An Introduction to the Theory of Groups 4th ed

Joseph J. Rotman

An Introduction to the Theory of Groups

Fourth Edition

With 37 Illustrations

Springer

Joseph J. Rotman
Department of Mathematics
University of Illinois
at Urbana-Champaign
Urbana, IL 61801
USA

Editorial Board

S. Axler
Mathematics Department
San Francisco State
University
San Francisco, CA 94132
USA

F.W. Gehring
Mathematics Department
East Hall
University of Michigan
Ann Arbor, MI 48109
USA

K.A. Ribet
Department of Mathematics
University of California at
Berkeley
Berkeley, CA 94720-3840
USA

Mathematics Subject Classifications (1991): 20-01

Library of Congress Cataloging-in-Publication Data
Rotman, Joseph J., 1934–
An introduction to the theory of groups / Joseph Rotman. — 4th ed.
p. cm. — (Graduate texts in mathematics)
Includes bibliographical references and index.
ISBN 0-387-94285-8
1. Group theory. I. Title. II. Series.
QA174.2.R67 1994 94-6507
512'.2—dc20

Printed on acid-free paper.

© 1995 Springer-Verlag New York, Inc.
Earlier editions © 1984, 1973, and 1965 by Allyn & Bacon.
All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (Springer-Verlag New York, Inc., 175 Fifth Avenue, New York, NY 10010, USA), except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden.
The use of general descriptive names, trade names, trademarks, etc., in this publication, even if the former are not especially identified, is not to be taken as a sign that such names, as understood by the Trade Marks and Merchandise Marks Act, may accordingly be used freely by anyone.

Production coordinated by Brian Howe and managed by Bill Imbornoni;
manufacturing supervised by Gail Simon.
Typeset by Asco Trade Typesetting Ltd., Hong Kong.
Printed and bound by Sheridan Books, Ann Arbor, MI.
Printed in the United States of America.

9 8 7 6 5 4 3 2 (Corrected second printing, 1999).

ISBN 0-387-94285-8 Springer-Verlag New York Berlin Heidelberg SPIN 10728456
ISBN 3-540-94285-8 Springer-Verlag Berlin Heidelberg New York

Graduate Texts in Mathematics 148

Editorial Board
S. Axler F.W. Gehring K.A. Ribet

Springer
New York
Berlin
Heidelberg
Barcelona
Hong Kong
London
Milan
Paris
Singapore
Tokyo

Graduate Texts in Mathematics

1 TAKEUTI/ZARING. Introduction to Axiomatic Set Theory. 2nd ed.
2 OXTOBY. Measure and Category. 2nd ed.
3 SCHAEFER. Topological Vector Spaces. 2nd ed.
4 HILTON/STAMMBACH. A Course in Homological Algebra. 2nd ed.
5 MAC LANE. Categories for the Working Mathematician. 2nd ed.
6 HUGHES/PIPER. Projective Planes.
7 SERRE. A Course in Arithmetic.
8 TAKEUTI/ZARING. Axiomatic Set Theory.
9 HUMPHREYS. Introduction to Lie Algebras and Representation Theory.
10 COHEN. A Course in Simple Homotopy Theory.
11 CONWAY. Functions of One Complex Variable I. 2nd ed.
12 BEALS. Advanced Mathematical Analysis.
13 ANDERSON/FULLER. Rings and Categories of Modules. 2nd ed.
14 GOLUBITSKY/GUILLEMIN. Stable Mappings and Their Singularities.
15 BERBERIAN. Lectures in Functional Analysis and Operator Theory.
16 WINTER. The Structure of Fields.
17 ROSENBLATT. Random Processes. 2nd ed.
18 HALMOS. Measure Theory.
19 HALMOS. A Hilbert Space Problem Book. 2nd ed.
20 HUSEMOLLER. Fibre Bundles. 3rd ed.
21 HUMPHREYS. Linear Algebraic Groups.
22 BARNES/MACK. An Algebraic Introduction to Mathematical Logic.
23 GREUB. Linear Algebra. 4th ed.
24 HOLMES. Geometric Functional Analysis and Its Applications.
25 HEWITT/STROMBERG. Real and Abstract Analysis.
26 MANES. Algebraic Theories.
27 KELLEY. General Topology.
28 ZARISKI/SAMUEL. Commutative Algebra. Vol.I.
29 ZARISKI/SAMUEL. Commutative Algebra. Vol.II.
30 JACOBSON. Lectures in Abstract Algebra I. Basic Concepts.
31 JACOBSON. Lectures in Abstract Algebra II. Linear Algebra.
32 JACOBSON. Lectures in Abstract Algebra III. Theory of Fields and Galois Theory.
33 HIRSCH. Differential Topology.
34 SPITZER. Principles of Random Walk. 2nd ed.
35 ALEXANDER/WERMER. Several Complex Variables and Banach Algebras. 3rd ed.
36 KELLEY/NAMIOKA et al. Linear Topological Spaces.
37 MONK. Mathematical Logic.
38 GRAUERT/FRITZSCHE. Several Complex Variables.
39 ARVESON. An Invitation to C^*-Algebras.
40 KEMENY/SNELL/KNAPP. Denumerable Markov Chains. 2nd ed.
41 APOSTOL. Modular Functions and Dirichlet Series in Number Theory. 2nd ed.
42 SERRE. Linear Representations of Finite Groups.
43 GILLMAN/JERISON. Rings of Continuous Functions.
44 KENDIG. Elementary Algebraic Geometry.
45 LOÈVE. Probability Theory I. 4th ed.
46 LOÈVE. Probability Theory II. 4th ed.
47 MOISE. Geometric Topology in Dimensions 2 and 3.
48 SACHS/WU. General Relativity for Mathematicians.
49 GRUENBERG/WEIR. Linear Geometry. 2nd ed.
50 EDWARDS. Fermat's Last Theorem.
51 KLINGENBERG. A Course in Differential Geometry.
52 HARTSHORNE. Algebraic Geometry.
53 MANIN. A Course in Mathematical Logic.
54 GRAVER/WATKINS. Combinatorics with Emphasis on the Theory of Graphs.
55 BROWN/PEARCY. Introduction to Operator Theory I: Elements of Functional Analysis.
56 MASSEY. Algebraic Topology: An Introduction.
57 CROWELL/FOX. Introduction to Knot Theory.
58 KOBLITZ. p-adic Numbers, p-adic Analysis, and Zeta-Functions. 2nd ed.
59 LANG. Cyclotomic Fields.
60 ARNOLD. Mathematical Methods in Classical Mechanics. 2nd ed.
61 WHITEHEAD. Elements of Homotopy Theory.

(continued after index)

此为试读，需要完整PDF请访问：www.ertongbook.com

לזכרון נצח אבי מורי הנכבד
אליהו בן יוסף יונה הלוי

Preface to the Fourth Edition

Group Theory is a vast subject and, in this Introduction (as well as in the earlier editions), I have tried to select important and representative theorems and to organize them in a coherent way. Proofs must be clear, and examples should illustrate theorems and also explain the presence of restrictive hypotheses. I also believe that some history should be given so that one can understand the origin of problems and the context in which the subject developed.

Just as each of the earlier editions differs from the previous one in a significant way, the present (fourth) edition is genuinely different from the third. Indeed, this is already apparent in the Table of Contents. The book now begins with the unique factorization of permutations into disjoint cycles and the parity of permutations; only then is the idea of group introduced. This is consistent with the history of Group Theory, for these first results on permutations can be found in an 1815 paper by Cauchy, whereas groups of permutations were not introduced until 1831 (by Galois). But even if history were otherwise, I feel that it is usually good pedagogy to introduce a general notion only after becoming comfortable with an important special case. I have also added several new sections, and I have subtracted the chapter on Homological Algebra (although the section on Hom functors and character groups has been retained) and the section on Grothendieck groups.

The format of the book has been changed a bit: almost all exercises now occur at ends of sections, so as not to interrupt the exposition. There are several notational changes from earlier editions: I now write $H \leq G$ instead of $H \subset G$ to denote "H is a subgroup of G"; the dihedral group of order $2n$ is now denoted by D_{2n} instead of by D_n; the trivial group is denoted by 1 instead of by $\{1\}$; in the discussion of simple linear groups, I now distinguish *elementary transvections* from more general *transvections*; I speak of the

fundamental group of an abstract simplicial complex instead of its *edgepath group*.

Here is a list of some other changes from earlier editions.

Chapter 3. The *cycle index* of a permutation group is given to facilitate use of Burnside's counting lemma in coloring problems; a brief account of motions in the plane introduces bilinear forms and symmetry groups; the affine group is introduced, and it is shown how affine invariants can be used to prove theorems in plane geometry.

Chapter 4. The number of subgroups of order p^s in a finite group is counted mod p; two proofs of the Sylow theorems are given, one due to Wielandt.

Chapter 5. Assuming Burnside's $p^\alpha q^\beta$ theorem, we prove P. Hall's theorem that groups having p-complements are solvable; we give Ornstein's proof of Schur's theorem that $G/Z(G)$ finite implies G' finite.

Chapter 6. There are several proofs of the basis theorem, one due to Schenkman; there is a new section on operator groups.

Chapter 7. An explicit formula is given for every outer automorphism of S_6; stabilizers of normal series are shown to be nilpotent; the discussion of the wreath product has been expanded, and it is motivated by computing the automorphism group of a certain graph; the theorem of Gaschütz on complements of normal p-subgroups is proved; a second proof of Schur's theorem on finiteness of G' is given, using the transfer; there is a section on projective representations, the Schur multiplier (as a cohomology group), and covers; there is a section on derivations and H^1, and derivations are used to give another proof (due to Gruenberg and Wehrfritz) of the Schur–Zassenhaus lemma. (Had I written a new chapter entitled Cohomology of Groups, I would have felt obliged to discuss more homological algebra than is appropriate here.)

Chapter 8. There is a new section on the classical groups.

Chapter 9. An imbedding of S_6 into the Mathieu group M_{12} is used to construct an outer automorphism of S_6.

Chapter 10. Finitely generated abelian groups are treated before divisible groups.

Chapter 11. There is a section on coset enumeration; the Schur multiplier is shown to be a homology group via Hopf's formula; the number of generators of the Schur multiplier is bounded in terms of presentations; universal central extensions of perfect groups are constructed; the proof of Britton's lemma has been redone, after Schupp, so that it is now derived from the normal form theorem for amalgams.

Chapter 12. Cancellation diagrams are presented before giving the difficult portion of the proof of the undecidability of the word problem.

In addition to my continuing gratitude to those who helped with the first three editions, I thank Karl Gruenberg, Bruce Reznick, Derek Robinson, Paul Schupp, Armond Spencer, John Walter, and Paul Gies for their help on this volume.

Urbana, Illinois
1994

Joseph J. Rotman

From Preface to the Third Edition

Quand j'ai voulu me restreindre, je suis tombé dans l'obscurité;
j'ai préféré passer pour un peu bavard.

H. POINCARÉ, Analysis situs,
Journal de l'École Polytechnique, 1895, pp. 1–121.

Although permutations had been studied earlier, the theory of groups really began with Galois (1811–1832) who demonstrated that polynomials are best understood by examining certain groups of permutations of their roots. Since that time, groups have arisen in almost every branch of mathematics. Even in this introductory text we shall see connections with number theory, combinatorics, geometry, topology, and logic.

By the end of the nineteenth century, there were two main streams of group theory: topological groups (especially Lie groups) and finite groups. In this century, a third stream has joined the other two: infinite (discrete) groups. It is customary, nowadays, to approach our subject by two paths: "pure" group theory (for want of a better name) and representation theory. This book is an introduction to "pure" (discrete) group theory, both finite and infinite.

We assume that the reader knows the rudiments of modern algebra, by which we mean that matrices and finite-dimensional vector spaces are friends, while groups, rings, fields, and their homomorphisms are only acquaintances. A familiarity with elementary set theory is also assumed, but some appendices are at the back of the book so that readers may see whether my notation agrees with theirs.

I am fortunate in having attended lectures on group theory given by I. Kaplansky, S. Mac Lane, and M. Suzuki. Their influence is evident through-

out in many elegant ideas and proofs. I am happy to thank once again those who helped me (directly and indirectly) with the first two editions: K.I. Appel, M. Barr, W.W. Boone, J.L. Britton, G. Brown, D. Collins, C. Jockusch, T. McLaughlin, C.F. Miller, III. H. Paley, P. Schupp, F.D. Veldkamp, and C.R.B. Wright. It is a pleasure to thank the following who helped with the present edition: K.I. Appel, W.W. Boone, E.C. Dade, F. Haimo, L. McCulloh, P.M. Neumann, E. Rips, A. Spencer, and J. Walter. I particularly thank F. Hoffman, who read my manuscript, for his valuable comments and suggestions.

Addendum to Second Corrected Printing

Many mistakes in the first printing have been corrected in this new printing. I thank those readers, especially Hung-jen Hsu, Dae Hyun Paek, and Jack Shamash, who brought them to my attention.

February, 1999 Joseph Rotman

To the Reader

Exercises in a text generally have two functions: to reinforce the reader's grasp of the material and to provide puzzles whose solutions give a certain pleasure. Here, the exercises have a third function: to enable the reader to discover important facts, examples, and counterexamples. The serious reader should attempt all the exercises (many are not difficult), for subsequent proofs may depend on them; the casual reader should regard the exercises as part of the text proper.

此为试读,需要完整PDF请访问: www.ertongbook.com

Contents

Preface to the Fourth Edition vii

From Preface to the Third Edition ix

To the Reader xv

CHAPTER 1
Groups and Homomorphisms 1

Permutations 2
Cycles 3
Factorization into Disjoint Cycles 6
Even and Odd Permutations 7
Semigroups 10
Groups 12
Homomorphisms 16

CHAPTER 2
The Isomorphism Theorems 20

Subgroups 20
Lagrange's Theorem 24
Cyclic Groups 28
Normal Subgroups 29
Quotient Groups 32
The Isomorphism Theorems 35
Correspondence Theorem 37
Direct Products 40

CHAPTER 3
Symmetric Groups and G-Sets 43

Conjugates 43
Symmetric Groups 46
The Simplicity of A_n 50
Some Representation Theorems 51
G-Sets 55
Counting Orbits 58
Some Geometry 63

CHAPTER 4
The Sylow Theorems 73

p-Groups 73
The Sylow Theorems 78
Groups of Small Order 82

CHAPTER 5
Normal Series 89

Some Galois Theory 91
The Jordan–Hölder Theorem 98
Solvable Groups 102
Two Theorems of P. Hall 108
Central Series and Nilpotent Groups 112
p-Groups 119

CHAPTER 6
Finite Direct Products 125

The Basis Theorem 125
The Fundamental Theorem of Finite Abelian Groups 131
Canonical Forms; Existence 133
Canonical Forms; Uniqueness 141
The Krull–Schmidt Theorem 144
Operator Groups 151

CHAPTER 7
Extensions and Cohomology 154

The Extension Problem 154
Automorphism Groups 156
Semidirect Products 167
Wreath Products 172
Factor Sets 178
Theorems of Schur–Zassenhaus and Gaschütz 188
Transfer and Burnside's Theorem 193
Projective Representations and the Schur Multiplier 201
Derivations 211

CHAPTER 8
Some Simple Linear Groups 217

Finite Fields 217
The General Linear Group 219
PSL(2, K) 224
PSL(m, K) 227
Classical Groups 234

CHAPTER 9
Permutations and the Mathieu Groups 247

Multiple Transitivity 247
Primitive G-Sets 256
Simplicity Criteria 259
Affine Geometry 264
Projective Geometry 272
Sharply 3-Transitive Groups 281
Mathieu Groups 286
Steiner Systems 293

CHAPTER 10
Abelian Groups 307

Basics 307
Free Abelian Groups 312
Finitely Generated Abelian Groups 318
Divisible and Reduced Groups 320
Torsion Groups 325
Subgroups of $\mathbb{Q}$ 331
Character Groups 335

CHAPTER 11
Free Groups and Free Products 343

Generators and Relations 343
Semigroup Interlude 349
Coset Enumeration 351
Presentations and the Schur Multiplier 358
Fundamental Groups of Complexes 366
Tietze's Theorem 374
Covering Complexes 377
The Nielsen–Schreier Theorem 383
Free Products 388
The Kurosh Theorem 391
The van Kampen Theorem 394
Amalgams 401
HNN Extensions 407

CHAPTER 12
The Word Problem 418

Introduction 418
Turing Machines 420
The Markov–Post Theorem 425
The Novikov–Boone–Britton Theorem: Sufficiency of Boone's Lemma 430
Cancellation Diagrams 433
The Novikov–Boone–Britton Theorem: Necessity of Boone's Lemma 438
The Higman Imbedding Theorem 450
Some Applications 464

Epilogue 471

APPENDIX I
Some Major Algebraic Systems 475

APPENDIX II
Equivalence Relations and Equivalence Classes 477

APPENDIX III
Functions 479

APPENDIX IV
Zorn's Lemma 481

APPENDIX V
Countability 483

APPENDIX VI
Commutative Rings 485

Bibliography 495

Notation 498

Index 503

CHAPTER 1

Groups and Homomorphisms

Generalizations of the quadratic formula for cubic and quartic polynomials were discovered in the sixteenth century, and one of the major mathematical problems thereafter was to find analogous formulas for the roots of polynomials of higher degree; all attempts failed. By the middle of the eighteenth century, it was realized that permutations of the roots of a polynomial $f(x)$ were important; for example, it was known that the coefficients of $f(x)$ are "symmetric functions" of its roots. In 1770, J.-L. Lagrange used permutations to analyze the formulas giving the roots of cubics and quartics,[1] but he could not fully develop this insight because he viewed permutations only as rearrangements, and not as bijections that can be composed (see below). Composition of permutations does appear in work of P. Ruffini and of P. Abbati about 1800; in 1815, A.L. Cauchy established the calculus of permutations, and this viewpoint was used by N.H. Abel in his proof (1824) that there exist quintic polynomials for which there is no generalization of the qua-

[1] One says that a polynomial (or a rational function) f of μ variables is ***r-valued*** if, by permuting the variables in all possible ways, one obtains exactly r distinct polynomials. For example, $f(x_1, x_2, x_3) = x_1 + x_2 + x_3$ is a 1-valued function, while $g(x_1, x_2, x_3) = x_1x_2 + x_3$ is a 3-valued function.

To each polynomial $f(x)$ of degree μ, Lagrange associated a polynomial, called its *resolvent*, and a rational function of μ variables. We quote Wussing (1984, English translation, p. 78): "This connection between the degree of the resolvent and the number of values of a rational function leads Lagrange ... to consider the number of values that can be taken on by a rational function of μ variables. His conclusion is that the number in question is always a divisor of $\mu!$. ... Lagrange saw the 'metaphysics' of the procedures for the solution of algebraic equations by radicals in this connection between the degree of the resolvent and the valuedness of rational functions. His discovery was the starting point of the subsequent development due to Ruffini, Abel, Cauchy, and Galois.... It is remarkable to see in Lagrange's work the germ, in admittedly rudimentary form, of the group concept." (See Examples 3.3 and 3.3′ as well as Exercise 3.38.)

dratic formula. In 1830, E. Galois (only 19 years old at the time) invented groups, associated to each polynomial a group of permutations of its roots, and proved that there is a formula for the roots if and only if the group of permutations has a special property. In one great theorem, Galois founded group theory and used it to solve one of the outstanding problems of his day.

Permutations

Definition. If X is a nonempty set, a ***permutation*** of X is a bijection $\alpha: X \to X$. We denote the set of all permutations of X by S_X.

In the important special case when $X = \{1, 2, \ldots, n\}$, we write S_n instead of S_X. Note that $|S_n| = n!$, where $|Y|$ denotes the number of elements in a set Y.

In Lagrange's day, a permutation of $X = \{1, 2, \ldots, n\}$ was viewed as a rearrangement; that is, as a list $i_1, i_2, \ldots, i_n$ with no repetitions of all the elements of X. Given a rearrangement $i_1, i_2, \ldots, i_n$, define a function $\alpha: X \to X$ by $\alpha(j) = i_j$ for all $j \in X$. This function α is an injection because the list has no repetitions; it is a surjection because all of the elements of X appear on the list. Thus, every rearrangement gives a bijection. Conversely, any bijection α can be denoted by two rows:

$$\alpha = \begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha 1 & \alpha 2 & \ldots & \alpha n \end{pmatrix},$$

and the bottom row is a rearrangement of $\{1, 2, \ldots, n\}$. Thus, the two versions of permutation, rearrangement and bijection, are equivalent. The advantage of the new viewpoint is that two permutations in S_X can be "multiplied," for the composite of two bijections is again a bijection. For example, $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ and $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ are permutations of $\{1, 2, 3\}$. The product $\alpha\beta$ is $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$; we compute this product[2] by first applying β and then α:

$$\alpha\beta(1) = \alpha(\beta(1)) = \alpha(2) = 2,$$
$$\alpha\beta(2) = \alpha(\beta(2)) = \alpha(3) = 1,$$
$$\alpha\beta(3) = \alpha(\beta(3)) = \alpha(1) = 3.$$

Note that $\beta\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, so that $\alpha\beta \neq \beta\alpha$.

[2] We warn the reader that some authors compute this product in the reverse order: first α and then β. These authors will write functions on the right: instead of $f(x)$, they write $(x)f$ (see footnote 4 in this chapter).

此为试读,需要完整PDF请访问: www.ertongbook.com