Graduate Texts in Mathematics

148

An Introduction to the Theory of Groups

Springer-Verlag

Joseph J. Rotman

An Introduction to the Theory of Groups

Fourth Edition

With 37 Illustrations

Springer-Verlag
New York Berlin Heidelberg London Paris
Tokyo Hong Kong Barcelona Budapest

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

Production coordinated by Brian Howe and managed by Bill Imbornoni; manufacturing super vised by Gail Simon.
Typeset by Asco Trade Typesetting Ltd., Hong Kong.
Printed and bound by R.R. Donnelley & Sons, Harrisonburg, VA.
Printed in the United States of America.

9 8 7 6 5 4 3 2 1

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

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.

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.

Contents

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 $\alpha\colon X \to X$. 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 $\alpha\colon X \to X$ 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).

EXERCISES

1.1. The identity function 1_X on a set X is a permutation, and we usually denote it by 1. Prove that $1\alpha = \alpha = \alpha 1$ for every permutation $\alpha \in S_X$.

1.2. For each $\alpha \in S_X$, prove that there is $\beta \in S_X$ with $\alpha\beta = 1 = \beta\alpha$ (*Hint*. Let β be the *inverse function* of the bijection α).

1.3. For all $\alpha, \beta, \gamma \in S_X$, prove that $\alpha(\beta\gamma) = (\alpha\beta)\gamma$. Indeed, if X, Y, Z, W are sets and $f: X \to Y$, $g: Y \to Z$, and $h: Z \to W$ are functions, then $h(gf) = (hg)f$. (*Hint*: Recall that two functions $f, g: A \to B$ are equal if and only if, for all $a \in A$, one has $f(a) = g(a)$.)

Cycles

The two-rowed notation for permutations is not only cumbersome but, as we shall see, it also disguises important features of special permutations. Therefore, we shall introduce a better notation.

Definition. If $x \in X$ and $\alpha \in S_X$, then α ***fixes*** x if $\alpha(x) = x$ and α ***moves*** x if $\alpha(x) \neq x$.

Definition. Let $i_1, i_2, \ldots, i_r$ be distinct integers between 1 and n. If $\alpha \in S_n$ fixes the remaining $n - r$ integers and if

$$\alpha(i_1) = i_2, \alpha(i_2) = i_3, \ldots, \alpha(i_{r-1}) = i_r, \alpha(i_r) = i_1,$$

then α is an ***r-cycle***; one also says that α is a cycle of ***length*** r. Denote α by $(i_1\ i_2\ \cdots\ i_r)$.

Every 1-cycle fixes every element of X, and so all 1-cycles are equal to the identity. A 2-cycle, which merely interchanges a pair of elements, is called a ***transposition***.

Draw a circle with $i_1, i_2, \ldots, i_r$ arranged at equal distances around the circumference; one may picture the r-cycle $\alpha = (i_1\ i_2\ \cdots\ i_r)$ as a rotation taking i_1 into i_2, i_2 into i_3, etc., and i_r into i_1. Indeed, this is the origin of the term *cycle*, from the Greek word κύκλοσ for circle; see Figure 1.1.

Here are some examples:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1\ 2\ 3\ 4);$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 2 & 3 \end{pmatrix} = (1\ 5\ 3\ 4\ 2);$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} = (1\ 2\ 3)(4)(5) = (1\ 2\ 3).$$

Nous observerons d'abord que, si dans la substitution $\binom{A_s}{A_t}$ formée par deux permutations prises à volonté dans la suite

$$A_1, \quad A_2, \quad A_3, \quad \ldots, \quad A_N,$$

les deux termes A_s, A_t renferment des indices correspondants qui soient respectivement égaux, on pourra, sans inconvénient, supprimer les mêmes indices pour ne conserver que ceux des indices correspondants qui sont respectivement inégaux. Ainsi, par exemple, si l'on fait $n = 5$, les deux substitutions

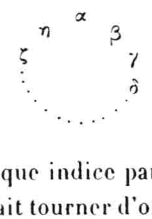
$$\begin{pmatrix} 1.2.3.4.5 \\ 2.3.1.4.5 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1.2.3 \\ 2.3.1 \end{pmatrix}$$

seront équivalentes entre elles. Je dirai qu'une substitution aura été réduite à sa plus simple expression lorsqu'on aura supprimé, dans les deux termes, tous les indices correspondants égaux.

Soient maintenant $\alpha, \beta, \gamma, \ldots, \zeta, \eta$ plusieurs des indices $1, 2, 3, \ldots, n$ en nombre égal à p, et supposons que la substitution $\binom{A_s}{A_t}$ réduite à sa plus simple expression prenne la forme

$$\begin{pmatrix} \alpha & \beta & \gamma & \ldots & \zeta & \eta \\ \beta & \gamma & \delta & \ldots & \eta & \alpha \end{pmatrix},$$

en sorte que, pour déduire le second terme du premier, il suffise de ranger en cercle, ou plutôt en polygone régulier, les indices $\alpha, \beta, \gamma, \delta, \ldots, \zeta, \eta$ de la manière suivante :



et de remplacer ensuite chaque indice par celui qui, le premier, vient prendre sa place lorsqu'on fait tourner d'orient en occident le polygone

A. Cauchy, Mémoire sur le nombre des valeurs qu'une fonction peut acquérir, lorsqu'on y permute de toutes les manières possibles les quantités qu'elle renferme, *J. de l'École Poly XVII Cahier*, tome X (1815), pp. 1–28.
From: *Oeuvres Completes d'Augustin Cauchy*, II Serie, Tome I, Gauthier-Villars, Paris, 1905.

Figure 1.1

Multiplication is easy when one uses the cycle notation. For example, let us compute $\gamma = \alpha\beta$, where $\alpha = (1\ \ 2)$ and $\beta = (1\ \ 3\ \ 4\ \ 2\ \ 5)$. Since multiplication is composition of functions, $\gamma(1) = \alpha \circ \beta(1) = \alpha(\beta(1)) = \alpha(3) = 3$; Next, $\gamma(3) = \alpha(\beta(3)) = \alpha(4) = 4$, and $\gamma(4) = \alpha(\beta(4)) = \alpha(2) = 1$. Having returned to 1, we now seek $\gamma(2)$, because 2 is the smallest integer for which γ has not yet been evaluated. We end up with

$$(1\ \ 2)(1\ \ 3\ \ 4\ \ 2\ \ 5) = (1\ \ 3\ \ 4)(2\ \ 5).$$

The cycles on the right are *disjoint* as defined below.

Definition. Two permutations $\alpha, \beta \in S_X$ are ***disjoint*** if every x moved by one is fixed by the other. In symbols, if $\alpha(x) \neq x$, then $\beta(x) = x$ and if $\beta(y) \neq y$, then $\alpha(y) = y$ (of course, it is possible that there is $z \in X$ with $\alpha(z) = z = \beta(z)$). A family of permutations $\alpha_1, \alpha_2, \ldots, \alpha_m$ is ***disjoint*** if each pair of them is disjoint.

Exercises

1.4. Prove that $(1\ \ 2\ \cdots\ r-1\ \ r) = (2\ \ 3\ \cdots\ r\ \ 1) = (3\ \ 4\ \cdots\ 1\ \ 2) = \cdots = (r\ \ 1\ \cdots\ r\ -1)$. Conclude that there are exactly r such notations for this r-cycle.

1.5. If $1 \leq r \leq n$, then there are $(1/r)[n(n-1)\ldots(n-r+1)]$ r-cycles in S_n.

1.6. Prove the ***cancellation law*** for permutations: if either $\alpha\beta = \alpha\gamma$ or $\beta\alpha = \gamma\alpha$, then $\beta = \gamma$.

1.7. Let $\alpha = (i_1\ \ i_2\ \cdots\ i_r)$ and $\beta = (j_1\ \ j_2\ \cdots\ j_s)$. Prove that α and β are disjoint if and only if $\{i_1, i_2, \ldots, i_r\} \cap \{j_1, j_2, \ldots, j_s\} = \varnothing$.

1.8. If α and β are disjoint permutations, then $\alpha\beta = \beta\alpha$; that is, α and β ***commute***.

1.9. If $\alpha, \beta \in S_n$ are disjoint and $\alpha\beta = 1$, then $\alpha = 1 = \beta$.

1.10. If $\alpha, \beta \in S_n$ are disjoint, prove that $(\alpha\beta)^k = \alpha^k\beta^k$ for all $k \geq 0$. Is this true if α and β are not disjoint? (Define $\alpha^0 = 1$, $\alpha^1 = \alpha$, and, if $k \geq 2$, define α^k to be the composite of α with itself k times.)

1.11. Show that a power of a cycle need not be a cycle.

1.12. (i) Let $\alpha = (i_0\ \ i_1\ \ldots\ i_{r-1})$ be an r-cycle. For every $j, k \geq 0$, prove that $\alpha^k(i_j) = i_{k+j}$ if subscripts are read modulo r.
(ii) Prove that if α is an r-cycle, then $\alpha^r = 1$, but that $\alpha^k \neq 1$ for every positive integer $k < r$.
(iii) If $\alpha = \beta_1\beta_2\ldots\beta_m$ is a product of disjoint r_i-cycles β_i, then the smallest positive integer l with $\alpha^l = 1$ is the least common multiple of $\{r_1, r_2, \ldots, r_m\}$.

1.13. (i) A permutation $\alpha \in S_n$ is ***regular*** if either α has no fixed points and it is the product of disjoint cycles of the same length or $\alpha = 1$. Prove that α is regular if and only if α is a power of an n-cycle β; that is, $\alpha = \beta^m$ for some m. (*Hint*: if $\alpha = (a_1 a_2 \ldots a_k)(b_1 b_2 \ldots b_k)\ldots(z_1 z_2 \ldots z_k)$, where there are m letters $a, b, \ldots, z$, then let $\beta = (a_1 b_1 \ldots z_1 a_2 b_2 \ldots z_2 \ldots a_k b_k \ldots z_k)$.)
(ii) If α is an n-cycle, then α^k is a product of (n, k) disjoint cycles, each of length $n/(n, k)$. (Recall that (n, k) denotes the gcd of n and k.)
(iii) If p is a prime, then every power of a p-cycle is either a p-cycle or 1.