Derek J. S Robinson

A Course in the Theory of Groups

Derek J. S. Robinson

A Course in the Theory of Groups

Springer-Verlag
New York Heidelberg Berlin

Derek J. S. Robinson

Department of Mathematics
University of Illinois at Urbana-Champaign
Urbana, Illinois 61801

AMS Subject Classification (1980): 20-01

Library of Congress Cataloging in Publication Data
Robinson, Derek John Scott.
A course in the theory of groups.
(Graduate texts in mathematics; v. 80)
Bibliography: p.
Includes index.
1. Groups, Theory of. I. Title. II. Series: Graduate
texts in mathematics; 80.
QA171.R568 512'.22 81-8881
AACR2

Printed in the United States of America

9 8 7 6 5 4 3 2 1

ISBN 0-387-90600-2 Springer-Verlag New York Heidelberg Berlin
ISBN 3-540-90600-2 Springer-Verlag Berlin Heidelberg New York

Preface

"A group is defined by means of the laws of combinations of its symbols," according to a celebrated dictum of Cayley. And this is probably still as good a one-line explanation as any. The concept of a group is surely one of the central ideas of mathematics. Certainly there are a few branches of that science in which groups are not employed implicitly or explicitly. Nor is the use of groups confined to pure mathematics. Quantum theory, molecular and atomic structure, and crystallography are just a few of the areas of science in which the idea of a group as a measure of symmetry has played an important part.

The theory of groups is the oldest branch of modern algebra. Its origins are to be found in the work of Joseph Louis Lagrange (1736–1813), Paulo Ruffini (1765–1822), and Evariste Galois (1811–1832) on the theory of algebraic equations. Their groups consisted of permutations of the variables or of the roots of polynomials, and indeed for much of the nineteenth century all groups were finite permutation groups. Nevertheless many of the fundamental ideas of group theory were introduced by these early workers and their successors, Augustin Louis Cauchy (1789–1857), Ludwig Sylow (1832–1918), Camille Jordan (1838–1922) among others.

The concept of an abstract group is clearly recognizable in the work of Arthur Cayley (1821–1895) but it did not really win widespread acceptance until Walther von Dyck (1856–1934) introduced presentations of groups.

The stimulus to study infinite groups came from geometry and topology, the influence of Felix Klein (1849–1925), Sophus Lie (1842–1899), Henri Poincaré (1854–1912), and Max Dehn (1878–1952) being paramount. Thereafter the standard of infinite group theory was borne almost single-handed by Otto Juljevič Schmidt (1891–1956) until the establishment of the Russian school headed by Alexander Gennadievič Kuroš (1908–1971).

In the meantime the first great age of finite group theory had reached its apogee in the period immediately before the First World War with the work of Georg Frobenius (1849–1917), William Burnside (1852–1927), and Issai Schur (1875–1936). After 1928, decisive new contributions were made by Philip Hall, Helmut Wielandt, and, in the field of group representations, Richard Dagobert Brauer (1901–1977). The present intense interest in the classification of finite simple groups is very largely the legacy of their work.

This book is intended as an introduction to the general theory of groups. Its aim is to make the reader aware of some of the main accomplishments of group theory while at the same time providing a reasonable coverage of basic material. The book is addressed primarily to the student who wishes to learn the subject, but it is hoped that it will also prove useful to specialists in other areas as a work of reference.

An attempt has been made to strike a balance between the different branches of group theory, abelian groups, finite groups, infinite groups, and to stress the unity of the subject. In choice of material I have been guided by its inherent interest, accessibility, and connections with other topics. No book of this type can be comprehensive, but I hope it will serve as an introduction to the several excellent research level texts now in print.

The reader is expected to have at least the knowledge and maturity of a graduate student who has completed the first year of study at a North American university or of a first year research student in the U.K. He or she should be familiar with the more elementary facts about rings, fields, and modules, possess a sound knowledge of linear algebra and be able to use Zorn's Lemma and transfinite induction. However, no knowledge of homological algebra is assumed: those homological methods required in the study of group extensions are introduced as they become necessary. This said, the theory of groups is developed from scratch. Many readers may therefore wish to skip certain sections of Chapters 1 and 2 or to regard them as a review.

A word about the exercises, of which there are some 650. They are to be found at the end of each section and must be regarded as an integral part of the text. Anyone who aspires to master the material should set out to solve as many exercises as possible. They vary from routine tests of comprehension of definitions and theorems to more challenging problems, some theorems in their own right. Exercises marked with an asterisk are referred to at some subsequent point in the text.

Notation is by and large standard, and an attempt has been made to keep it to a minimum. At the risk of some unpopularity, I have chosen to write all functions on the right. A list of commonly used symbols is placed at the beginning of the book.

While engaged on this project I enjoyed the hospitality and benefited from the assistance of several institutions: the University of Illinois in Urbana-Champaign, the University of Warwick, Notre Dame University, and the University of Freiburg. To all of these and to the National Science

Foundation I express my gratitude. I am grateful to my friends John Rose and Ralph Strebel who read several chapters and made valuable comments on them. It has been a pleasure to cooperate with Springer-Verlag in this venture and I thank them for their unfailing courtesy and patience.

University of Illinois
Urbana, Illinois
August, 1980

DEREK ROBINSON

Notation

$G, H, \ldots$	Sets, groups, rings, etc.
$\mathfrak{X}, \mathfrak{Y}$	Classes of groups
$\alpha, \beta, \gamma, \ldots$	Functions
$x, y, z, \ldots$	Elements of a set
$x\alpha$ or x^{α}	Image of x under α
x^{y}	$y^{-1}xy$
$[x, y]$	$x^{-1}y^{-1}xy$
$H \simeq G$	H is isomorphic with G
$H \leq G, H < G$	H is a subgroup, a proper subgroup of the group G.
$H \lhd G$	H is a normal subgroup of G
H sn G	H is a subnormal subgroup of G
$H_1 H_2 \cdots H_n, \prod\limits_{\lambda \in \Lambda} H_{\lambda}$	Products of subsets of a group
$\langle X_{\lambda} \mid \lambda \in \Lambda \rangle$	Subgroup generated by subsets X_{λ} of a group
$\langle X \mid R \rangle$	Group presented by generators X and relators R
$d(G)$	Minimum number of generators of G.
$r_p(G), r_0(G), r(G)$	p-rank, 0-rank, (Prüfer) rank of G

G^n, nG	Subgroup generated by all g^n or ng where $g \in G$
$G[n]$	Subgroup generated by all $g \in G$ such that $g^n = 1$ or $ng = 0$.
$\lvert S \rvert$	Cardinality of the set S
$\lvert G : H \rvert$	Index of the subgroup H in the group G
$\lvert x \rvert$	Order of the group element x
$C_G(H)$, $N_G(H)$	Centralizer, normalizer of H in G
H^G, H_G	Normal closure, core of H in G
Aut G, Inn G	Automorphism group, inner automorphism group of G
Out G	Aut G/Inn G, outer automorphism group of G
Hol G	Holomorph of G
$\mathrm{Hom}_\Omega(G, H)$	Set of Ω-homomorphisms from G to H
$\mathrm{End}_\Omega G$	Set of Ω-endomorphisms of G
$H_1 \times \cdots \times H_n, H_1 \oplus \cdots \oplus H_n$ $\operatorname*{Dr}_{\lambda \in \Lambda} H_\lambda$	Direct products, direct sums
$H \ltimes N$, $N \rtimes H$	Semidirect products
$\operatorname*{Cr}_{\lambda \in \Lambda} H_\lambda$	Cartesian product, Cartesian sum
$H \wr K$	Wreath product
$H_1 * \cdots * H_n$, $\operatorname*{Fr}_{\lambda \in \Lambda} H_\lambda$	Free products
$H \otimes K$	Tensor product
$G' = [G, G]$	Derived subgroup of a group G
G_{ab}	G/G'
$G^{(\alpha)}$	Term of the derived series of G
$\gamma_\alpha G$, $\zeta_\alpha G$	Terms of the lower central series, the upper central series of G
ζG	Centre of G

Fit G	Fitting subgroup of G
Frat G	Frattini subgroup of G
$M(G)$	Schur multiplicator of G
$O_\pi(G)$	Maximal normal π-subgroup of G
$l_\pi(G)$	π-length of G
$\mathrm{St}_G(X)$, X_G	Stabilizer of X in G
Sym X	Symmetric group on X
S_n, A_n	Symmetric, alternating groups of degree n
D_n	Dihedral group of order n
Q_{2^n}	Generalized quaternion group of order 2^n
$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$	Sets of integers, rational numbers, real numbers, complex numbers
$\mathbb{Z}_n$	$\mathbb{Z}/n\mathbb{Z}$
R^*	Group of units of a ring R with identity
RG	Group ring of a group G over a ring R with identity element
I_G, $\bar{I}_G$	Augmentation ideals
$GL(V)$	Group of nonsingular linear transformations of a vector space V
$GL(n, R)$, $SL(n, R)$	General linear and special linear groups
$PGL(n, R)$, $PSL(n, R)$	Projective general linear and projective special linear groups
$T(n, R)$, $U(n, R)$	Groups of triangular, unitriangular matrices
$B(n, e)$	Free Burnside group with n generators and exponent e
M^G, χ^G	Induced module, induced character
max, min	Maximal, minimal conditions
E_{ij}	Matrix with (i, j) entry 1 and other entries 0.

Contents

Chapter 5
Soluble and Nilpotent Groups

Chapter 6
Free Groups and Free Products

Chapter 7
Finite Permutation Groups

Chapter 8
Representations of Groups

Chapter 9
Finite Soluble Groups

Chapter 10

Chapter 11

Chapter 12

Chapter 13

Chapter 14

Chapter 1

Fundamental Concepts of Group Theory

In this first chapter we introduce the basic concepts of group theory, developing fairly rapidly the elementary properties that will be familiar to most readers.

1.1 Binary Operations, Semigroups, and Groups

A binary operation on a set is a rule for combining two elements of the set. More precisely, if S is a nonempty set, a *binary operation* on S is a function $\alpha: S \times S \rightarrow S$. Thus α associates with each ordered pair (x, y) of elements of S an element $(x, y)\alpha$ of S. It is better notation to write $x \circ y$ for $(x, y)\alpha$, referring to "$\circ$" as the binary operation.

If $\circ$ is *associative*, that is, if

(i) $(x \circ y) \circ z = x \circ (y \circ z)$ is valid for all x, y, z in S, the pair $(S, \circ)$ is called a *semigroup*.

Here we are concerned with a very special type of semigroup. A semigroup $(G, \circ)$ is called a *group* if it has the following properties.

(ii) There exists in G an element e, called a *right identity*, such that $x \circ e = x$ for all x in G.

(iii) To each element x of G there corresponds an element y of G, called a *right inverse* of x, such that $x \circ y = e$.

While it is clear how to define left identity and left inverse, the existence of such elements is not presupposed; indeed this is a consequence of the group axioms.

It is customary not to distinguish between the group $(G, \circ)$ and its underlying set G provided there is no possibility of confusion as to the intended group operation. However it should be borne in mind that there are usually several possible group operations on a given set.

The *order* of a group is defined to be the cardinality of the underlying set G. This is written $|G|$. If the group operation is *commutative*, that is, if $x \circ y = y \circ x$ is always valid, the group $(G, \circ)$ is called *abelian*.*

Before giving some standard examples of groups we shall list the most immediate consequences of the group axioms. The first of these is a generalization of the associative law to four or more elements.

1.1.1 (Generalized Associative Law). *If an element of a group is constructed from a sequence of elements $x_1, x_2, \dots, x_n$ in this order by repeatedly inserting brackets and applying the group operation, the element must equal*

$$(\dots((x_1 \circ x_2) \circ x_3) \dots) \circ x_n$$

and so is independent of the mode of bracketing.

Proof. Certainly we may assume that $n > 2$. If u is an element constructed from $x_1, x_2, \dots, x_n$ in the prescribed manner, we can write $u = v \circ w$ where v and w are constructed from $x_1, x_2, \dots, x_i$ and $x_{i+1}, \dots, x_n$ respectively $(1 \leq i < n)$. If $w = x_n$, the result follows by induction on n. Otherwise we can write $w = w' \circ x_n$ and $u = (v \circ w') \circ x_n$: once again the result follows by induction on n. □

Consequently in any expression formed from the elements $x_1, \dots, x_n$ in that order brackets can be omitted without ambiguity, an enormous simplification in notation.

1.1.2. *Let x be an element of a group G, let e be a right identity and let y be a right inverse of x. Then*

(i) $y \circ x = e$,
(ii) $e \circ x = x$,
(iii) *e is the unique left identity and the unique right identity; y is the unique left inverse of x and the unique right inverse of x.*

Proof. (i) Let $z = y \circ x$; then $z \circ z = y \circ (x \circ y) \circ x = z$ by 1.1.1. Now there is a w in G such that $z \circ w = e$. Since $z \circ z = z$, we have $z \circ (z \circ w) = z \circ w$ or $z = e$.

(ii) By (i) we have $x = x \circ e = x \circ (y \circ x) = (x \circ y) \circ x = e \circ x$.

(iii) By (ii) a right identity is a left identity. If e' is any left identity, then $e' = e' \circ e = e$. By (i) a right inverse of x is a left inverse. If t is any left inverse of x, then $t = t \circ (x \circ y) = (t \circ x) \circ y = y$. □

* After Niels Henrik Abel (1802–1829).

In view of the last result it is meaningful to speak of *the* identity of G and *the* inverse of x in G.

There are two commonly used ways of writing the group operation of a group $(G, \circ)$. In the *additive notation* $x \circ y$ is written as a "sum" $x + y$ and the identity element 0_G or 0, while $-x$ denotes the inverse of x. This notation is often used for abelian groups. We shall generally employ the *multiplicative notation* wherein $x \circ y$ is written as a "product" xy, the identity element is 1_G or 1 and x^{-1} is the inverse of x.

1.1.3. *In any (multiplicative) group the equation $xa = b$ implies that $x = ba^{-1}$ and the equation $ax = b$ implies that $x = a^{-1}b$.*

Proof. If $xa = b$, then $x = (xa)a^{-1} = ba^{-1}$: similarly for the second part. □

1.1.4. *In any group $(xy)^{-1} = y^{-1}x^{-1}$ and $(x^{-1})^{-1} = x$.*

Proof. Let $z = (xy)^{-1}$; then $xyz = 1$, whence $yz = x^{-1}$ and $z = y^{-1}x^{-1}$ by 1.1.3. Since $xx^{-1} = 1$, we have $x = (x^{-1})^{-1}$ by 1.1.3 again. □

Powers of an Element

Let x be an element of a multiplicatively written group G and let n be an integer. The nth *power* x^n of x is defined recursively in the following manner:

(i) $x^0 = 1_G$, $x^1 = x$, and x^{-1} is the inverse of x,
(ii) $x^{n+1} = x^n x$ if $n > 0$,
(iii) $x^n = (x^{-n})^{-1}$ if $n < 0$.

Naturally, if G is written additively, we shall write nx instead of x^n and speak of a *multiple* of x.

1.1.5 (The Laws of Exponents). *Let m and n be integers and let x be an element of a group G. Then*

(i) $x^m x^n = x^{m+n} = x^n x^m$,
(ii) $(x^m)^n = x^{mn} = (x^n)^m$.

Proof. (i) Let $m \geq 0$ and $n \geq 0$; then by induction on n and the definition $x^m x^n = x^{m+n}$. Applying 1.1.3 we deduce that $x^n = x^{-m}x^{m+n}$ and $x^m = x^{m+n}x^{-n}$. Finally inversion of the equation $x^m x^n = x^{m+n}$ and application of 1.1.4 yield $x^{-n}x^{-m} = x^{-m+(-n)}$. Hence the law is established in all cases.

(ii) If $n \geq 0$, it follows from the definition that $(x^m)^n = x^{mn}$. Now assume that $n < 0$; then $(x^m)^n = ((x^m)^{-n})^{-1} = (x^{-mn})^{-1} = x^{mn}$ since $x^{-mn}x^{mn} = 1$. □

Isomorphism

If G and H are groups, a function $\alpha: G \to H$ is called an *isomorphism* if it is a *bijection* (or one-one correspondence) and if $(xy)\alpha = (x)\alpha \cdot (y)\alpha$. The symbolism $G \simeq H$ signifies that there is at least one isomorphism from G to H. If $\alpha: G \to H$ is an isomorphism, an application of α to $1_G 1_G = 1_G$ shows that $1_G\alpha = 1_H$, and to $xx^{-1} = 1_G$ that $(x^{-1})\alpha = (x\alpha)^{-1}$. It is easy to prove that isomorphism is an equivalence relation on groups.

One can see from the definition that isomorphic groups have exactly corresponding underlying sets and group operations. Thus any property of a group deducible from its cardinality and group operation will be possessed by all groups isomorphic to it. For this reason one is not usually interested in distinguishing between a group and groups that are isomorphic to it.

Exercises 1.1

1. Show that a semigroup with a left identity and left inverses is a group.
2. The identity $(x_1x_2\dots x_n)^{-1} = x_n^{-1}\dots x_2^{-1}x_1^{-1}$ holds in any group.
3. If the identity $x^2 = 1$ holds in a group G, then G is abelian.
4. Show from first principles that a group of even order contains an *involution*, that is, an element $g \neq 1$ such that $g^2 = 1$.
5. The equation $(xy)^n = x^n y^n$ holds identically in a group for all n if and only if the group is abelian.

1.2 Examples of Groups

We shall now review some of the more obvious sources of groups.

(i) Groups of Numbers

Let $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ denote respectively the sets of all integers, rational numbers, real numbers, and complex numbers. Each set becomes a group if we specify ordinary addition as the group operation, zero as the identity and $-x$ as the inverse of x. The axioms of arithmetic guarantee the validity of the group axioms as well as the commutativity of the group operation. Thus all four groups are abelian.

The sets $\mathbb{Q}\backslash\{0\}$, $\mathbb{R}\backslash\{0\}$, and $\mathbb{C}\backslash\{0\}$ are groups with respect to multiplication, 1 being the identity and $1/x$ being the inverse of x. Again all the groups are abelian.