary to the assumption that $\text{ord}(a^3b) = 4$. If $ba = a^2b$, then $a = b^4a = e$, which is impossible. Thus, $ba = a^3b$.

7 The equations $a^4 = b^4 = e$, $a^2 = b^2$, and $ba = a^3b$ completely determine the table of G . Write this table. (G is known as the *quaternion group* Q .)

Thus, the only groups of order 8 (up to isomorphism) are $\mathbf{Z}_8$, $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$, $\mathbf{Z}_4 \times \mathbf{Z}_2$, D_4 , and Q .

† I. Conjugate Elements

If $a \in G$, a *conjugate* of a is any element of the form xax^{-1} , where $x \in G$. (Roughly speaking, a conjugate of a is any product consisting of a sandwiched between any element and its inverse.) Prove each of the following:

1 The relation “ a is equal to a conjugate of b ” is an equivalence relation in G . (Write $a \sim b$ for “ a is equal to a conjugate of b .”)

This relation $\sim$ partitions any group G into classes called *conjugacy classes*. (The conjugacy class of a is $[a] = \{xax^{-1} : x \in G\}$.)

For any element $a \in G$, the *centralizer* of a , denoted by C_a , is the set of all the elements in G which commute with a . That is,

$$C_a = \{x \in G : xa = ax\} = \{x \in G : xax^{-1} = a\}$$

Prove the following:

2 For any $a \in G$, C_a is a subgroup of G .

3 $x^{-1}ax = y^{-1}ay$ iff xy^{-1} commutes with a iff $xy^{-1} \in C_a$.

4 $x^{-1}ax = y^{-1}ay$ iff $C_ax = C_ay$. (HINT: Use Exercise El.)

5 There is a one-to-one correspondence between the set of all the conjugates of a and the set of all the cosets of C_a . (HINT: Use part 4.)

6 The number of distinct conjugates of a is equal to $(G : C_a)$, the index of C_a in G . Thus, *the size of every conjugacy class is a factor of $|G|$* .

† J. Group Acting on a Set

Let A be a set, and let G be any subgroup of S_A . G is a group of permutations of A ; we say it is a *group acting on the set* A . Assume here that G is a finite group. If $u \in A$, the *orbit of* u (with respect to G) is the set

$$O(u) = \{g(u) : g \in G\}$$

1 Define a relation $\sim$ on A by $u \sim v$ iff $g(u) = v$ for some $g \in G$. Prove that $\sim$ is an equivalence relation on A , and that the orbits are its equivalence classes.

If $u \in A$, the *stabilizer of u* is the set $G_u = \{g \in G: g(u) = u\}$, that is, the set of all the permutations in G which leave u fixed.

2 Prove that G_u is a subgroup of G .

3 Let $\alpha = (1\ 2)(3\ 4)(5\ 6)$ and $\beta = (2\ 3)$ in S_6 . Let G be the following subgroup of S_6 : $G = \{\varepsilon, \alpha, \beta, \alpha\beta, \beta\alpha, \alpha\beta\alpha, \beta\alpha\beta, (\alpha\beta)^2\}$. Find $O(1)$, $O(2)$, $O(5)$, G_1 , G_2 , G_4 , G_5 .

4 Let $f, g \in G$. Prove that f and g are in the same left coset of G_u iff $f(u) = g(u)$. (HINT: Use Exercise E1 modified for left cosets.)

5 Use part 4 to show that the number of elements in $O(u)$ is equal to the index of G_u in G . [HINT: If $f(u) = v$, match the coset of f with v .]

6 Conclude from part 5 that the size of every orbit (with respect to G) is a factor of the order of G . In particular, if $f \in S_A$, the length of each cycle of f is a factor of the order of f in S_A .

K. Coding Theory: Coset Decoding

In order to undertake this exercise set, the reader should be familiar with the introductory paragraphs (preceding the exercises) of [Exercises F and G](#) of [Chapter 3](#) and [Exercise H](#) of [Chapter 5](#).

Recall that $\mathbb{B}^n$ is the group of all binary words of length n . A *group code* C is a subgroup of $\mathbb{B}^n$. To *decode* a received word $\mathbf{x}$ means to find the codeword $\mathbf{a}$ closest to $\mathbf{x}$, that is, the codeword $\mathbf{a}$ such that the distance $d(\mathbf{a}, \mathbf{x})$ is a minimum.

But $d(\mathbf{a}, \mathbf{x}) = w(\mathbf{a} + \mathbf{x})$, the weight (number of 1s) of $\mathbf{a} + \mathbf{x}$. Thus, to decode a received word $\mathbf{x}$ is to find the codeword $\mathbf{a}$ such that the weight $w(\mathbf{a} + \mathbf{x})$ is a minimum. Now, the coset $C + \mathbf{x}$ consists of all the sums $\mathbf{c} + \mathbf{x}$ as $\mathbf{c}$ ranges over all the codewords; so by the previous sentence, if $\mathbf{a} + \mathbf{x}$ is the word of minimum weight in the coset $C + \mathbf{x}$, then $\mathbf{a}$ is the word to which $\mathbf{x}$ must be decoded.

Now $\mathbf{a} = (\mathbf{a} + \mathbf{x}) + \mathbf{x}$; so $\mathbf{a}$ is found by adding $\mathbf{x}$ to the word of minimum weight in the coset $C + \mathbf{x}$. To recapitulate: In order to decode a received word $\mathbf{x}$ you examine the coset $C + \mathbf{x}$, find the word $\mathbf{e}$ of minimum weight in the coset (it is called the *coset leader*), and add $\mathbf{e}$ to $\mathbf{x}$. Then $\mathbf{e} + \mathbf{x}$ is the codeword closest to $\mathbf{x}$, and hence the word to which $\mathbf{x}$ must be decoded.

1 Let C_1 be the code described in Exercise G of [Chapter 3](#).

(a) List the elements in each of the cosets of C_1 .

(b) Find a coset leader in each coset. (There may be more than one word of minimum weight in a coset; choose one of them as coset leader.)

(c) Use the procedure described above to decode the following words $\mathbf{x}$: 11100, 01101, 11011, 00011.

2 Let C_3 be the Hamming code described in Exercise H2 of [Chapter 5](#). List the elements in each of the cosets of C_3 and find a leader in each coset. Then use coset decoding to decode the following words $\mathbf{x}$: 1100001, 0111011, 1001011.

3 Let C be a code and let $\mathbf{H}$ be the parity-check matrix of C . Prove that $\mathbf{x}$ and $\mathbf{y}$ are in the same coset of C if and only if $\mathbf{H}\mathbf{x} = \mathbf{H}\mathbf{y}$. (HINT: Use Exercise H8, [Chapter 5](#).)

If $\mathbf{x}$ is any word, $\mathbf{H}\mathbf{x}$ is called the *syndrome* of $\mathbf{x}$. It follows from part 3 that all the words in the same coset have the same syndrome, and words in different cosets have different syndromes. The

syndrome of a word $\mathbf{x}$ is denoted by $\text{syn}(\mathbf{x})$.

4 Let a code C have q cosets, and let the coset leaders be $\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_q$. Explain why the following is true: To decode a received word $\mathbf{x}$, compare $\text{syn}(\mathbf{x})$ with $\text{syn}(\mathbf{e}_1), \dots, \text{syn}(\mathbf{e}_q)$ and find the coset leader $\mathbf{e}_i$ such that $\text{syn}(\mathbf{x}) = \text{syn}(\mathbf{e}_i)$. Then $\mathbf{x}$ is to be decoded to $\mathbf{x} + \mathbf{e}_i$.

5 Find the syndromes of the coset leaders in part 2. Then use the method of part 4 to decode the words $\mathbf{x} = 1100001$ and $\mathbf{x} = 1001011$.