Cyril F. Gardiner

A First Course in Group Theory

Cyril F. Gardiner

A First Course in Group Theory

Springer-Verlag
New York Heidelberg Berlin

Cyril F. Gardiner
University of Exeter
Department of Mathematics
North Park Road
Exeter, EX4 4QE
England

AMS Subject Classification: 20-01

Library of Congress Cataloging in Publication Data

Gardiner, Cyril F
A first course in group theory.

(Universitext)
Bibliography: p.
Includes index.
1. Groups, Theory of. I. Title.
QA171.G27 512:22 80-25160

Printed in the United States of America.

9 8 7 6 5 4 3 2 1

ISBN 0-387-90545-6 Springer-Verlag New York Heidelberg Berlin
ISBN 3-540-90545-6 Springer-Verlag Berlin Heidelberg New York

PREFACE

One of the difficulties in an introductory book is to communicate a sense of purpose. Only too easily to the beginner does the book become a sequence of definitions, concepts, and results which seem little more than curiousities leading nowhere in particular. In this book I have tried to overcome this problem by making my central aim the determination of all possible groups of orders 1 to 15, together with some study of their structure. By the time this aim is realised towards the end of the book, the reader should have acquired the basic ideas and methods of group theory. To make the book more useful to users of mathematics, in particular students of physics and chemistry, I have included some applications of permutation groups and a discussion of finite point groups. The latter are the simplest examples of groups of particular interest to scientists. They occur as symmetry groups of physical configurations such as molecules.

Many ideas are discussed mainly in the exercises and the solutions at the end of the book. However, such ideas are used rarely in the body of the book. When they are, suitable references are given. Other exercises test and reinforce the text in the usual way.

A final chapter gives some idea of the directions in which the interested reader may go after working through this book. References to help in this are listed after the outline solutions. Also in this chapter I have included the usual results on series and solvable groups required for the study of the Galois group occurring in field theory and algebraic number theory.

In my experience, the value of a book to the average student is increased considerably by the inclusion of solutions to the exercises. This is true in particular for students who, by choice or necessity, work largely on their own. For this reason, I have included outline solutions of all the exercises at the end of the book. However, the student is advised to make a determined effort to solve the problems himself (or herself) before looking at the given solutions. I have made no attempt to grade the problems. In any case one person's difficulty may be another person's triviality.

For the basic notions of sets, relations, functions, and linear algebra the reader is referred to my book 'Modern Algebra; A Natural Approach, with Applications' (Ellis Horwood Ltd.). As a general reference this will be denoted by [G] in the text. In general, references will be denoted by [n] for some number n as given in detail in the bibliography at the end of the book.

This book is based on lectures given over many years at Exeter both to specialist mathematicians and to those whose main interests lay elsewhere yet who required the usual basic ideas in group theory. The interests of the latter are served by the first four chapters of this book, though I would be delighted should they read further.

Exeter, 1980. C. F. Gardiner

CONTENTS

CHAPTER 5 FINITELY GENERATED ABELIAN GROUPS

CHAPTER 6 THE SYLOW THEOREMS

CHAPTER 7 GROUPS OF ORDERS 1 TO 15

CHAPTER 8 EPILOGUE

OUTLINE SOLUTIONS TO THE EXERCISES

CHAPTER 1.
FIRST IDEAS

1.1 Introduction

There is some evidence to suggest that a sense of symmetry is at least as fundamental as a sense of number, although the concept of number predates the concept of symmetry.

An implicit use of symmetry occurs in mathematics, particularly geometry, as far back as the Greeks some 2,500 years ago. But strangely, the Greeks never captured the essence of symmetry explicitly. A detailed, but informal, discussion of symmetry is given by H. Weyl in his book "Symmetry" published by the Princeton University Press in 1952. The reader is recommended to study Weyl's book alongside the present one. For a visual representation of some of the ideas that we shall discuss, see "The Graphic Work of M. C. Escher" - Escher (Pan-Ballantine 1972, Oldbourne Press 1961).

In this book we regard group theory as the conscious and explicit study of symmetry. As such the subject emerged around 1830 A.D. At that time most of the leading mathematicians of the day were engrossed in the following problem.

For any real numbers a, b, c, with $a \neq 0$, the equation $ax^2 + bx + c = 0$ has a solution formula, namely:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

The cubic and quartic equations also have solution formulae of a similar form involving root operations on the coefficients of the equation, though more complicated and with roots other than square roots.

Problem: Is there a solution formula of this form for **any** quintic equation: $ax^5 + bx^4 + cx^3 + dx^2 + ex + c = 0$?

Around 1830, Abel answered this question in the negative. Shortly afterwards Galois gave the complete solution for equations of any degree; and more besides. His methods exploited symmetry explicitly in a way that led to the study of groups, at least of a certain type, the so-called permutation groups.

However, perhaps the most obvious way of seeing the connection between formal group theory and the intuitive idea of symmetry that it attempts to capture is by way of geometry, as follows.

Take an equilateral triangle in space and ask how you can move it so that it appears not to have moved. This is to be the measure of its symmetry. Two motions are considered distinct if and only if their 'end effects' are different. To be more precise we number the vertices 1, 2 and 3, and consider two motions to be distinct if they produce different arrangements of the vertices in space, that is different permutations of the set $\{1, 2, 3\}$, when the triangle has apparently returned to its original position.

Take L to be a line through the vertex 1 perpendicular to the side joining vertices labelled 2 and 3 (see Figure 1.1.1).

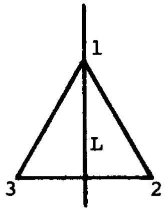


Figure 1.1.1

We consider L to be fixed in space and move the triangle about it. We consider two basic motions.

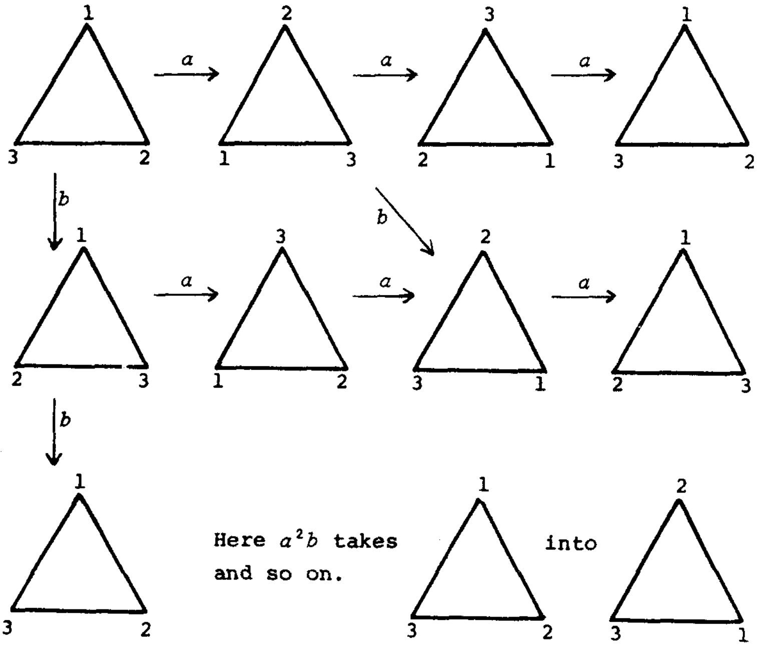
(1) A rotation about an axis perpendicular to the plane of the triangle in an anti-clockwise sense through 2π/3 radians. Denote this motion by the symbol a.

(2) A rotation about the axis L through π radians. Denote this motion by the symbol b.

We write ab to denote the motion b followed by the motion a. We write b^2 to denote b followed by b, and so on.

The reader may find it convenient to cut an equilateral triangle out of cardboard in order to carry out the following manipulations. This avoids the tedium of making countless drawings.

We consider the effect of each of the following motions on the triangle in its starting position as shown in Figure 1.1.1 a, a^2, a^3, b, b^2, ab, a^2b, a^3b, ba. The results are shown in Figure 1.1.2.



Here a^2b takes into and so on.

Figure 1.1.2

In this way we obtain the 6 possible permutations on the set {1, 2, 3} of vertices of the triangle. Since we cannot get any more permutations, we must have obtained all possible distinct motions of the triangle in space which leave it apparently fixed in space.

From a given starting position we have obtained all possible permutations on the vertices and hence all possible symmetries of the triangle, using just the motions a and b. In fact there are 6 possible motions, as measured by their effects, namely: a, a^2, b, ab, a^2b, and $a^3 = b^2 = e$, where we use e to denote the identity motion; that is the motion leaving the triangle fixed.

As is customary in modern mathematics we wish to express the above procedure of treating symmetry in an axiomatic form; that is a form which does not depend on the particular example that we have used in our discussion. To this end we consider the essential ideas involved in our discussion of the symmetry of the equilateral triangle.

The symmetry appears to be described by 6 motions symbolised by a, a^2, b, ab, a^2b, and $a^3 = b^2 = e$; and the way in which these 6 motions can be combined in a kind of product. For example: a^2b followed by ab has the same effect (starting from the same initial position, such as that in Figure 1.1.1) as a^2.

We can represent this by writing $ab.a^2b = a^2$.

In order to express this in an abstract way we need:

(1) a set G (of motions)

(2) a product defined on G; that is a rule which assigns a unique element z of G to a given ordered pair of elements x, y of G. In other words, we want a binary operation on G.

This is often expressed by saying that there is a function f: $G \times G \to G$, where $f((x, y)) = z$. We shall write $f((x, y)) = xy$.

But this is not enough. We also need some axioms telling us how the product behaves. For example, if we were talking about a product of integers, then we would expect to have an axiom which said:

$$x(yz) \quad = \quad (xy)z$$

Because, if x, y and z are interpreted as integers and xy is the usual product of x and y, then the associative rule holds; in particular with $x = 3$, $y = 7$, $z = 2$, we have: $3 \times (7 \times 2) = (3 \times 7) \times 2$.

Our next task, therefore, is to find the rules which govern the behaviour of the product in our case. Now for us $x(yz)$ means the motion z followed by the motion y and then the result followed by the motion x. This is exactly the same as $(xy)z$. Thus, $(xy)z = x(yz)$. Hence we want the associative rule just as for the usual product of integers.

For integers, $xy = yx$, but we note that in our case $ab \neq ba$. Hence the commutative rule does not hold for us. However, in our way of using motions to express the symmetry of an object in space, it is clear that we must always have an identity motion, as represented by the symbol e in our example, with the property that $ex = x = xe$ for all x. Moreover for each motion x there must be an inverse motion which undoes the effect of x. For example, in the symmetry of the equilateral triangle $ba^2.ab = e$. Hence ba^2 undoes the effect of ab. If x den›tes the motion, then we use the symbol x^{-1} to denote the motion which undoes the effect of x. We call x^{-1} the inverse of x. From $x^{-1}.x = e = x.x^{-1}$ we deduce that if x^{-1} is the inverse of x, then x is the inverse of x^{-1}.

Putting together the various parts of the above discussion we arrive at the following attempt at an abstract formulation of the intuitive notion of symmetry.

1.2 <u>The Definition of a Group</u>

A <u>group</u> consists of:

(1) a set G,

(2) a product on G, where xy denotes the product

of the elements x and y of G; together with the following axioms.

(3) The associative rule $x(yz) = (xy)z$ holds for all $x, y, z \in G$.

(4) There exists e in G with the property that $ex = x = xe$ for all x in G. (e is unique and is called the identity of G. The proof of uniqueness is in Exercise 1.1.)

(5) To each $x \in G$ there exists x' in G with the property that $x'x = e = xx'$. (x' is unique and is called the inverse of x. The proof of uniqueness is in Exercise 1.1. Once uniqueness is established the inverse of x can be given a special symbol, namely x^{-1}.)

If we have also:

(6) $xy = yx$ for all $x, y \in G$, we call G an abelian or commutative group.

If G has a finite number of elements it is called a finite group, otherwise it is an infinite group.

Note: (1) Unless otherwise stated, e will always be used to denote the identity of the group.

(2) Indices are defined as follows:

$x^0 = e$, $x^n = x\,x\,x \ldots x$ (n factors), $x^{-n} = (x^{-1})^n$, $n > 0$. By the uniqueness of the inverse, $(x^n)^{-1} = (x^{-1})^n$.

We leave the reader to check that the usual laws of indices hold.

The group concept attempts to make precise our intuitive notion of symmetry. In fact, the above axioms 3, 4, 5 assert more than is actually required to define a group. This question is taken up in Exercises 1.2 and 1.3.

1.3 The General Associative Law

This law asserts that we can insert brackets in any way that makes sense in the product of $n \geq 3$ elements of the group without affecting the value of the product. For example:

$$((ab)c)(d(gf)) \quad = \quad (a((bc)(dg)))f \quad .$$

PROOF The required result is true when $n = 3$. This is just the ordinary associative law.

Suppose the result is true for products of less than n elements. We consider a product of n elements. Suppose it has been calculated in one way to give a final product of 2 factors:

$$(a_1a_2 \dots a_r)(a_{r+1}a_{s+2} \dots a_n)$$

and in another way to give a product of the 2 factors:

$$(a_1a_2 \dots a_s)(a_{s+1}a_{s+2} \dots a_n) \quad .$$

Let $r \leq s$. Notice that the products within each bracket involve less than n factors so are well-defined whatever the positions of the brackets within them. If $r = s$, the required result follows at once. If $r < s$, since $s < n$, we can write:

$$\begin{aligned}(a_1a_2 \dots a_s)(a_{s+1} \dots a_n) \quad &= \quad ((a_1a_2 \dots a_r)(a_{r+1} \dots a_s))(a_{s+1} \dots a_n \\ &= \quad (a_1a_2 \dots a_r)((a_{r+1} \dots a_s)(a_{s+1} \dots a_n) \\ &\qquad \text{by ordinary associativity,} \\ &= \quad (a_1a_2 \dots a_r)(a_{r+1} \dots a_n) \quad .\end{aligned}$$

Thus the required result holds for products of n elements if it holds for products of less than n elements. An appeal to induction completes the proof.

1.4 Further Examples of Groups

We derived the concept of a group from our consideration of the symmetry of the equilateral triangle. At the moment this provides us with our only example of a group. Let us pause for a moment to remedy this.

We leave the reader to check that the following are indeed examples of groups.

(1) The set of all non-singular $n \times n$ matrices over the real numbers under ordinary matrix multiplication. This is called the general linear group of degree n over $\underline{\mathbf{R}}$ and is denoted by $GL_n(\underline{\mathbf{R}})$ (see [G].)

(2) The set of integers under addition. This group is abelian and is denoted by $(\underline{\mathbf{Z}}, +)$.

(3) The set of residue classes of integers modulo n under addition, denoted by $(\underline{\mathbf{Z}}_n, +)$. This group is constructed as follows.

Take $\underline{\mathbf{Z}}$ and define on it an equivalence relation $\equiv$ as follows. $a \equiv b$ if and only if n divides $a - b$, written $n \mid (a - b)$.

The equivalence class containing a we write as $\bar{a}$. We define addition of classes by $\bar{a} + \bar{b} = \overline{(a + b)}$.

The reader should check that this is a valid definition bearing in mind that $\bar{a} = \bar{a}'$, whenever $n \mid (a - a')$, and that our definition has been given in terms of particular elements of the equivalence classes involved.

(4) The set $\{\bar{1}, \bar{2}, \bar{3}, \ldots, \overline{(p - 1)}\}$ of non-zero elements of $\underline{\mathbf{Z}}_p$, the set of residue classes of integers modulo a prime p, under the multiplication: $\bar{a}.\bar{b} = \overline{(ab)}$.

This group is denoted by $\underline{\mathbf{Z}}_p^* = (\underline{\mathbf{Z}}_p - \{\bar{0}\}, .)$. Here $\underline{\mathbf{Z}}_p - \{\bar{0}\}$ means the set $\underline{\mathbf{Z}}_p$ less the zero $\bar{0}$. If $p = 5$, we have:

$$\underline{\mathbf{Z}}_p^* = (\underline{\mathbf{Z}}_5 - \{\bar{0}\}, .) = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$$

(5) The set $\{1, i, -1, -i\}$ under the usual product of complex numbers. Note that all members of this group may be written in terms of i as follows: $\{i, i^2, i^3, i^4\}$. Such a group is said to be cyclic. All its members are powers of a single member.

(6) The set of 2 × 2 matrices:

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\}$$

under the usual multiplication of matrices.

(7) If F is a field then $F^* = F - \{0\}$ is a group under the multiplication in the field F (see (4) above).

(8) Let F be any field. Then F is a group under the addition in the field. We denote this group by $(F, +)$.

1.5 Aims

In any science one of the major preoccupations is the classification of the objects of study. Another preoccupation is the investigation of structure; that is the way in which the objects of interest are constructed from simpler objects and how this affects their properties.

In group theory the object of study is the group. Hence the major aims of group theory are to classify the different types of group and to see how groups can be constructed from other groups which are simpler according to some well-defined criteria.

However, in a short introductory book like this, we can treat only a few elementary cases. Some of these will be discussed in the text, others will occur in exercises. In the course of following these aims many ideas, methods, and results will be considered which will prove useful in the applications of group theory to other branches of mathematics and to other sciences.

Let us return now to a closer study of the symmetry group of the equilateral triangle. This study will provide us with some basic ideas and techniques which will enable us to answer immediately the problem of classification for groups which have 1, 2, 3, or 4 elements.