Graduate Texts in Mathematics

M.I. Kargapolov
Ju.I. Merzljakov

Fundamentals of the Theory of Groups

Springer—Verlag
New York Heidelberg Berlin
World Publishing Corporation Beijing China

M.I. Kargapolov
Ju.I. Merzljakov

Fundamentals of the Theory of Groups

Translated from
the Second Russian Edition by
Robert G. Burns

Springer-Verlag
New York Heidelberg Berlin
World Publishing Corporation,Beijing,China

M.I. Kargapolov
formerly of
Institute of Mathematics
Novosibirsk, 90
U.S.S.R.

Ju.I. Merzljakov
Institute of Mathematics
Novosibirsk, 90
U.S.S.R.

Robert G. Burns
Translator
Department of Mathematics
York University
Downsview, Ontario M3J 1P3
Canada

AMS Classification: 20-01

Kargapolov, Mikhail Ivanovich.
Fundamentals of the theory of groups.
(Graduate texts in mathematics; 62)
Translation of Osnovy teorii grupp.
Bibliography: p.
Includes indexes.
1. Groups, Theory of. I. Merzliakov, IUrii
Ivanovich, joint author. II. Title. III. Series.
QA171.K3713   512'.22   79-10239

The original Russian edition *Osnovy Teorii Grupp* was
published in 1977 by Nauka, Moscow.

Reprinted in China by World Publishing Corporation
For distribution and sale in the People's Republic of China only
只限在中华人民共和国发行

ISBN 0-387-90396-8 Springer-Verlag New York
ISBN 3-540-90396-8 Springer-Verlag Berlin Heidelberg
ISBN 7-5062-0092-9 World Publishing Corporation China

Preface to the Second Edition

The present edition differs from the first in several places. In particular our treatment of polycyclic and locally polycyclic groups—the most natural generalizations of the classical concept of a finite soluble group—has been expanded.

We thank Ju. M. Gorčakov, V. A. Čurkin and V. P. Šunkov for many useful remarks.

The Authors
Novosibirsk,
Akademgorodok,
January 14, 1976.

Preface to the First Edition

This book consists of notes from lectures given by the authors at Novosibirsk University from 1968 to 1970. Our intention was to set forth just the fundamentals of group theory, avoiding excessive detail and skirting the quagmire of generalizations (however a few generalizations are nonetheless considered—see the last sections of Chapters 6 and 7). We hope that the student desiring to work in the theory of groups, having become acquainted with its fundamentals from these notes, will quickly be able to proceed to the specialist literature on his chosen topic.

We have striven not to cross the boundary between abstract and scholastic group theory, elucidating difficult concepts by means of simple examples wherever possible. Four types of examples accompany the theory: numbers under addition, numbers under multiplication, permutations, and matrices. For understanding the basic text, knowledge gained from a general course in algebra will suffice; more special facts are used at times in the examples. The examples and exercises are in part used in the basic text, so that a reading of their statements should not be omitted, nor their solution postponed for too long. Solutions are included with some of these exercises. We were guided in our nomenclature by the principle of a reasonable minimum of basic terms, which required small departures from the prevailing terminology—these are noted at the appropriate places in the text.

The bibliography contains mostly group-theoretical surveys and monographs. A few references to journal articles are given immediately in the text and in general are rather random (a complete bibliography of group theory would have several thousand entries).

In a few places unsolved problems are mentioned. A rather complete collection of such problems, reflecting the interests of a wide circle of specialists in group theory, can be found in the latest edition of the "Kourovka Notebook".

The first version of this book was published in Issues 3 and 4 of the duplicated series "Library of the Department of Algebra and Mathematical Logic of NGU". We offer heartfelt thanks to all who communicated their observations to us, in particular to Ju. E. Vapne, V. D. Marzurov, V. N. Remeslennikov, N. S. Romanovskiĭ, A. I. Starostin, S. N. Černikov, and V. A. Čurkin.

The Authors
Novosibirsk,
Akademgorodok,
February 3, 1971

Translator's Remarks

1. In his paper [Infinite groups with cyclic subgroups. Doklady Akad. Nauk SSSR **245**, No. 4 (1979)] A. Ju. Ol'šanskiĭ has announced a construction of an infinite 2-generator group all of whose proper subgroups are cyclic of prime order (where the set of primes occurring as orders is infinite). This solves at one blow Šmidt's problem (p. 14), the maximal problem (p. 137), and the minimal problem (p. 139). (Ol'šanskiĭ has also constructed a nonabelian 2-generator group, all of whose proper subgroups are infinite cyclic.) The details will appear soon in Izestija Akad. Nauk SSSR.

2. It may be useful to explain the various notations for functions (or maps) used in the text. Let S denote a set, s an element of it, and ϕ a map with domain S. The "exponential" notation S^{ϕ}, s^{ϕ} for the images of S, s, is used only when S is being considered as a multiplicatively written group, and ϕ is a homomorphism. If S is an additive group, the notation $S\phi$, $s\phi$ is used instead. If ϕ is not primarily a group homomorphism, then the notations $S\phi$, $s\phi$; $\phi(S)$, $\phi(s)$, are used variously.

In the Russian editions the authors had introduced improvements to the conventional terminology. Unfortunately, this went almost unnoticed by the translator, so that the English terminology used is more standard. There may however be some point in mentioning a few of the authors' original terms: thus, for example, they used "period" for "exponent", "automorphically invariant" for "characteristic", and a single word (meaning "step") for "class" (of nilpotency) and "length" (of solubility).

3. I take the opportunity of thanking Janis Leach for her excellent typing, and Maxine Burns and Abe Shenitzer for their kind advice and encouragement. Support from the National Research Council of Canada is also gratefully acknowledged.

R. G. Burns,
York University,
Toronto,
August 10, 1979

Introduction

Why does a square seem to us a symmetrical figure, a circle even more symmetrical, but the numeral "4" completely asymmetrical? To answer this question, let us consider the motions leaving each of these figures in the same place as before. It is easy to see that for the square there are eight such motions, for the circle infinitely many, but for the numeral "4" only one, the identity, which leaves each point of the numeral fixed. The set G of different motions leaving a given figure occupying the same space as before serves as a measure of its degree of symmetry: the more numerous the elements of G, i.e. the motions, the more symmetrical the figure. We define on the set G a rule of composition of its elements (or "operation") as follows: if x, y are two motions from G, then the result of composing them (called their "product" and written xy) is defined to be the motion equivalent to the successive application first of the motion x and then of the motion y. For example if x, y are the reflections of a square in its diagonals, then xy is the rotation about its centre through 180°. This composition of the elements of G clearly has the following properties: (1) $(xy)z = x(yz)$ for all elements x, y, z from G; (2) there exists in G an element e such that $xe = ex = x$ for all x from G; (3) for each x from G there exists an element x^{-1} in G such that $xx^{-1} = x^{-1}x = e$. In fact it is obvious that for e we may take the identical (or "trivial") motion, and for x^{-1} the motion opposite to x, i.e. returning each point of the figure from its new position to its old one.

Let us now leave aside our examples and consider an arbitrary set G on which an operation is given; i.e. for each two elements x, y in G there is defined an element xy again in G. If this operation satisfies conditions (1), (2), (3), then the set G with the given operation is called a *group*. Groups are basic among algebraic systems, and the theory of groups is basic among the various subdisciplines of modern algebra.

It required the work of several generations of mathematicians, spanning in all about a hundred years, before the concept of a group had crystallized out with its present clarity. In the context of the theory of algebraic equations the course of development of the group concept can be traced from Lagrange, who, in essence, applied groups of permutations to the solution of algebraic equations by radicals (1771), through the work of Ruffini (1799) and Abel (1824), to Évariste Galois, in whose work (1830) the group concept is used quite explicitly (it was he who first used the name). Independently, and for other reasons, the group concept made its appearance in geometry when in the mid-19th century the single geometry of antiquity gave way to a multitude of geometries, and the question arose of establishing the relationships between these new geometries and of classifying them. The answer was provided by the *Erlanger Programm* of Klein (1872), which proposed the idea of a group of transformations as the basis for a classification of geometries. A third source of the group concept was number theory; here among the instigators we mention only Euler, with his remainders (or "residues") after division of powers (1761), and Gauss with his composition of binary quadratic forms (1801).

The realization at the end of the 19th century that the group-theoretical ideas existing up till then independently in various areas of mathematics were essentially the same, led to the formation of the modern abstract concept of a group (by Lie, von Dyck, and others), and so to one of the earliest instances of an abstract algebraic system. This abstract group concept served in many ways as a model for the reworking, at the turn of the century, of other areas of algebra, and of mathematics generally: for these areas the process was then not so tortuous or difficult. The study of groups without the assumption of finiteness, and entirely without assumptions as to the nature of their elements, was formally inaugurated as an independent branch of mathematics with the appearance in 1916 of O. Ju. Šmidt's book "The Abstract Theory of Groups".

At the present time, group theory is one of the most highly developed branches of algebra, with numerous applications both within mathematics and beyond its boundaries: for instance to topology, function theory, crystallography, quantum mechanics, among other areas of mathematics and the natural sciences. In addition the theory has an independent life of its own, whose ultimate goal is the description of all possible group operations.

We shall now give some examples of applications of groups in algebra, in mathematics generally, and in the natural sciences.

1. *Galois groups*. Classical Galois theory consists in the application of group theory to the study of fields in the following way. Let K be a finite, separable and normal extension of a field k. The automorphisms of the field K leaving fixed the elements of the subfield k, form a group under composition of functions. This group is called the *Galois group* (G say) *of the extension* K/k. The fundamental theorem of Galois theory asserts that if we

associate with each subgroup $H \leq G$ its fixed subfield

$$K^H = \{x \mid x \in K, xh = x \quad \text{for all } h \in H\},$$

we obtain an anti-isomorphism of the lattice of subgroups of G onto the lattice of subfields intermediate between k and K. The field extension K^H/k will be normal if and only if the subgroup H is normal in G, and then the restriction to K^H of the automorphisms in G will yield a homomorphism, with kernel H, of the group G onto the Galois group of the extension K^H/k.

The application to the question of the solubility of equations by radicals can then be described as follows. Let f be a polynomial in x over the field k, and K the splitting field of f. Let G be the Galois group of the extension K/k. This group is also called the *Galois group of the polynomial* f over the field k. (Its elements are represented in the natural way as permutations of the roots of the equation $f(x) = 0$.) It turns out that the equation $f(x) = 0$ is soluble by radicals if and only if the Galois group of the polynomial f is soluble.

Analogous to Galois theory is the Picard-Vessiot theory in which groups are used to study extensions of differential rings and where, in particular, the question of the solubility by quadratures of differential equations is resolved. The role which in Galois theory is played by permutation groups, is in the Picard–Vessiot theory assumed by algebraic groups of matrices.

In these examples groups arise as groups of automorphisms of mathematical structures. Not only is this one of the most important ways in which they occur, but also, generally speaking, this guise is peculiar to groups and secures for them a special position in algebra. The reason for this is that one may always, in the words of Galois, "group" the automorphisms of any structure, while it is only in special cases that a ring structure or some other useful structure can be defined conveniently on the set of automorphisms.

2. *Homology groups.* The central idea of homology theory involves the application of the theory of (abelian) groups to the study of the category of topological spaces. With each space X is associated a sequence of abelian groups $H_0(X), H_1(X), \ldots$, and with each continuous map $f: X \to Y$, a sequence of homomorphisms $f_n: H_n(X) \to H_n(Y)$, $n = 0, 1, 2, \ldots$. The study of the homology groups $H_n(X)$ and their homomorphisms by the methods of group theory often allows the solution of problems originally topological in nature. A typical example is the extension problem: Can a map $g: A \to Y$, defined on a subspace A of the space X be extended to all of X; i.e. can g be expressed as the composite of the inclusion map $h: A \to X$, and some continuous map $\hat{g}: X \to Y$? If the answer is yes, then by homology theory we must have $g_n = \hat{g}_n h_n$, i.e. each homorphism $g_n: H_n(A) \to H_n(Y)$, can be factored through $H_n(X)$, with the factor h_n given. If this algebraic problem has a negative solution then, according to the theory, so does the original topological problem.

With this method important positive results can be obtained. By way of illustration we sketch a proof of Brouwer's fixed-point theorem: Every continuous map f of the n-dimensional ball E^n to itself has a fixed point. Suppose, on the contrary, that $f(x) \neq x$ for all $x \in E^n$. Suppose the half-line beginning at $f(x)$ and passing through the point x meets the sphere S^{n-1} (the boundary of E^n) at the point $g(x)$. Obviously g is continuous, and restricts to the identity map on S^{n-1}. Therefore the identity map on S^{n-1} can be extended to a continuous map $E^n \to S^{n-1}$. For $n = 1$ this gives a contradiction at once. If for $n \geq 2$ we compute the homology groups with coefficients from the group $\mathbf{Z}$ of integers, we find that $H_{n-1}(E^n) = 0, H_{n-1}(S^{n-1}) = \mathbf{Z}$, $h_{n-1} = 0$, $g_{n-1} = 1$, whence it is clear that the answer to the corresponding algebraic problem is in the negative, yielding a second, and final, contradiction.

This example from homology theory illustrates a typical mode of application of algebra (in particular group theory) to the study of non-algebraic objects: propeities of the latter are elicited with the aid of algebraic systems (in particular groups) which mirror some of their structure. Such is the basic technique of algebraic topology. In the last few decades analogous techniques have been evolved, and used successfully, for studying algebraic systems themselves (for example in the theory of group extensions).

3. *Symmetry groups.* As mentioned above, the group concept allows us to give a precise meaning to the formerly slightly vague idea of the symmetry of a geometrical figure. Using this sort of approach E. S. Fedorov (1890) solved the problem, fundamental for crystallography, of classifying the regular arrangements, or lattices, of points in the Euclidean plane and in space. There turned out to be altogether just 17 planar Fedorov groups, which he discovered immediately, and 230 spatial Fedorov groups, the exhaustive classification of which relied in an essential way on group theory. This represented the first direct application of group theory to the natural sciences.

Group theory plays an analogous role in physics. Thus in quantum mechanics the state of a physical system is represented by a point of an infinite-dimensional vector space. If the system undergoes a change of state then its representing point is subjected to a certain linear transformation. Here, in addition to considerations of symmetry, the theory of representations of groups by linear transformations is important.

These examples illustrate the classifying role played by groups wherever symmetry is involved. In questions of symmetry one is dealing essentially with automorphisms of structures (not necessarily mathematical), so that in such questions group theory is irreplaceable. In mathematics itself this classifying function is of great utility: of this Klein's *Erlanger Programm* is sufficient testimony.

To summarize: the group concept, fundamental in modern mathematics, is a highly versatile tool for mathematics itself: it is used as an important constituent of many algebraic systems (e.g. rings, fields), as a sensitive register of the properties of various topological objects, as a proving-ground for the theory of algorithmic decidability, and in many other ways. It provides, in addition, a sensitive instrument for investigating symmetry, one of the most pervasive and elemental phenomena of the real world.

We conclude by listing some of the more important classes of groups.

The oldest branch of group theory, which is nonetheless developing as intensively now as it ever did in the past, is the theory of finite groups. In this theory the predominant activity at present is the search for finite *simple* groups: these embrace many of the classical groups of matrices over fields, several series of groups of automorphisms of Lie algebras, and certain isolated, "sporadic" groups. At the opposite end of the spectrum we have the finite *soluble* groups, where interest is usually concentrated on specific systems of subgroups (Hall, Carter subgroups, etc.), determining in large measure the structure of the group itself. Finite groups often arise as groups of permutations, or as matrices over finite fields; a large, and to some extent independent, segment of finite group theory occupies itself with the study of representations of groups by permutations and matrices.

In the theory of infinite groups the technique of broadest application consists in the imposition of one or another "finiteness condition". Among the classes resulting from the myriad such conditions the following come in for most attention: periodic groups, locally finite groups, groups with the maximal condition on subgroups, groups with the minimal condition on subgroups, finitely generated groups, groups of finite rank, and residually finite groups.

In abelian group theory the leading roles are played by the classes of: divisible abelian groups, torsion-free abelian groups, and by periodic abelian groups and their pure and primary subgroups. The study of general abelian groups reduces in large measure to applications of the theories of these particular classes and the theory of extensions of abelian groups, the methodology of which is largely homological in nature.

The classes of nilpotent and soluble groups, larger than that of abelian groups, can also boast of highly developed theories. Of the teeming generalizations of nilpotence and solubility we mention only: local nilpotence, the normalizer condition, the Engel condition, and the multitude of classes of groups defined by the possession of a subnormal system of one kind or another.

Several important classes of groups are obtained by imposing additional structures linked in some way to the group operation. Under this head fall, for instance, topological groups, Lie groups, linear groups and orderable groups.

Of the remaining classes we make mention of only: groups free in some variety, divisible (non-abelian) groups, groups having some property residually, automorphism groups of various mathematical structures, groups determined by conditions on their generators and defining relations, and groups with prescribed subgroup-lattices.

Contents

Chapter 3

Abelian Groups

Chapter 4

Finite Groups

Chapter 5

Free Groups and Varieties

Chapter 6

Nilpotent Groups

Definition and Most Important Subsets of a Group 1

§1. Definition of a Group

1.1. Axioms. Isomorphism

Every mathematical theory reduces ultimately to the study of two kinds of objects: sets and functions on sets. If the arguments of a function f run through a set M, in which the function also takes its values, then f is called an *algebraic operation* on M. That study which concerns itself with algebraic operations is called *algebra*. Viewed this way, algebra is concerned only with how one or another algebraic operation acts, and not at all with the set on which it is defined. The concept of isomorphism allows us to shift attention from the second of these concerns and concentrate on the first. Suppose two sets are given, together with one or more operations on each, and that there is a one-to-one correspondence between the sets themselves, and also between the sets of operations on them, such that corresponding operations are functions of the same number of variables and take corresponding values when the variables are assigned corresponding values. The sets with their operations are then said to be *isomorphic*. Isomorphic objects have identical structures as far as their operations are concerned, so that in algebra they are either not distinguished or else are regarded as exact copies of each other—much as we regard copies of a novel as being the same, even though printed with different types and on different paper, if we are interested only in the content. It makes sense to regard each class of isomorphic objects as exactly determining a certain type of algebraic operation. This reduces the problem of algebra—the study of algebraic operations—to the more concrete problem of the study of sets with operations with accuracy only up to isomorphism.

Certain kinds of algebraic operation are met with so frequently in mathematics that they have become the objects of study of independent theories. One such is the operation defining the group concept—the object of study of the theory of groups. A group is a set with one binary (i.e. two-variable) operation, satisfying certain axioms. The value of a binary operation f on a pair of elements x, y is more conveniently written, not as $f(x, y)$ as for other functions, but as xfy—this notation economises on symbols and accords well with the usual notation for numerical operations: after all we write $2+3=5$, and not $+(2, 3)=5$. In a group the binary operation is generally called multiplication and denoted by a dot (which is almost always omitted); more rarely, $+$, $\circ$, $*$, and other symbols are used. The dot notation is sometimes also referred to as the multiplicative notation, while that employing the plus sign is called the additive notation.

1.1.1. Definition. A set G with a binary operation $\cdot$ is called a *group*, if:

1. the operation is *associative*; i.e. $(ab)c = a(bc)$ for all a, b, c in G;
2. the operation guarantees an identity element; i.e. in G there is an element e—called the *identity element*—such that $ae = ea = a$ for all a in G;
3. the operation guarantees inverse elements; i.e. for each a in G there is in G an element x—called the *inverse* of a—such that $ax = xa = e$.

1.1.2. Definition. A set G with binary operation $\cdot$ is called a *group*, if

1. the operation is associative;
2. the operation guarantees left and right quotients; i.e. for each pair of elements a, b in G there are G elements x, y—called respectively *left* and *right quotients* of b by a—such that $ax = b$, $ya = b$.

1.1.3. Exercise. Definitions 1.1.1 and 1.1.2 are equivalent. The identity element of any group G is unique. Each element a in G has a unique inverse (denoted by a^{-1}). For each pair of elements a, b in G both quotients of b by a are unique. (We write $a\backslash b$ for the left quotient, and b/a for the right quotient.)

In accordance with the usual group-theoretic terminology we call a one-to-one product preserving mapping ϕ from one group onto another an *isomorphism*. In other words a map from a group G to a group G^* (in symbols $\phi: G \to G^*$) is an isomorphism, if, firstly, distinct elements have distinct images; i.e. writing a^ϕ for the image of a under the map ϕ,

$$a^\phi \neq b^\phi \text{ whenever } a \neq b, \qquad a, b \in G,$$

secondly, every element of G^* has the form g^ϕ for some $g \in G$, and, finally, the image of a product is the product of the images;

$$(ab)^\phi = a^\phi b^\phi.$$

The two groups are then said to be *isomorphic* (in symbols $G \simeq G^*$).

For example, the set G of positive real numbers is a group under the usual multiplication of numbers; the set G^* of all real numbers is a group under the usual addition of numbers; and the map $\phi: G \to G^*$, defined by the formula $a^\phi = \log a$, is an isomorphism between G and G^*. When we use a logarithmic slide-rule we are simply reaping the benefits of this isomorphism. The concern of group theory is to study group operations, or, what amounts to the same thing, groups up to isomorphism. The theory of groups would be complete once a catalogue of all possible groups up to isomorphism were compiled. Happily for group theory, but unhappily for its applications, the compilation of such a catalogue is in practice impossible.

1.2. Examples

Thanks to the associative law for groups the element $(ab)c = a(bc)$ may be written simply as abc; for the same reason the product $a_1 a_2 \cdots a_n$ of n elements—without bracketing but in the given order—is uniquely defined. The product of n elements all equal to a is called the *nth power* of the element a, and is denoted by a^n. For zero and negative integers n we define $a^0 = e$, $a^n = (a^{-n})^{-1}$ or $a^n = (a^{-1})^{-n}$, which as it is easy to see, are equivalent.

1.2.1. Exercise. If a is any element of a group and m, n are integers, then $a^m a^n = a^{m+n}$, $(a^m)^n = a^{mn}$.

It may happen that $a^n = e$ for some $n > 0$, in which case, if $a \neq e$, the smallest n with this property is called the *order* or *period* of the element a and is denoted by $|a|$. If $a^n \neq e$ for every $n > 0$, the element a is ascribed infinite order and we write $|a| = \infty$.

1.2.2. Exercise. If $a^n = e$ then $|a|$ divides n.

1.2.3. Exercise. If the elements a, b commute, i.e. $ab = ba$, and their orders are relatively prime, then $|ab| = |a| \cdot |b|$.

1.2.4. Exercise. Suppose elements a, b commute and have orders m, n. Then the group contains an element—not always the product ab—whose order is the lowest common multiple of m and n.

We say that a group G is *torsion-free* if every nonidentity element of G has infinite order. If on the other hand every element of G has finite order then we say that G is *periodic*. If the orders of all the elements of a periodic group are bounded, then the lowest common multiple of their orders is called the *exponent* of the group. Let p be a prime. If the orders of all the elements of a periodic group are powers of p, then we call the group a *p-group*. The cardinal $|G|$ of the group G is called the *order* of G. If this cardinal is finite then we say that the group is *finite*; and in the contrary case *infinite*. If the operation in the group G is commutative, i.e. $ab = ba$ for all a, b in G, then it