THE THEORY OF GROUPS

THE THEORY OF GROUPS

BY

A. G. KUROSH

TRANSLATED FROM THE RUSSIAN
AND EDITED BY

K. A. HIRSCH

VOLUME ONE

SECOND ENGLISH EDITION

CHELSEA PUBLISHING COMPANY
NEW YORK, N. Y.

The present work, published in two volumes, is a translation into English, by K. A. Hirsch, of the second Russian edition of the book TEORIYA GRUPP by A. G. Kuroš, with supplementary material by the translator

Library of Congress Catalog Card Number 60-8965

Printed in the United States of America

TRANSLATOR'S PREFACE

The book *Teoriya Grupp* by Professor A. G. Kuroš has been widely acclaimed as the first modern text on the general theory of groups, with the major emphasis on infinite groups. An English translation of the work was, therefore, highly desirable. When I got in touch with the author and learned that the first Russian edition was out of print and that he was actively engaged in the preparations for a completely rewritten second edition, I decided to postpone my translation until the new book became available. This explains the delay between the first announcement and the actual issue of the present volume. (A German translation of the first Russian edition was published in 1953 by the Akademie-Verlag, Berlin.)

In this translation I have followed the time-honoured maxim: "As literally as possible and as freely as necessary." Thus, while the book should read like an English text-book, it has, I hope, retained some of the flavour of the Russian original. A characteristic feature that the reader will notice is the author's sparing use of an elaborate symbolism and his reliance on a full verbal exposition of the mathematical argument.

The changes I have made in the text can be described briefly as follows:

(i) Throughout the text I have distinguished between $g \in G$ ("g is an element of G") and $H \subset G$ ("H is contained in G"). This distinction is not made in the Russian text, where the symbol $\subset$ is used in both meanings. Frequently I have changed the notation for certain subgroups, elements, subscripts, indices, etc. to bring it into line with English usage.

(ii) I have slightly altered a few definitions (such as that of a free product and that of an element of infinite height) in order to avoid cumbersome case distinctions and to achieve more concise statements of some theorems.

(iii) I have eliminated a number of misprints of the Russian text and have removed a few minor slips. Occasionally I have recast a proof where I thought it would lead to greater clarity.

(iv) The appendix notes, which are marked in the text by sans-serif superior letters, contain a few additional remarks and some references to recent developments. This applies particularly to Parts Three and Four of the book, which are concerned with topics where progress is most rapid at present.

(v) I have tried to keep the bibliography up to date by adding to Volume II a separate list of references to relevant group-theoretical literature of the last few years.

I may mention that the recent monograph by I. Kaplansky, *Infinite Abelian Groups* (University of Michigan Press, 1954), is an excellent supplement to Part Two of this book, partly because the two books do not overlap too much in the material they cover, and partly because where they do overlap the two authors' different techniques make an interesting comparison.

As the majority of the readers is likely to be in the United States, I have at the Publisher's request adopted American usage in spelling and terminology. Thus, I talk of the center, of parentheses, and (somewhat reluctantly) of solvable groups, where in England it would have been the centre, brackets, and soluble groups.

In the advanced parts of the book there is, quite understandably, much emphasis on the work of the very vigorous Russian group-theoretical school. The author is aware of this; in a recent letter to me he writes: "The creation of the contemporary theory of groups was, and is, the work of a large world-wide community of scholars, but the task of preparing a book that reflects the contemporary state of the theory of groups cannot be solved collectively." I hope that my translation will make English readers better acquainted with the trends of research in Russia and that in this way it will make a contribution to establishing a closer contact with our Russian colleagues.

A final word about the use of the book as a text for graduate (or, in England, advanced undergraduate) courses. I believe that in the hands of an experienced instructor the book will serve admirably as a text for students who have achieved a certain maturity of mathematical thinking. The instructor may have to make a few judicious omissions (of more difficult material) and additions (of further examples and exercises). But in the theory of infinite groups good exercises of the right degree of difficulty are notoriously scarce—they tend to be either too trivial or too hard. During the last academic year, which I have spent as a Visiting Professor in the University of Colorado, at Boulder, I have covered both Part One and Part Two, each in a one-semester three-hour course.

I welcome this opportunity of expressing my thanks to the official agencies, the institutions, and the many colleagues who have helped to make my stay in the United States such a pleasant one.

August, 1955

KURT A. HIRSCH

PREFACE TO THE SECOND EDITION

The author concluded his work on the first edition of this book in 1940, the proofs were read in the following year, and only the military circumstances of the time delayed the appearance of the book until 1944. Thus, nearly twelve years have passed since the book was completed. During these years the general theory of groups has undergone a remarkable change—many problems have been solved, a number of new problems have arisen, and new directions of research have opened up, some of which now occupy a very conspicuous place in the theory of groups. In this rapid development of the theory of groups Soviet algebraists have played a prominent part. Young research workers have been systematically recruited, and continue to be recruited, into the Russian group-theoretical school, which was founded by O. J. Schmidt. Their creative interests span almost all branches of the theory of groups, and in many directions the papers of Soviet scientists are among the leading ones. The first edition of the present book has also contributed in some measure to the development of the group-theoretical studies —it might be mentioned that a typewritten copy was deposited in 1940 at the Institute for Mathematics and Mechanics of the University of Moscow and was accessible for study.

When I began to prepare the second edition two years ago, I wanted to bring the book again up to the level our science had then attained. For this purpose I had to write virtually a new book. Not only does it differ from the old one in the planning of the material—many new sections have been added and many that were taken over from the old book have been completely revised—but hardly a single section has been transferred to the new book without some alterations. On the other hand, the increase in the volume of the book, which unfortunately could not be avoided, compelled me to omit a number of points that were in the old book and occasionally entire sections; however, they were of such a nature that their inclusion in the original book cannot be regarded as having been a mistake. I have therefore found it appropriate in some cases, when referring the reader to additional literature, to refer him also to the corresponding section of the first edition of the book.

I must emphasize, however, that the new book has the old one as its basis and is very close to it in conception. This justifies me, I think, in keeping the old title for the book with the qualification "Second Edition, Revised."

I do not intend to give a complete survey of the book, but I shall point out the principal differences between its main parts and the corresponding

parts of the first edition. Part One contains what one would naturally refer to as the *elements of group theory*. A thorough acquaintance with this material is assumed in all subsequent parts of the book. I mention one detail: The concept of the factor group and the homomorphism theorem appear in the book long before the concept of a normal subgroup is introduced. This interchange is not due to the needs of group theory itself and has been made only in order to expose the triviality of those all-too-numerous generalizations of the group concept whose theory does not go much further than the homomorphism theorem. As is well known, this theorem can, in fact, be formulated and proved for sets with an arbitrary number of algebraic operations.

The *theory of abelian groups* has been subjected to a drastic revision. This refers to primary abelian groups, in particular, whose theory has been considerably reorganized and enriched by the work of L. Y. Kulikov. As far as torsion-free abelian groups are concerned, the method of presenting the groups by systems of p-adic matrices has here been omitted, as it is of little help in the study of these groups; instead, the theory of completely decomposable groups has been included.

A considerable number of significant additions has been made in the *theory of free groups and free products*. In particular, some results recently obtained by B. H. Neumann and his collaborators have been incorporated in the book.

In the *theory of direct products of groups* large re-dispositions have been undertaken; as a result of papers by the author and later by R. Baer, this theory is drawing appreciably closer to its completion. Therefore it was natural to deduce in the book the theorem of Schmidt (often also called theorem of Remak-Schmidt or Krull-Schmidt) from one of the much more general theorems obtained in recent years. This necessitated the development of a large auxiliary apparatus and compelled me to combine the chapter on direct products with the chapter on lattices.

In the first edition, only one section was devoted to *group extensions*. In the second edition it has grown into a whole chapter: this is due to the appearance of the cohomology theory in groups. Of course, even now the classification of extensions is far from having reached that degree of perfection which would allow the solving of any problem on extensions by a simple reference to this classification; but the whole position cannot be compared to what it was twelve years ago.

Particularly deep changes have occurred in the *theory of solvable and nilpotent infinite groups*. The first edition of the book reflected only the first timid steps in this direction, and the relevant sections were included

in the book more as a hint of subsequent developments than as an exposition of the results achieved at the time. To-day this is, in fact, one of the largest and richest branches of the theory of groups, a branch whose program can be expressed in these words: the study of groups which are closely related to abelian groups, under restrictions which in one sense or another are close to finiteness of the number of elements of the group.

This new branch of the theory of groups has been created almost entirely by Soviet scientists. A special place belongs to S. N. Černikov whose initiative and creative contributions have determined the development of the researches in this domain to a remarkable degree. A number of results concerning very deep theorems have also been obtained by A. I. Mal'cev.

Now a word about those parts of the theory of groups that have been omitted from the framework of the book. Among them there is above all the *theory of finite groups*. At the time when I worked on the first edition I set myself the task of showing that the theory of groups is not merely the theory of finite groups, and therefore the book contained almost nothing about finite groups in particular. This task can be regarded today as accomplished. Indeed, just the other way around: it has now become necessary to recall that the theory of finite groups is an important and integral part of the general theory of groups. Although some material on finite groups is now incorporated in this book, the above problem is by no means solved in it.

It would be useful if one of the Soviet specialists on finite groups would write a small book devoted entirely to finite groups using the present book as a basis (that is, without expounding the elements of group theory over again).

Even more urgent, perhaps, would be the writing of a book whose title could be given provisionally as *the algebraic theory of groups of transformations*. It would have to contain the well-worked theory of permutation groups, the theory of groups of matrices, and also the general theory of representations of abstract groups. Isomorphic representations of groups by matrices, monomial groups and representations, the classical groups over an arbitrary field, and many other topics would also have to find a place in it. In a certain sense this is applied theory of groups. A systematic exposition of this entire branch of the theory of groups, using the results and methods of the general theory of groups, would be very useful.

The prerequisite knowledge that the reader of the book is assumed to possess has been indicated at the end of the Introduction to the First Edition. In addition, I might add that he should be acquainted with the concept of a ring and the simplest concepts connected with it.

The bibliography has been revised, and supplemented by those papers published in recent years that have a bearing on the contents of the book.

Before and during the work on the second edition I received many comments and much advice—in letters, in personal talks, and in seminar meetings—from many Soviet algebraists. To all these fellow-mathematicians who have helped me with their advice I offer my sincere thanks.

Moscow, May 1952

A. KUROŠ

FROM THE INTRODUCTION TO THE FIRST EDITION

The theory of groups has a long and rich history. Arising from the needs of Galois theory, it developed at first as the theory of finite substitution groups (Cauchy, Jordan, Sylow). However, it was fairly soon discovered that for the majority of problems that are of interest to the theory this special material—namely substitutions—used in the construction of the groups is not essential and that the actual topic is the study of properties of a single algebraic operation defined in a set consisting of a finite number of elements of an arbitrary nature. This discovery, which may appear trivial to-day, turned out to be, in fact, very fruitful and led to the creation of the general theory of finite groups. True, the transition from substitution groups to arbitrary finite groups did not essentially extend the realm of the objects to be studied; however, it put the theory on an axiomatic basis, gave it order and clarity, and thus facilitated its further growth.

The golden age of the theory of finite groups came at the end of the last century and the first decade of the present. During this period the fundamental results of the theory were obtained, the fundamental directions of research were laid down, and the fundamental methods were created; generally, through the work of its principal promoters (Frobenius, Hölder, Burnside, Schur, Miller) the theory of finite groups acquired at this time all the essential features it has at the present day. But later it became clear that the finiteness of a group is a restriction that is too strong and not always natural. It was of particular importance that this restriction very soon led to conflicts with the needs of neighboring branches of mathematics: in several parts of geometry, the theory of automorphic functions, topology, in all of these one again and again came across algebraic formations similar to groups, but infinite, and so demands were made upon the theory of groups that the theory of finite groups was not in a position to satisfy. Moreover, from the point of view of algebra itself—of which the theory of groups is a part—a situation could hardly be regarded as normal in which such very simple and important groups as, for example, the additive group of integers remained outside the limits of the theory. The finite group must therefore be a special case of the general concept of a group, and the theory of finite groups must be a chapter in the general theory of "infinite" (that is, not necessarily finite) groups.

An exposition of the elements of group theory without the assumption that the groups under consideration were finite was, for the first time in the whole literature, made in the book *Abstract Theory of Groups* [in

Russian] by O. J. Schmidt (Kiev 1916), a book which even now remains a reference work for all Soviet algebraists. But the broader development of the general theory of groups began somewhat later and was linked with that radical reorganization and transition to a set-theoretical foundation in algebra which occurred in the twenties of the present century (Emmy Noether). It was from here that the new concepts of operator systems and chain conditions were introduced into the theory of groups.

Subsequently the work on the general theory of groups became very vigorous and varied, and at the present time this part of mathematics has become a wide and rich science occupying one of the foremost places in contemporary algebra. Clearly this development of the general theory of groups could not ignore the achievements of the theory of finite groups. On the contrary, many results sprang from the corresponding parts of the theory of finite groups; the guiding principle was the endeavour to replace the finiteness of the group by other natural restrictions under which a given theorem or a given theory remain valid but without which they cease to hold. Furthermore, very often a problem that is simple and completely solved in the case of finite groups changes to a broad theory, yet far from complete; this happens, for example, in the theory of abelian groups, one of the most important parts of contemporary group theory. At the same time a number of new branches arose, linked essentially with the study of infinite groups—the theory of free groups and of free products. Finally, in some cases, above all in the problem of giving a group by defining relations, the theory of groups achieved for the first time a clarity and rigor that had been lacking in the preceding stage of its development.

The theory of groups is far from complete. The variety of concrete problems confronting it and the fact that in some directions the research work has only recently begun justify us in assuming that the general theory of groups has not yet passed the climax of its growth. Nevertheless the time has come to systematize the rich material already accumulated and thus to present to a wide circle of mathematicians the basic trends of contemporary group theory, its methods, its principal achievements, and finally, the immediate problems facing it and the paths along which it will necessarily develop in the near future.

The present book does not pretend, obviously, to range over the whole theory of groups; but almost all the main branches of our science are presented in it, to an extent sufficient to show the reader the wealth of its contents and the variety of its methods.

The reader is not required to have a preliminary acquaintance with the elementary concepts of the theory of groups. A basic course of higher algebra

is a prerequisite only for some initial examples of groups, such as matrices, permutations, roots of unity. As to the theory of numbers, the reader need only know the elements of the theory of congruences. On the other hand, the reader should be thoroughly acquainted with the elements of the theory of sets, as far as the first four chapters of the book *Set Theory* by Hausdorff (Chelsea, 1956). In particular, in many constructions and proofs transfinite induction is an essential tool.

The bibliography contains, as far as possible, a complete list of papers on the general theory of groups, including some that have come out recently but have not influenced the book. Of the rich literature on finite groups the bibliography includes only a few directly connected with the contents of the book. References to the bibliography are given in the text by the name of the author and (in brackets) the number of the paper quoted.

Moscow, October 1940

CONTENTS

PART TWO: ABELIAN GROUPS

Joseph Louis Lagrange, 1736—1812

Carl Friedrich Gauss, 1777—1855

Augustin Louis Cauchy, 1789—1857

Niels Henrik Abel, 1802—1829

Sir William Rowan Hamilton, 1805—1865

Evariste Galois, 1811—1832

Arthur Cayley, 1821—1895

Richard Dedekind, 1831—1916

Ludwig Sylow, 1832—1918

Camille Jordan, 1838—1922

Georg Frobenius, 1849—1917

Felix Klein, 1849—1925

Ludwig Stickelberger, 1850—1936

William Burnside, 1852—1927

Giovanni Frattini, 1852—1925

Henri Poincaré, 1854—1912

Walther von Dyck, 1856—1934

Otto Holder, 1859—1937

George Abram Miller, 1863—1951

Ernst Steinitz, 1871—1928

Issai Schur, 1875—1941

Max Dehn, 1878—1952

Emmy Noether, 1882—1935

Joseph Henry Maclaglan Wedderburn, 1882—1948

Robert Remak, 1888—194?

Heinz Prüfer, 1896—1934

Otto Schreier, 1901—1929

Hans Fitting, 1906—1938

PART ONE

THE ELEMENTS OF GROUP THEORY

CHAPTER I

DEFINITION OF A GROUP

§ 1. Algebraic operations

In any course on higher algebra the reader will have become acquainted with sets in which algebraic operations are defined. Fields and rings—that is, sets with two independent operations, called addition and multiplication—play a fundamental rôle in such a course. Very often, however, one encounters sets in which only *one* algebraic operation is defined (or is studied for the moment). We recall the definition of an algebraic operation.

Let a set M be given. We say that an *algebraic operation* is defined in M if we have a rule by which we can assign to any two (distinct or equal) elements of M, taken in a definite order, a third well-defined element of the same set.

It is therefore part of the definition of an algebraic operation that it shall be single-valued and that it shall be applicable to any pair of elements. Furthermore, the definition indicates that the order in which the elements are taken may be relevant when the operation is performed. In other words, it is not excluded that the elements of M that correspond to the pair a, b and to the pair b, a of M may be *distinct*, i.e., that the operation under consideration is *non-commutative.*

Numerous examples can be given of sets with numbers as elements and with an operation that satisfies the above definition. We leave the construction of such examples to the reader and merely indicate some sets that do not satisfy the definition: the set of negative integers under multiplication, the set of odd numbers under addition, and the set of real numbers with division as the operation—the latter because division by zero is impossible.

Various algebraic operations performed on objects other than numbers are also well known; some examples are: the addition of vectors in an n-dimensional vector space, vector multiplication of vectors in a three-dimensional euclidean space, multiplication of square matrices of order n, addition of real functions of a real variable, multiplication of such functions, etc. An example of an algebraic operation that will be of great importance in the sequel is the *multiplication of permutations.* A permutation of degree n is, of course, a one-to-one mapping of the set of the first n natural numbers onto itself. The result of carrying out two permutations of degree n in

succession is itself a permutation of degree n, which is called the *product* of the first of the given permutations by the second. If, for example, we consider the permutations

$$a = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$$

where $n = 3$, then their product is the permutation

$$ab = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

An algebraic operation in the set of permutations of degree n is thus defined. It is easy to see that it is non-commutative; the product of b by a for the above two permutations has the form

$$ba = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

We shall, as a rule, use multiplicative terminology and symbolism for studying sets with one algebraic operation; the operation will be called *multiplication*, and the result of performing the operation on the pair of elements a, b will be called their *product* ab. In some cases, however, it will be convenient to employ the additive notation, in other words, to call the operation *addition* and to speak of the *sum* $a + b$ of the elements a, b.

We have already mentioned that the *commutativity* of an operation, that is, the validity of the equation

$$ab = ba$$

for arbitrary elements a, b of the set M, is not part of the definition. Examples of non-commutative operations are: multiplication of square matrices of order n for $n \geqq 2$; multiplication of permutations of degree n, not only for $n = 3$ as was illustrated above, but for all $n \geqq 3$; and vector multiplication of vectors of a three-dimensional euclidean space. Subtraction of numbers can also be regarded as an example of a non-commutative operation.

Furthermore, the definition of an algebraic operation does not require that the operation be *associative*, that is, that for arbitrary elements a, b, c of the set M the equation

$$(ab)c = a(bc)$$

shall hold. Vector multiplication of vectors of a three-dimensional space serves as an example of a non-associative operation; so does the subtraction of integers. On the other hand, as is well known, the multiplication of matrices is associative. Again, the multiplication of permutations is associative; this follows from the following more general result.

Let S be any finite or infinite set. We consider the totality of *single-valued mappings of the set S into itself*, that is, mappings that associate with every element of S a well-defined element of the same set, where various elements of S may possibly be mapped onto one and the same element and where there may be elements in S onto which nothing is mapped. If we understand by the product of two such mappings the result of performing them in succession, then we obtain an associative algebraic operation in the set of mappings.

For let φ, ψ, and χ be three single-valued mappings of a set S into itself. Further, let a be an arbitrary element of S, and let it go over into the element b under the mapping φ, while b goes over into c under the mapping ψ, and finally c into d under the mapping χ. Then the mapping $\varphi\psi$ carries the element a into c, so that under the mapping $(\varphi\psi)\chi$, a goes over into d. However, the mapping $\psi\chi$ carries the element b into d, and therefore under the mapping $\varphi(\psi\chi)$ a also goes over into d. Thus it has been shown that the mappings $(\varphi\psi)\chi$ and $\varphi(\psi\chi)$ coincide.

Let us see what deductions can be made from the validity of the associative law for an operation given in a set M. From the definition of an algebraic operation it follows that the product of any *two* elements of M, taken in a definite order, exists and is unique. But we cannot, in general, speak of the product of *three* elements: for, the product of the elements a, b, and c, taken in this order, may depend on whether the product of a and b is multiplied by c, or a is multiplied by the product of b and c. The associative law, however, permits us to refer without ambiguity to the product of three elements of M; the element $(ab)c$, being equal to $a(bc)$, will simply be denoted by abc. Clearly, the product of three elements may change, in general, with a permutation of the factors.

Furthermore, the associativity of an operation permits us to speak without ambiguity of the *product of any finite number of elements of M*, taken in a definite order; in other words, it enables us to prove that the *final result is independent of the initial distribution of parentheses.* Let us show this for the case of n factors ($n > 3$), on the assumption that it has already been proved for a smaller number of factors. Let

$$a_1, a_2, \ldots, a_n,$$

be an ordered system of n elements of M in which parentheses are distributed in some way indicating the order in which the operations shall be carried out. If we perform in succession the multiplications indicated by the parentheses, then we must carry out in the last step the multiplication of the product of the first i elements $a_1, a_2, \ldots, a_i (1 \leqq i \leqq n-1)$ by the product $a_{i+1} \ldots a_n$. Since these products consist of fewer than n factors and are therefore, by assumption, determined uniquely, it only remains to show that we can go over from $(a_1 a_2 \ldots a_i)(a_{i+1} a_{i+2} \ldots a_n)$ to $(a_1 a_2 \ldots a_j)(a_{j+1} \ldots a_n)$, where $i \neq j$. It obviously suffices to perform this transition for the case $j = i + 1$, and we achieve this by a simple application of the associative law: if

$$a_1 a_2 \ldots a_i = b, \quad a_{i+2} a_{i+3} \ldots a_n = c,$$

then

$$b(a_{i+1} c) = (b a_{i+1}) c.$$

This does not give us the right, however, to speak of the product of an infinite set of elements of M.

The set M in which an algebraic operation is given sometimes has a *unit element*, that is, an element 1 for which

$$a \cdot 1 = 1 \cdot a = a$$

for all a in M. *Only one element having this property can exist in* M: if there were another unit element $1'$, then the product $1 \cdot 1'$ would be equal both to 1 and to $1'$; hence $1 = 1'$. When the additive notation is used, the unit element is called the *null element* (or zero) and is denoted by the symbol 0.

Examples of sets with an algebraic operation that do not have a unit element (or a zero) are: the set of natural numbers with respect to addition, the set of even numbers with respect to multiplication, and the set of vectors of a three-dimensional euclidean space with respect to vector multiplication. On the other hand, the multiplication of square matrices of order n has a unit element, namely the unit matrix. A unit element also exists for the multiplication of permutations of degree n; this is easily seen to be the identity permutation

$$\begin{pmatrix} 1 & 2 \ldots n \\ 1 & 2 \ldots n \end{pmatrix}.$$

More generally, in the set of all single-valued mappings of a set S into itself with multiplication defined as the result of performing the mappings in succession, there exists a unit element, the identity mapping of S onto itself.

Finally, let us introduce the concept of an *inverse operation*. We know from higher algebra that in a ring the operation inverse to addition is subtraction, and in a field—if we restrict ourselves to elements different from zero—the operation inverse to multiplication is division. In the light of these examples, it is natural to ask the following question in the case of an arbitrary set M with one (not necessarily commutative) operation: Do there exist for given elements a and b certain elements x and y for which

$$ax = b, \quad ya = b \tag{1}$$

holds? These equations may or may not be solvable in M. Moreover, they may have distinct solutions. We shall say that *an operation, given in M, has an inverse operation* if for every a and b each of the equations (1) has *one and only one* solution; in the non-commutative case the solutions x and y of these two equations need not of course coincide.

An example of an operation for which equations (1) may have several distinct solutions is multiplication in any ring having divisors of zero, in particular in the ring of functions and in the ring of matrices. Very simple examples of operations for which equations (1) are not always solvable are: the operation of addition in the set of natural numbers and the operation of multiplication in the ring of integers and in the field of real numbers as well—the latter because division by zero is impossible.

§ 2. Isomorphism. Homomorphism

Let M and M' be two given sets in each of which an algebraic operation is defined; we shall assume that in both sets these operations are called multiplication. The sets M and M' are said to be *isomorphic* with respect to these operations if a one-to-one correspondence between their elements can be established for which the following holds: If the elements a and b of M correspond to the elements a' and b' of M', and if

$$ab = c, \quad a'b' = c',$$

then the element c of M shall correspond to the element c' and to no other element of M'. Such a one-to-one correspondence is called an *isomorphic relation* or *isomorphism* between M and M'. An isomorphism of the sets M and M' will be denoted by the symbol $M \simeq M'$.

Examples of isomorphic sets with one algebraic operation can readily be

given. Thus, the set of even numbers can be put into one-to-one correspondence with the set of all multiples of 3 by associating the even number $2k$ of the first set with the number $3k$ of the second set. This mapping is obviously an isomorphism with respect to addition, which is an operation defined in each of the two sets.

Further, let us compare the operation of multiplication in the set of positive real numbers with the operation of addition in the set of all real numbers. We obtain a one-to-one mapping of the first of these sets onto the second by associating with each positive real number its logarithm to the base 10. The equation

$$\log (ab) = \log a + \log b$$

shows that this mapping is an isomorphism.

The reader is familiar with many examples of isomorphic sets in higher algebra. Let us recall one of these; the set of linear transformations of an n-dimensional vector space over a field F, with the product of linear transformations defined as the result of their being performed in succession, is isomorphic to the set of square matrices of order n over the field F with matrix multiplication as the algebraic operation. This isomorphism depends, of course, on the choice of basis in the vector space. Thus, when the sets M and M', each with one operation, are isomorphic, then the isomorphism between them can be established, in general, in many different ways.

Each set with an operation is obviously isomorphic to itself: it is sufficient to take the identity mapping of the set onto itself. The relation of isomorphism, moreover, is (i) symmetrical: from $M_1 \simeq M_2$ follows $M_2 \simeq M_1$, and (ii) transitive: from $M_1 \simeq M_2$ and $M_2 \simeq M_3$ follows $M_1 \simeq M_3$.

From the definition of isomorphism it follows that isomorphic sets have the same cardinal number; if in particular they are finite, they consist of the same number of elements.

Isomorphic sets with operations may differ from one another in the nature of their elements and, possibly, in the name of the operation and the symbolism used to denote it. They are indistinguishable, however, as far as the properties of the operations are concerned: given a set with an operation, whatever can be proved about the basic properties of this operation without reference to the individual properties of the elements of the set goes over automatically to all sets isomorphic to the given one. In what follows we shall, therefore, consider isomorphic sets to be merely distinct copies of a set with one and the same operation and by so doing we shall single out the algebraic operation itself as the true object of our study. Only in our con-

struction of examples shall we speak, for convenience, of concrete sets and of operations whose definitions depend on properties of the elements of these sets. Besides, we shall later learn (in Chapter V) how to construct concrete examples of operations without making any assumptions about the nature of the elements on which the operations are performed.

The concept of isomorphism is not specifically an algebraic one. In fact, every branch of mathematics identifies the objects of its study by certain criteria and emphasizes in this way those properties of the objects that form the true subject matter of that branch. To clarify this remark, the reader need only reflect on the way one of the fundamental mathematical concepts —that of a whole number—is formed.

We obtain a generalization of the concept of an isomorphic mapping by omitting from the definition the postulate that the correspondence be one-to-one. Let M and M' be sets, each with one operation, say multiplication. We consider a mapping φ of the set M onto the set M' which associates with every element of M a well-defined *image* $a' = a\varphi$ in M', while each element of M' has at least one, but in general several distinct, *originals*, or *inverse images*, in M. This mapping is called a *homomorphism* if for any a and b in M it follows from

$$a\varphi = a' \qquad b\varphi = b'$$

that

$$(ab)\varphi = a'b'.$$

We shall then say that the set M' is a *homomorphic image* of the set M.

It is not permissible, of course, to identify two sets one of which is mapped homomorphically onto the other. In this respect the concept of homomorphism is less fundamental than the concept of isomorphism, but in the subsequent development of the theory its rôle will, nevertheless, be very important. Let us give a few examples of homomorphic mappings.

Let M be the set of all integers, with addition as the algebraic operation; and let M' be the set consisting of the numbers 1 and -1 with multiplication as operation. By associating 1 with every even number and -1 with every odd number we obtain a homomorphic mapping of M onto M'; indeed the rule "even plus odd is odd" corresponds to the equation $1 \cdot (-1) = -1$, and similar equations correspond to the other rules.

Next let M be the set of all plane vectors whose initial point is the origin of the coordinate system and M' the set of those vectors of M which lie along the axis of abscissas, with vector addition in both cases as the algebraic operation. We obtain a homomorphic mapping of M onto M' if we associate

with every vector of M its projection onto the axis of abscissas; for, the projection of a sum is, of course, the sum of the projections of the summands.

If a set M with one operation is mapped homomorphically onto a set M', in particular if these two sets are isomorphic, then *the validity of the associative or of the commutative law in M entails the validity of the corresponding law in M'.* For example, let the operation in M be commutative. If a' and b' are arbitrary elements of M', if a is one of the originals of a', and if b is one of the originals of b', then the element ab corresponds in the homomorphism under consideration to $a'b'$, the element ba to $b'a'$; and therefore the equation $ab = ba$ and the uniqueness of the image under a homomorphic mapping imply the equation $a'b' = b'a'$. If the operation in M is associative, the corresponding proof proceeds along the same lines.

Furthermore, if the set M has a unit element 1, then its image must be the unit element in the set M'. For let us denote the image of the unit element by e'; if a' is an arbitrary element of M' and a one of its originals, then the equations $a \cdot 1 = 1 \cdot a = a$ and the homomorphic property of the mapping imply the equations $a'e' = e'a' = a'$. Thus we have shown that e' is indeed a unit element for the set M'.

We note that if a set M has an inverse operation, it cannot be inferred that the same is true of a homomorphic image M' of M; for it is impossible to prove the uniqueness of the solutions of each of the equations (1) of the preceding paragraph. However, we can prove that those equations have solutions. For if a' and b' are elements of M', and if a is one of the originals of a' and b one of the originals of b' in M, that is,

$$a\varphi = a', \quad b\varphi = b',$$

and if the element c in M satisfies the equation $ax = b$, then by the homomorphic property of the mapping the element

$$c' = c\varphi$$

satisfies $a'x = b'$ in M'.

As regards the various converses: from the validity of the associative or the commutative law in M' or from the existence of a unit element or of an inverse operation in M' the corresponding statement for the set M does not follow.

We shall now describe a method of obtaining all the possible homomorphic images of a given set M with one operation. For this purpose we introduce the following concept. Suppose that there is given a partition of the set M into disjoint subsets, which we shall call *classes* and denote by the letters

$A, B, \ldots$. Such a partition of M into disjoint classes is called *regular* if from the fact that the elements a_1 and a_2 lie in one class A, and the elements b_1 and b_2 lie in one class B, it follows that the elements $a_1 b_1$ and $a_2 b_2$ also lie in one and the same class C.

This definition implies that the class C is completely determined by the classes A and B: the product of any element of A by any element of B is contained in C. If we call the class C the *product* of the class A by the class B, then an algebraic operation is defined in the set $\overline{M}$ of all classes of our regular partition. We shall call the set $\overline{M}$ with this operation the *factor set* of M with respect to the regular partition.

The set M can be mapped homomorphically onto the factor set $\overline{M}$. For it is sufficient to associate with each element of M the class in which the element lies and to make use of the definition of multiplication in the set $\overline{M}$. This mapping of the set M onto the factor set $\overline{M}$ is called the *natural* or *canonical* homomorphism.

The factor sets of M with respect to its regular partitions essentially exhaust all the possible homomorphic images of M. More precisely, the following theorem holds.

If M' is an arbitrary homomorphic image of the set M, and φ a homomorphic mapping of M onto M', then there exists a regular partition of M into disjoint classes such that M' is isomorphic to the factor set $\overline{M}$ constructed by means of this partition. Moreover, there exists an isomorphic mapping ψ of the set M' onto the set $\overline{M}$ such that the result of performing the mappings φ and ψ in succession coincides with the natural homomorphism of M onto $\overline{M}$.

For the proof, we note that we obtain a partition of M into disjoint classes if we collect into one class all the elements whose images under the mapping φ coincide. This partition is regular; if the elements a_1 and a_2 lie in one class, that is, if

$$a_1\varphi = a_2\varphi = a',$$

and if the same applies to the elements b_1 and b_2, that is, if

$$b_1\varphi = b_2\varphi = b',$$

then by the homomorphism of the mapping φ

$$(a_1 b_1)\varphi = (a_2 b_2)\varphi = a'b',$$

so that the elements $a_1 b_1$ and $a_2 b_2$ belong to one and the same class. This

enables us to define a multiplication, in the way described above, in the set $\overline{M}$ of all classes of the partition that we have obtained, in other words, to turn $\overline{M}$ into a factor set. Between all the elements of the set M' and all the classes (that is, elements of the set $\overline{M}$) there now exists a one-to-one correspondence ψ: we need only associate each element of M' with the class consisting of all the originals of this element. The correspondence ψ is an isomorphism: if the elements a' and b' are linked with the classes A and B respectively, and if elements are chosen in these classes, a from A and b from B, then AB is the class that contains the element ab. However,

$$(ab)\varphi = (a\varphi)(b\varphi) = a'b',$$

so that the element $a'b'$ is associated under the mapping ψ with the class AB. To conclude the proof, we choose an arbitrary element a of M. Let

$$a\varphi = a', \qquad a'\psi = A.$$

Since the element a is one of the originals of a', a is contained in A; in other words, the result of performing the mappings φ and ψ in succession does, in fact, coincide with the natural homomorphic mapping of M onto $\overline{M}$. This completes the proof.

§ 3. Groups

A further investigation of sets with an arbitrary operation would not be a very fruitful undertaking: the concept, being too general, is poor in content. Historically, sets of a special type with one operation—called *groups*—were first selected for detailed study, owing to their many applications both in mathematics itself and beyond its boundaries. This is one of the most fundamental concepts of contemporary mathematics: it combines an affinity to familiar operations on numbers with an exceptionally wide domain of applicability.

A non-empty set G with one algebraic operation is called a *group* if the following conditions are satisfied:

(1) the operation in G is associative;
(2) the inverse operation can be performed in G.

The operation in G need not be commutative. If it is commutative, then G is called a *commutative* or *abelian* group, after N. H. Abel who studied a type of equation whose theory is linked with the theory of commutative

groups. It is clear that the operations in this class of groups are particularly close to the ordinary operations on numbers; a large part of the sequel will be devoted to a detailed study of the properties of abelian groups.

If in an arbitrary group G the commutative law holds for two given elements a and b, then these elements are called *permutable*.

If a group G consists of a finite number of elements, then it is called a *finite* group, and the number of its elements is called the *order* of the group. The existence of groups of any finite order, and of groups of any infinite cardinal number will be shown in the next section.

For finite groups the condition (2) *in the definition of a group can be weakened to the mere requirement that the solutions of the two equations*

$$ax = b, \qquad ya = b, \tag{1}$$

be unique; we can then deduce that solutions of these equations do exist.

For let G be a finite set, consisting of n elements, with one operation and with unique solutions of the equations (1), provided these solutions exist at all; let a and b be elements of G. If we multiply the element a on the right by the element x of G, in other words, if we form the product ax and let x run through all elements of G, then by our assumption we obtain n distinct elements of G, that is, we obtain all the elements of G; there exists, then, an element x_0 for which ax_0 is equal to the given b. This proves the existence of a solution for the first of the equations (1). The existence of a solution of the second equation is proved in the same way.

A similar weakening of condition (2) is not possible in the infinite case, as is shown by the example of the set of positive integers with the operation of addition. In this example, the operation can always be performed and it is single-valued and associative; however, the inverse operation—subtraction—although it is single-valued, cannot always be performed.

We now proceed to determine the simplest consequences of the definition of a group.

Let us take an arbitrary element a in a group G. From condition (2) there follows the existence and uniqueness in G of an element e_a which satisfies the condition $ae_a = a$, that is, which plays the rôle of a unit element, for the element a, under multiplication on the *right*. This element e_a has, moreover, the same property with respect to *all* the elements of the group; if b is any other element of G and if y is an element of the group that satisfies the equation $ya = b$—the existence of y follows from condition (2)—then on multiplying both sides of the equation $ae_a = a$ on the left by y and

applying the associative law to the left-hand side we obtain $be_a = b$. We have thus proved the existence and uniqueness in G of a *right unit element* e' having the property $xe' = x$ for all the elements x of G.

In the same way we can prove the existence and uniqueness in G of a *left unit element* e'' that satisfies the condition $e''x = x$ for all x in G. The elements e' and e'' moreover coincide, as the equations $e''e' = e'$ and $e''e' = e''$ show. *We have thus proved the existence and uniqueness in every group G of an element e that satisfies the condition*

$$xe = ex = x$$

for all elements x of G. This element is the *unit element* of the group G (cf. § 1) and will be denoted by the symbol 1. As we have just seen, the unit element is permutable with every element of the group.

From condition (2) there follows, further, for any given element a the existence and uniqueness of elements a' and a'' which satisfy the conditions

$$aa' = 1, \qquad a''a = 1.$$

The elements a' and a'' in fact coincide: from

$$a''aa' = a''(aa') = a'' \cdot 1 = a''$$

and

$$a''aa' = (a''a)a' = 1 \cdot a' = a'$$

it follows that $a' = a''$. We shall denote this element by a^{-1} and call it the *inverse* of a. Every element a of G has, therefore, a uniquely determined inverse a^{-1} which satisfies the conditions

$$aa^{-1} = a^{-1}a = 1.$$

From the last equation it follows that *the inverse of a^{-1} is a itself*, i.e. $(a^{-1})^{-1} = a$, and that every element is permutable with its inverse. It is easy to verify, moreover, that *the inverse of a product of several elements is the product of the inverses of the factors taken in the reverse order*, i.e.

$$(a_1a_2 \ldots a_{n-1}a_n)^{-1} = a_n^{-1}a_{n-1}^{-1} \ldots a_2^{-1}a_1^{-1}.$$

The unit element is its own inverse.

The concept of an inverse element enables us to write down explicitly

the elements x and y which by condition (2) satisfy the equations $ax = b$ and $ya = b$ for given a and b; for, an immediate verification shows that

$$x = a^{-1}b, \qquad y = ba^{-1}.$$

Hence it follows that in the non-commutative case x and y may be distinct elements of the group. In the case of abelian groups this is, of course, impossible.

The existence and uniqueness of the inverse elements, which we have deduced from condition (2), can actually replace that condition. We shall show this below and shall not even assume uniqueness of the unit and the inverse elements but shall limit ourselves to the assumption that one-sided (right-hand, say) unit and inverse elements exist. Such a weakening of condition (2) sometimes simplifies the task of verifying that a given set with an operation is a group.

If G is a set with an associative operation, then condition (2) *follows from the conditions*

(2′) there exists in G at least one *right unit element* e with the property

$$ae = a \qquad \text{for all } a \text{ in } G,$$

(2″) among the right unit elements of G there is an element e_0 such that for each a in G at least one *right inverse element* a^{-1} exists satisfying

$$aa^{-1} = e_0.$$

Proof. Let a^{-1} be one of the right inverse elements of a. Multiplying both sides of the equation $aa^{-1} = e_0$ on the left by e_0 we obtain

$$e_0aa^{-1} = e_0e_0 = e_0,$$

and hence

$$e_0aa^{-1} = aa^{-1}.$$

Multiplying both sides of this equation on the right by one of the right inverses of a^{-1} we obtain

$$e_0ae_0 = ae_0,$$

and hence $e_0a = a$. The element e_0 turns out to be also a left unit element for G.

Now if e_1 is an arbitrary right unit element and e_2 an arbitrary left unit element, then it follows from the equations

$$e_2 e_1 = e_1 \quad \text{and} \quad e_2 e_1 = e_2$$

that $e_1 = e_2$. Thus the uniqueness of the unit element e is proved.

Multiplying both sides of the equation $aa^{-1} = e$ on the left by a^{-1} we obtain

$$a^{-1}aa^{-1} = a^{-1}.$$

Multiplying both sides of this equation on the right by one of the right inverse elements of a^{-1} we obtain $a^{-1}a = e$, so that the element a^{-1} is also a left inverse of a. If now a_1^{-1} and a_2^{-1} are arbitrary right and left inverse elements respectively of a, then it follows from the equations

$$a_2^{-1}aa_1^{-1} = (a_2^{-1}a)\,a_1^{-1} = a_1^{-1},$$
$$a_2^{-1}aa_1^{-1} = a_2^{-1}(aa_1^{-1}) = a_2^{-1},$$

that $a_1^{-1} = a_2^{-1}$, in other words, the inverse element is unique.

Condition (2) can now be easily deduced. In order to satisfy the equations

$$ax = b, \qquad ya = b$$

it is sufficient to put $x = a^{-1}b$, $y = ba^{-1}$ The uniqueness of this solution for, say, the first equation follows from the fact that if $ax_1 = ax_2$, then by multiplying on the left by a^{-1} we obtain $x_1 = x_2$.

We note that the uniqueness of the solutions of the equations (1) allows us to introduce a *left* and a *right cancellation*: if

$$ab_1 = ab_2 \quad \text{or} \quad b_1a = b_2a,$$

then $b_1 = b_2$.

If a group G is mapped homomorphically (in particular, isomorphically) on a set G' with one operation, then G' is also a group.

For from what has been proved in the preceding section it follows that the operation in G' is associative, that the equations (1) have solutions in G', and that the image of the unit element of G is a unit element for the set G'. Thus conditions (2′) and (2″) are satisfied in G', and therefore, as shown above, G' is a group.

In particular, the factor set of a group G with respect to any regular partition is itself a group. We shall therefore speak in future of the

factor group of a group G with respect to a regular partition.

The theorem proved at the end of the preceding section now goes over into the following very important *homomorphism theorem* for groups:

Homomorphism Theorem: *If φ is a homomorphic mapping of a group G onto a group G', then there exists a regular partition of G such that G' can be mapped isomorphically onto the factor group $\bar{G}$ of G with respect to this partition. Moreover, the isomorphism ψ of G' onto $\bar{G}$ can be so chosen that the result of performing the mappings φ and ψ in succession coincides with the natural homomorphism of G onto the factor group $\bar{G}$.*

We add another remark about homomorphic mappings.

If the homomorphism φ of a group G onto a group G' carries the element a of G into the element a' of G',

$$a\varphi = a',$$

then the image of the element a^{-1} is the element a'^{-1}:

$$a^{-1}\varphi = a'^{-1}.$$

For we know that $1\varphi = 1'$. If we now put $a^{-1}\varphi = b'$, then

$$1\varphi = (aa^{-1})\varphi = a\varphi \cdot a^{-1}\varphi = a'b',$$

that is,

$$a'b' = 1', \text{ and hence } b' = a'^{-1}.$$

The axiomatic investigations of the present section on the definition of a group could be extended considerably, but we shall not pursue the matter further; we merely mention that in the paper of Baer and Levi [1][1] the definition of a group is split into seven independently formulated axioms: existence of a product and of a left and a right quotient, uniqueness of each of these three, and associativity. The authors then determine all the minimal subsystems of this system of axioms that suffice as a complete definition of a group. Another approach to the problem can be found in the paper by Lorenzen [1].

The orders of elements. The product of n equal elements a in a group G is called the *n-th power* of a and is denoted by a^n. Negative powers of a can be defined either as elements of G that are inverse to positive powers of a,

[1] See also § 4 of the first edition of this book (Moscow-Leningrad, 1944; German translation: Berlin, 1953).

or as products of equal factors a^{-1}. As a matter of fact, these definitions coincide:

$$(a^n)^{-1} = (a^{-1})^n.$$

To prove this it is sufficient to take the product of $2n$ factors of which the first n are a and the rest a^{-1}, and then to carry out all the cancellations. We shall denote the negative powers of a by a^{-n}. By a^0 we shall, of course, mean the element 1.

It is easy to verify that for any exponents m and n, positive, negative, or zero, the following equations hold:

$$a^m \cdot a^n = a^n \cdot a^m = a^{m+n}$$

$$(a^m)^n = a^{mn}.$$

The first of these equations shows that powers of one and the same element are permutable.

If all the powers of an element a are distinct elements of the group, then a is called an *element of infinite order*. Suppose, however, that among the powers of an element a there are equal elements, for example $a^k = a^l$ for $k \neq l$; this will always occur, in particular, in the case of finite groups. If $k > l$ then $a^{k-l} = 1$, so that there exist positive powers a equal to the unit element. Let n be the smallest positive power among them.

(1) $\quad a^n = 1, \quad n > 0$

(2) if $a^k = 1$, $k > 0$, then $k \geqq n$.

In that case we say that a is an *element of finite order*, specifically, *of order* n.

If the element a is of order n, then all the elements

$$1, a, a^2, \ldots, a^{n-1}$$

are easily seen to be distinct. *Every other power of a, positive or negative, is equal to one of these elements.* For if $k = nq + r$, $0 \leqq r < n$, then

$$a^k = (a^n)^q \cdot a^r = a^r.$$

Hence it follows that if a is of order n and if $a^k = 1$, then k must be divisible by n.

Every group has one and only one element of order 1, namely the element 1. The inverse of an element a of finite order n is obviously the element a^{n-1}.

All the elements of a finite group are of finite order; in the following section we shall show that there exist also infinite groups with elements of finite orders only. A group whose elements all have finite order is called *periodic*. There exist, on the other hand, groups in which the orders of all the elements, except the unit element, are infinite. Such groups are usually called *torsion-free* groups.[1] Finally, it is natural to call a group *mixed* if it contains elements of infinite order as well as elements, other than the unit element, of finite order.

If the *additive* notation is chosen for a group G, then some corresponding changes in terminology and notation are required. As we have already pointed out in § 1, we speak in this case of the null element of the group instead of the unit element, and denote it by 0. Further, the element inverse to a is then called the *opposite* element and is denoted by $-a$; and we speak of *multiples* of a instead of powers of a and write them as ka.

§ 4. Examples of groups

In this section we collect some very simple examples of groups, which we shall often have occasion to refer to in the sequel. In most cases it will be left to the reader to verify that all the postulates entering the definition of a group are satisfied.

1. All the positive and negative integers form a group with respect to addition—the *additive group of integers*. This group is abelian. The number zero plays the rôle of the unit element, and all the elements of the group except zero are of infinite order, that is, the group is torsion-free.

2. Similarly, we can obtain the *additive groups of all rational numbers, of all real numbers, and of all complex numbers.*

3. All the even numbers also form a group under addition. This *additive group of even numbers* is isomorphic to the additive group of integers (Example 1), because the correspondence which associates the integer k with an even number $2k$ is an isomorphism. All the multiples of a given number n also form a group under addition. But the set of all the odd numbers is not a group under the operation of addition, since this operation leads outside the given set. Nor does the set of all non-negative integers form a group under addition, because the inverse operation—subtraction—cannot always be carried out.

---

[1] Another name for groups without elements of finite order except 1 is *locally infinite*. This is in keeping with a systematic terminology (see also § 55). [*Trans.*]

4. The integers do not form a group under multiplication, since the inverse operation—division—cannot always be performed. Nor do all the rational numbers form a group under multiplication, since division by zero is impossible. But all the rational numbers different from zero form a group under multiplication—the *multiplicative group of rational numbers.* The unit element of this group is the number 1. The number -1, which belongs to the group, is of order 2, while all the other elements are of infinite order.

5. We can also speak of the *multiplicative group of all positive rational numbers.* This group can be mapped homomorphically onto the additive group of integers as follows: Every positive rational number α can be written in the form

$$\alpha = 2^n \alpha',$$

where numerator and denominator of the number α' are prime to 2 and n is a positive or negative integer or zero. The mapping $\alpha \to n$ is the required homomorphism. Note that the negative rational numbers do not form a group under multiplication.

6. All the non-zero (or all the positive) real numbers and all the non-zero complex numbers also form groups under multiplication. We recall that, as shown in § 2, the multiplicative group of positive real numbers is isomorphic to the additive group of all real numbers.

7. The numbers 1 and -1 constitute a group under the operation of multiplication—a finite group of order 2. As shown in § 2, this group is a homomorphic image of the additive group of integers. It is also a homomorphic image of the multiplicative group of all real numbers—we need only map every positive number onto 1 and every negative number onto -1.

8. All the complex n-th roots of unity form a finite group of order n under multiplication. *This proves the existence of finite groups of every order.* For $n = 2$ we obtain the group of the preceding example. We recall that all the n-th roots of unity are powers of one of them, a so-called primitive n-th root of unity.

9. All the complex numbers which are roots of unity of any degree also form a group, the *group of all roots of unity.* It is an infinite, periodic group,

10. All the complex numbers of absolute value 1 form a group under multiplication. This group is isomorphic to the *group of rotations of a circle.* Let us consider the set of all counter-clockwise rotations of a circle about its center. We shall consider a rotation through the angle 2π to be the same as a rotation through the angle 0, and we shall identify, in general, any two rotations with angles differing by a multiple of 2π. In this set of

rotations we define a group operation in the following way: The sum of two rotations shall be the result of performing them in succession; the sum of the rotations by angles α and β will obviously be the rotation by the angle $\alpha + \beta$ if $\alpha + \beta < 2\pi$, and by the angle $\alpha + \beta - 2\pi$ if $\alpha + \beta \geqq 2\pi$. It is easy to verify that this yields a group. To obtain an isomorphic mapping of this group onto the multiplicative group of complex numbers of absolute value 1 it is sufficient to establish a correspondence between the rotation through the angle α and the complex number with argument α.

All the groups considered so far are commutative. We now pass on to examples of non-commutative groups.

11. All the permutations of n symbols, the group operation being the multiplication defined in § 1, constitute a group S_n—the *symmetric group of degree n*. This is a finite group of order $n!$ and for $n \geqq 3$ is non-commutative. For it was shown in § 1 that the multiplication of permutations is associative and that the identity permutation is the unit; the permutation inverse to

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix}$$

is the permutation

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_n \\ 1 & 2 & \dots & n \end{pmatrix}.$$

12. The reader will have learned in higher algebra[a] that all permutations of degree n fall into two classes, the odd and the even permutations, with $n!/2$ in each class. One of the possible definitions is the following. A permutation is called *even* if it is a product of an even number of transpositions and *odd* otherwise. Hence it follows that *the product of two even permutations is even*. Since the identity permutation is obviously even and the inverse of an even permutation is also even, we arrive at the group of all even permutations of degree n, denoted by A_n; it is called the *alternating* group of degree n. It is a finite group of order $n!/2$ and is non-commutative for $n \geqq 4$.

The odd permutations of degree n do not form a group, since the product of two odd permutations is even.

It is now easy to verify that there exists a homomorphic mapping of the symmetric group S_n onto the group of order 2 in Example 7: every even permutation is to be associated with the number 1, every odd permutation with the number -1.

13. We take an arbitrary set M and consider all the possible one-to-one

mappings of the set onto itself. Since the result of performing two such mappings in succession again yields a one-to-one mapping of M onto itself, we have here an operation in the set of these mappings. Its associativity has been proved in § 1, the identity mapping is the unit element, and every mapping has an inverse; hence we obtain the *group S_M of all one-to-one mappings of the set M onto itself.* If the set M is finite and consists of n elements, then this group turns out to be the symmetric group of degree n. It is clear that if the sets M and M' have the same cardinal number then the groups S_M and $S_{M'}$ are isomorphic.

This example is important, because in applications groups appear for the most part as *groups of transformations*, that is, as groups of one-to-one mappings of a set M onto itself with multiplication defined as the performing of mappings in succession. Not all such mappings are usually considered, it is true, but only those that have some additional property α or, briefly, *α-transformations.* In order that all α-transformations of a set M constitute a group it is obviously sufficient that the following conditions be satisfied:

(1) the product of two α-transformations must have the property α;

(2) the inverse mapping of an α-transformation must have the property α.

These remarks may be used to construct further examples, where in each case the group consists of all the α-transformations of some set M for some property α. In particular, *multiplication in these examples should always be understood as the performing of the mappings in succession.*

14. We take an infinite set of cardinal number $\mathfrak{m}$ and consider those one-to-one mappings of the set onto itself that affect only a finite, though possibly an arbitrarily large, number of symbols. These mappings constitute a periodic group of cardinal number $\mathfrak{m}$ which is called the *symmetric group of cardinal number* $\mathfrak{m}$. Since the above-defined concept of an even permutation can be adapted to the mappings with which we deal here—only the symbols actually affected need be considered—we obtain in a similar way the *alternating group of cardinal number* $\mathfrak{m}$.[b]

15. We consider an n-dimensional vector space over the field of real numbers (or, more generally, over an arbitrary field). The *non-degenerate linear transformations* of this space constitute a group under multiplication, which is non-commutative for $n \geqq 2$; from higher algebra the reader will recall that between the non-degenerate linear transformations and the *non-singular square matrices* of order n there exists a one-to-one correspondence that carries the product of transformations into the product of the corresponding matrices. Our group is therefore isomorphic to the *multiplicative group of non-singular matrices of order n.* We note that each of these groups may be mapped homomorphically onto the multiplicative group of

real numbers different from zero: We need only associate each matrix with its determinant and use the fact that the determinant of a product of matrices is equal to the product of the determinants of the factors.

16. The *rigid motions* of a three-dimensional euclidean space constitute a group. This is also true for those motions that leave a given point fixed, that is, the *rotations* about this point.

17. The rotations of a euclidean space under which a given cube with its center at the fixed point is mapped into itself constitute a group. This *group of the rotations of the cube* is finite, since its elements are in one-to-one correspondence with certain permutations of the set of vertices of the cube and, as is easily verified, it is non-commutative. The groups of rotations of other regular polyhedra are defined similarly.

CHAPTER II

SUBGROUPS

§ 5. Subgroups

A subset H of a group G is called a *subgroup* of G if it is itself a group with respect to the operation defined in G.

In order to establish that a (non-empty) subset H of a group G is a subgroup it is sufficient to verify:

(1) that the product of any two elements of H is contained in H;

(2) that the inverse of each element of H is also contained in H. For, the associative law holds in H because it holds for all elements of G, and since H is not empty it follows from properties (2) and (1) that the unit element of G belongs to H.

In the case of finite or, more generally, periodic groups the verification of property (2) is superfluous. For if an element a of order n belongs to H, then H must, by property (1), contain all the positive powers of a and must therefore contain a^{n-1}, the inverse of a. The example of the additive group of integers and the set of positive integers contained therein shows that in the general case it is necessary to verify property (2).

We emphasize that it is not permissible to replace the above definition of a subgroup by one which would make any subset of G into a subgroup merely because it happens to be a group. Thus, the set of positive rational numbers is a group with respect to *multiplication* and is contained as a subset in the *additive* group of all rational numbers, but it is not a subgroup of that additive group.

The relation "H is a subgroup of G" is transitive: If H is a subgroup of G and G a subgroup of $\overline{G}$, then H is also a subgroup of $\overline{G}$.

The subset of a group G which consists of the single element 1 is obviously a subgroup of G. This subgroup is called the *unit subgroup* or *trivial subgroup* of G and is denoted by the symbol E. On the other hand, the group G itself is one of its own subgroups. Every subgroup that is distinct from the whole group is called a *proper* subgroup.

Many of the groups in § 4 are subgroups of other of the groups listed there. Thus, the additive group of even numbers is a subgroup of the additive group of all integers and the latter, in turn, is a subgroup of the additive

group of rational numbers. All these groups and, more generally, all additive groups of numbers are subgroups of the additive group of complex numbers. The multiplicative group of positive rational numbers and the group consisting of the numbers 1 and -1 are subgroups of the multiplicative group of all non-zero rational numbers. The alternating group of degree n is a subgroup of the symmetric group of the same degree. All groups of α-transformations of a set M, in particular Examples 14-17 in § 4, are subgroups of the group S_M of all one-to-one mappings of the set M onto itself.

The first example mentioned above shows that a group may well be isomorphic to one of its proper subgroups; an isomorphism between the additive group of integers and that of even numbers was established in § 4. It is clear, however, that no finite group can be isomorphic to one of its proper subgroups.

Under a homomorphic (or, in particular, an isomorphic) mapping φ of a group G onto a group $\overline{G}$, a subgroup H of G is mapped onto a subset $\overline{H}$ of $\overline{G}$. The mapping φ is homomorphic (or, in particular, isomorphic) for H and therefore, as was proved in § 3, the *set* $\overline{H}$ is a group with respect to the operation defined in $\overline{G}$, i.e. *it is a subgroup of* $\overline{G}$. We shall say that the given homomorphic mapping in G *induces* homomorphic mappings in all its subgroups.

If two groups G and G' are given and if G' is isomorphic to a subgroup H of G, then we shall say that the group G' can be mapped isomorphically *into the group* G or that G' can be *embedded in* G. If, in particular, H coincides with G we shall speak of a mapping *onto* the group G. One must, however, take into account here that G' can in general be mapped isomorphically onto H in many different ways. Moreover, H need not be the only subgroup of G isomorphic to G': all the subgroups of G that are isomorphic to G' are isomorphic to each other, but they are different subsets of G and must therefore be distinguished inside G. Every isomorphic mapping of G' onto one of the subgroups of G that are isomorphic to G' gives only one of the possible ways of embedding G' in G.

Let us consider, for example, the symmetric group S_n of degree n. If i is one of the permuted symbols $1, 2, \ldots, n$, then all the permutations of S_n that leave the symbol i in place constitute a subgroup of S_n that is isomorphic to S_{n-1}. We can say, therefore, that *the symmetric group of degree* $n-1$ *can be embedded in the symmetric group of degree* n; we see, moreover, that the group S_n contains several distinct subgroups isomorphic to S_{n-1}.

If two groups A and B are given and if each of them is isomorphic to a

proper subgroup of the other, then it does not follow that the groups themselves are isomorphic, as one might at first think. It only follows that each of these groups is isomorphic to one of its proper subgroups, and this is not so very surprising; for if

$$A \simeq B' \subset B$$

and if under the given isomorphism of B into A the subgroup B' is mapped onto the subgroup A'', then A'' is isomorphic to A.

The following theorem shows that the subgroups of the finite symmetric groups essentially exhaust all the finite groups.

THEOREM OF CAYLEY. *Every finite group of order n is isomorphic to a subgroup of the symmetric group of degree n.*

For let G be a group of order n, and let the elements of G, written in a definite order, be

$$a_1, a_2, \ldots, a_n. \tag{1}$$

If b is an arbitrary element of G, then all the products $a_i b = a_{\beta_i}$ $(i = 1, 2, \ldots, n)$ are distinct, so that the system

$$a_{\beta_1}, a_{\beta_2}, \ldots, a_{\beta_n} \tag{2}$$

also contains all the elements of G and differs from (1) only in the order of the elements. We now associate with the element b the permutation

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ \beta_1 & \beta_2 & \ldots & \beta_n \end{pmatrix}. \tag{3}$$

To every element of G there corresponds in this way a well-defined permutation of degree n. Two distinct elements of G give rise to distinct permutations, since from $a_1 b = a_1 b'$ it would follow that $b = b'$. Let us find the permutation corresponding to the product bc, where c is also an element of G. If to c there corresponds the permutation

$$\begin{pmatrix} \beta_1 & \beta_2 & \ldots & \beta_n \\ \gamma_1 & \gamma_2 & \ldots & \gamma_n \end{pmatrix}, \tag{4}$$

so that

$$a_{\beta_i} c = a_{\gamma_i},$$

then from

$$a_i (bc) = a_{\beta_i} c = a_{\gamma_i}$$

it follows that to the element bc there corresponds the permutation

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \gamma_1 & \gamma_2 & \cdots & \gamma_n \end{pmatrix},$$

which is the product of the permutation (3) by the permutation (4). Thus we have proved that G is mapped isomorphically into the group S_n. The subgroup of S_n that corresponds to G obviously has the following properties: The order of the subgroup is equal to the number of permuted symbols, and each permutation in the subgroup with the exception of the unit element displaces each of the symbols. Such subgroups of the symmetric groups are called *regular*.

From the theorem of Cayley and the obvious remark that *a finite group has only a finite number of subgroups* it follows that *there exist only a finite number of non-isomorphic finite groups of a given order n*. Therefore, *the set of all non-isomorphic finite groups is countable*, since it is the sum of a countable set of finite sets.

The theorem of Cayley can be extended to infinite groups: Every group of cardinal number $\mathfrak{m}$ is isomorphic to a subgroup of the group $S_{\mathfrak{m}}$ of all one-to-one mappings of the set $\mathfrak{m}$ onto itself (cf. § 4, Example 13).[1] The proof remains completely unaltered. We have only to justify the assertion that after the multiplication of all group elements on the right by b we again obtain all the elements of the group; this, however, follows easily from the axiom of the existence of a left quotient.

The concept of a subgroup is fundamental in the theory of groups. The entire content of group theory is more or less linked up with questions about the existence, in a group, of subgroups having one or another special property, about groups that can be embedded in a given group, about properties that characterise the mutual disposition of subgroups in a group, about methods of constructing a group from its subgroups, etc. The classification of various special types of groups also depends mainly on the concept of a subgroup.

§ 6. Systems of Generators. Cyclic Groups

The intersection of two subgroups H and K of a group G cannot be empty, since every subgroup of G contains the element 1. *The intersection is, in fact, a subgroup of* G: if $D = H \cap K$ is the intersection of the sub-

[1] That is, the unrestricted symmetric group $S_{\mathfrak{m}}$.[b]

groups H and K, and if elements a, b belong to D, then their product and their inverses belong to H as well as to K and hence to D.

If subgroups of a group G are given—not just two, but an arbitrary finite or even infinite set—then the product of any two elements of the intersection of all these subgroups lies in each of them and therefore in their intersection. This holds also for the inverses. Hence *the intersection of any set of subgroups of a group G is itself a subgroup of G*. The intersection of *all* the subgroups of a group G is obviously the unit subgroup E.

Let M be an arbitrary non-empty subset of a group G (such a subset is sometimes called a *complex*). The intersection of all the subgroups of G that contain all the elements of M—one of these subgroups is, of course, the group G itself—is called the subgroup *generated* by the subset M and is denoted by the symbol $\{M\}$. Clearly it is contained in every subgroup of G that contains the whole subset M.

If the subset M consists of a single element a, then the subgroup $\{a\}$ generated by it is called the *cyclic subgroup of a*. All the powers of a belong, of course, to the subgroup $\{a\}$; but these powers already constitute a subgroup, since the product of a^m and a^n is equal to a^{m+n}, and the inverse of a^n is a^{-n} (cf. § 3). Hence it follows that *the cyclic subgroup $\{a\}$ consists of all the powers of a*. This shows that the cyclic subgroup $\{a\}$ is countable if a is an element of infinite order and finite if a is of finite order; in this case the order of $\{a\}$ is equal to the order of a.

A group that coincides with one of its cyclic subgroups, i.e. that consists of the powers of one of its elements, is called a *cyclic group*. An element whose powers constitute the given cyclic group is called a *generating element* or *generator* of the group. Every cyclic group is obviously commutative. An example of an infinite cyclic group is the additive group of integers, and one of its generators is the number 1; an example of a finite cyclic group of order n is the multiplicative group of the n-th roots of unity for $n = 1, 2, \ldots$. The following theorem shows that these examples essentially exhaust all cyclic groups.

All infinite cyclic groups are isomorphic; all finite cyclic groups of a given order n are isomorphic.

For, an infinite cyclic group with generator a can be mapped one to one onto the additive group of integers if we associate with a^k the number k; the isomorphism of this mapping follows from the fact that in the multiplication of powers of a the exponents are added. Similarly, we may obtain an isomorphic mapping of each cyclic group of order n onto the group of the n-th roots of unity.

This theorem allows us to speak in the sequel simply of *the infinite cyclic group* or of *the cyclic group of order n*.

Every subgroup of a cyclic group is cyclic.

For if $G = \{a\}$ is a cyclic group with generator a, of infinite order or of finite order n, and if H is a subgroup of G different from E, and if, further, the smallest positive power of a in H is a^k, then $\{a^k\} \subseteq H$. Suppose that H contains also an element a^l, where $l \neq 0$ and l is not divisible by k. Then if $(k, l) = d$, $d > 0$, is the greatest common divisor of k and l, there exist integers u and v for which $ku + lv = d$; therefore H must contain the element

$$(a^k)^u (a^l)^v = a^d;$$

but since $d < k$, this is in contradiction with the choice of the element a^k. Hence $H = \{a^k\}$.

In the infinite cyclic group with generator a we can also choose a^{-1} as generator; the cyclic subgroup generated by any other power of a is not the whole group. *In the cyclic group $\{a\}$ of order n we can choose the element a^k, $0 \leqq k < n$, as generator if and only if k and n are relatively prime.*

For if $(k, n) = 1$, then there exist a u and a v for which

$$ku + nv = 1.$$

Hence

$$(a^k)^u = a^{1-nv} = a \cdot a^{-nv} = a.$$

If, on the other hand, we have $(a^k)^s = a$ for some k, then the difference of the exponents $ks - 1$ must be divisible by n (cf. § 3):

$$ks - 1 = nq$$

so that

$$ks - nq = 1,$$

and $(k, n) = 1$.

If M is now again an arbitrary subset of a group G then, just as in the case of cyclic subgroups, it is easy to give a rule by which the elements of the subgroup $\{M\}$ are formed from the elements of M. The subgroup $\{M\}$ must contain the positive and negative powers of all the elements of M, and hence also all the possible products of any finite number of these powers taken in an arbitrary order. But all the elements of G that can be represented, possibly in more than one way, as a product of a finite number of powers of the elements of M, obviously form a subgroup of G that contains

all the elements of M. Thus we have proved that *the subgroup generated by a subset M consists of all the group elements that can be written as products of a finite number of powers of elements of M.*

If, in particular, a set of subgroups of a group G is given and if M is the set-theoretical union of these subgroups, that is, the set consisting of all the elements of G that lie in at least one of the given subgroups, then $\{M\}$ is the smallest subgroup of G that contains all these subgroups. This subgroup $\{M\}$ is called the *subgroup generated by*, or *join of*, the given subgroups and is denoted by the symbol $\{A_\alpha\}$, $\alpha \in N$, if the given subgroups are A_α, (where α ranges over some index set N); in particular, if only two subgroups A and B are given, then the subgroup $\{M\}$ is denoted by the symbol $\{A, B\}$, etc. From the above remarks we see that *the subgroup generated by a set of subgroups of G consists of all the elements that can be written as products of a finite number of elements from the given subgroups.*

If the subgroup $\{M\}$ generated in a group G by one of its subsets M coincides with the group G itself, then the subset M is called a *system of generating elements* or simply a *system of generators*, or a *generating set* of this group. Every group possesses systems of generators—it is sufficient to take all the elements of the group, or the set of all elements other than 1.[c] From the above remark on the subgroups generated by a subset it follows that *a subset M is a system of generators of a group G if and only if every element of G can be written in at least one way as a product of a finite number of powers of elements of M.*

If

$$G = \{M\}$$

then we call M an *irreducible system* of generators if no proper subsystem of M is a system of generators for G.

Examples: 1. Every cyclic group has a system of generators consisting of a single element, namely a generating element of the group. Conversely, every group with one generating element is cyclic. Note that in a cyclic group one can in general[1] choose irreducible systems of generators which consist of more than one element. Thus, for example, the numbers 2 and 3 form an irreducible system of generators for the additive group of integers.

2. It was mentioned in § 4 that every permutation of degree n is a product of transpositions. It follows that one system of generators of the symmetric group of degree n is the set of all transpositions contained in

[1] The exceptions are E and the cyclic groups of prime-power order; see § 17. [*Trans.*]

that group. The symmetric group of degree n can also be generated by two elements:

$$a = (12),$$
$$b = (12 \ldots n).$$

For,

$$b^{-k} a b^k = (k+1,\ k+2),\ k \leqq n-2.$$

If, now, $i < j-1$, then

$$(j,\ j-1) \ldots (i+2,\ i+1)(i,\ i+1)(i+1,\ i+2) \ldots (j-1,\ j) = (ij),$$

so that the subgroup $\{a, b\}$ contains all the transpositions and is therefore the whole symmetric group.

3. The numbers

$$1, \frac{1}{2}, \frac{1}{6}, \frac{1}{24}, \ldots, \frac{1}{n!}, \ldots$$

form a system of generators for the additive group of rational numbers R. It is easy to see that every infinite subset of this set is also a system of generators for R. Moreover, we can show that *the additive group of rational numbers R has no irreducible system of generators.* For let M be any system of generators of R and let a be an arbitrary element of M. We denote by H the subgroup generated by the set M' consisting of all elements of M except a; the set M' cannot be empty, since otherwise all the rational numbers would be multiples of a, which is not true. If b is an arbitrary element of M', then it follows from the properties of rational numbers that there exists an integer k, different from zero, for which ka is a multiple of b and hence is contained in H. The number $(1/k)a$, which belongs to R, must be expressible as a sum of a finite number of rational numbers which are multiples of numbers from M, that is,

$$(1/k)a = sa + h,$$

where s is an integer, possibly zero, and h is an element of H. Hence

$$a = s(ka) + kh,$$

so that a is contained in H and hence $H = R$. The set M' is, therefore, a system of generators for R.

4. The multiplicative group of positive rational numbers has an irreducible system of generators consisting of all the prime numbers.

If a group G has a system of generators consisting of a finite number of elements, then G is called a *group with a finite number of generators* or a *finitely generated group*. All finite and all cyclic groups are obviously of this type. The example of the infinite cyclic group shows that the finiteness of the group does not follow from the finiteness of the number of generators.

Every system of generators of a finitely generated group contains a finite subsystem which is an irreducible system of generators of the group.

Since a finite system of generators can always be made irreducible by the omission of superfluous elements we need only show that under our assumptions every infinite system of generators contains a finite subset which is also a system of generators for the group in question. Let G be a group with generators $a_1, a_2, \ldots, a_n$

$$G = \{a_1, a_2, \ldots, a_n\},$$

and let M be any other system of generators of G. Every element a_i, $i = 1, 2, \ldots, n$, can be written in the form of a product of powers of a *finite* number of elements of M. If for each i, $i = 1, 2, \ldots, n$, we choose one of these representations and collect all the elements of M that occur in these representations, we obtain a finite subset M' of M for which the subgroup $\{M'\}$ contains all the elements $a_1, a_2, \ldots, a_n$ and therefore coincides with G.

Note that distinct irreducible systems of generators of a finitely generated group may, in general, contain different numbers of elements (cf. Example 1).

Every homomorphic image of a finitely generated group is itself finitely generated.

Indeed, if

$$G = \{a_1, a_2, \ldots, a_n\}$$

and if the homomorphism φ maps G onto $\bar{G}$, then the elements

$$a_1\varphi, a_2\varphi, \ldots, a_n\varphi \tag{1}$$

generate $\bar{G}$. For if $\bar{a}$ is an arbitrary element of G and a is one of its originals in G, then $\bar{a}$ can be expressed in terms of powers of the elements (1) in the same way as a is expressed in terms of powers of $a_1, a_2, \ldots, a_n$. Some of the elements (1) may, of course, coincide, so that we obtain for $\bar{G}$ a *system of generators with repetitions*. These repetitions could be excluded. However, we shall continue to admit such systems of generators.

Every infinite group with a finite number of generators is countable.

For if $a_1, a_2, \ldots, a_n$ are the generators of G, then every element of G can be written in the form of a product

$$a_{i_1}^{\alpha_1} a_{i_2}^{\alpha_2} \ldots a_{i_s}^{\alpha_s}$$

(in general, in several different ways); each i_k is one of the numbers $1, 2, \ldots, n$ and we may have $i_k = i_l$ for $k \neq l$. Let us define the *length* of this product to be the sum of the absolute values of the exponents:

$$h = |\alpha_1| + |\alpha_2| + \ldots + |\alpha_s|.$$

It is easy to see that for a given length h there exist only a finite number of products of powers of the generators $a_1, a_2, \ldots, a_n$. The set of all power products of these elements being, therefore, the sum of a countable set of finite sets, is countable, so that G cannot be more than countable.

Examples 3 and 4 of the present section show that there exist countable groups that have no finite system of generators. Finitely generated groups are therefore a class of groups intermediate between the classes of finite and countable groups.

Every subgroup of a finitely generated group is, of course, at most countable. In Chapter IX, however, we shall encounter examples of finitely generated groups in which certain subgroups do not have finite systems of generators. Finitely generated groups will be studied in greater detail in Chapter X.

We remark that we can prove in the same manner as above that if a group G has an infinite system of generators (without repetitions) of cardinal number $\mathfrak{m}$, then the group has the cardinal number $\mathfrak{m}$.

§ 7. Ascending sequences of groups

Let

$$A_1, A_2, \ldots, A_n, \ldots,$$

be subgroups of a group G which form an *ascending sequence*: every subgroup A_n is contained in A_{n+1}, $A_n \subset A_{n+1}$, $n = 1, 2, \ldots$. We show that the set-theoretical union B of this ascending sequence of subgroups is itself a subgroup of G and is therefore the group generated by the A_n: Each element b of the set B lies in some subgroup A_n (and so in all A_k with $k \geqq n$); then b^{-1} lies in A_n also and hence in B; and if two elements b_1 and b_2 of B

are chosen, lying in A_n and A_k respectively, where $k \geqq n$ say, then both b_1 and b_2 lie in A_k, and their product $b_1 b_2$ also lies in A_k and hence in B. Thus we have shown that the set B is a subgroup of G.

Instead of a countable sequence of subgroups whose ordering is of the type of the natural numbers, we could have taken an arbitrary set of subgroups with the property that for any two subgroups A_α and A_β of this set one is contained in the other.[d] The set-theoretical union of these subgroups is itself a subgroup of G; this is proved by a literal repetition of the argument given above.

In the sequel we shall frequently have occasion to use the following

THEOREM. *If in a group G a subset M and a subgroup A are given, whose intersection is a subset D, then G has at least one subgroup that contains A, has the intersection D with M, and is not contained in any larger subgroup with these two properties.*

For let the elements of G be well-ordered:

$$1 = a_0, a_1, \ldots, a_\alpha, \ldots.$$

We put $A_0 = A$. Suppose now that for all $\beta < \alpha$ we have already chosen subgroups A_β of G which form an ascending sequence and all of which have the intersection D with M. If B_α is the union of the ascending sequence of subgroups A_β, $\beta < \alpha$, then we choose as A_α the subgroup $\{B_\alpha, a_\alpha\}$ if the intersection of this subgroup with M is D, and the subgroup B_α otherwise. The union $\bar{A}$ of the ascending sequence of all the subgroups A_α is the required subgroup: the intersection of $\bar{A}$ with M is obviously D; but if an element a_γ lies outside $\bar{A}$, then the intersection of $\{\bar{A}, a_\gamma\}$ with M is different from D, since we already have $\{B_\gamma, a_\gamma\} \cap M \neq D$.

It follows, in particular, that if G has a subgroup which has an empty intersection with the subset M, then among all such subgroups there is at least one that is maximal.

It can happen that the set-theoretical union of an ascending sequence of subgroups

$$A_1 \subseteq A_2 \subseteq \ldots \subseteq A_n \subseteq \ldots$$

of a group G coincides with G itself. Let us give a few examples of this.

1. The additive group of rational numbers R is the union of the following ascending sequence of cyclic subgroups:

$$\{1\} \subset \left\{\frac{1}{2}\right\} \subset \left\{\frac{1}{6}\right\} \subset \ldots \subset \left\{\frac{1}{n!}\right\} \subset \ldots$$

2. Let G be the multiplicative group of positive rational numbers and let

$$p_1, p_2, \ldots, p_n, \ldots$$

be all the prime numbers in ascending order. If

$$A_n = \{p_1, p_2, \ldots, p_n\}$$

—this is the collection of all rational numbers for which the numerator and denominator in reduced form contain only prime numbers from the system $p_1, p_2, \ldots, p_n$—then the group G is the union of the ascending sequence of subgroups A_n, $n = 1, 2, \ldots$.

3. Let S_ω be the restricted symmetric group on a countable set of symbols $x_1, x_2, \ldots$ (see § 4, Example 14). The subgroups S_n of this group consisting of those mappings that leave each of the symbols

$$x_{n+1}, x_{n+2}, \ldots$$

unchanged is obviously isomorphic to the symmetric group of degree n, and the group S_ω is the union of the subgroups S_n, $n = 1, 2, 3, \ldots$.

On the other hand, the following theorem holds:

A finitely generated group cannot be the union of an ascending sequence of proper subgroups.

Suppose the group G has a finite system of generators

$$G = \{a_1, a_2, \ldots, a_n\},$$

and is the union of an ascending sequence of proper subgroups

$$H_1 \subseteq H_2 \subseteq \ldots \subseteq H_k \subseteq \ldots.$$

Each element a_i, $i = 1, 2, \ldots, n$, belongs, as indeed every element of G does, to some subgroup H_{k_i} and so belongs to all the subgroups H_k with $k \geqq k_i$. If

$$l = \max(k_1, k_2, \ldots, k_n),$$

then the subgroup H_l contains $a_1, a_2, \ldots, a_n$ and cannot therefore be a proper subgroup of G.

This proof carries over to the case when we have in a finitely generated group an arbitrarily ordered ascending sequence of proper subgroups.

The union of an ascending sequence of countable subgroups and, in

particular, of finitely generated subgroups is clearly countable. Conversely, *every countable group is the union of an ascending sequence of finitely generated subgroups.*

For let the elements of a countable group G be numbered in an arbitrary way

$$g_1, g_2, \cdots, g_n, \cdots.$$

The subgroups

$$H_n = \{g_1, g_2, \ldots, g_n\},$$

are finitely generated. Each is contained in all the succeeding ones (though $H_n = H_{n+1}$ is possible) and the group G is the union of this ascending sequence of subgroups.

We now proceed to explain a construction that allows us to speak of an *ascending sequence of given groups* which are not *a priori* subgroups of a containing group.

Suppose we have the groups

$$G_1, G_2, \ldots, G_n, \ldots \tag{1}$$

and have for each n an isomorphic mapping φ_n of the group G_n into G_{n+1} (i.e. onto a subgroup of G_{n+1}).

$$g_n\varphi_n = g_{n+1}, \quad g_n \in G_n, \quad g_{n+1} \in G_{n+1}. \tag{2}$$

The groups (1) and the isomorphisms (2) enable us to construct a well-defined group $\overline{G}$ in the following way.

We define a *thread* to be any sequence of elements

$$\gamma = g_k, g_{k+1}, \ldots, g_n, \cdots \tag{3}$$

with the following properties:

1) $k \geqq 1$,

2) $g_n \in G_n$,

3) if $k > 1$, then g_k is not the image of any element of G_{k-1} under the isomorphism φ_{k-1},

4) g_{n+1} is the image of g_n under φ_n

$$g_n\varphi_n = g_{n+1}, \quad n = k, k+1, \ldots.$$

If two threads are given

$$\gamma' = g'_k, \quad g'_{k+1}, \ldots, g'_n, \ldots,$$
$$\gamma'' = g''_l, \quad g''_{l+1}, \ldots, g''_n, \ldots,$$

and if $k \neq l$, then the sequence of elements

$$g'_m g''_m, \quad g'_{m+1} g''_{m+1}, \ldots, g'_n g''_n, \ldots, \tag{4}$$

where $m = \max(k, l)$, is itself a thread. For

$$(g'_n g''_n)\varphi_n = g'_n \varphi_n \cdot g''_n \varphi_n = g'_{n+1} g''_{n+1},$$

and the element $g_m' g_m''$ is not the image of any element under the isomorphism φ_{m-1}, since one of the factors is such an image and the other is not. We shall call the thread (4) the *product* of the given threads and denote it by $\gamma'\gamma''$. If $k = l$, then the element $g_m' g_m''$ may have an original in G_{m-1} under the isomorphism φ_{m-1}. In that case we can make the sequence (4) into a thread by adding suitable elements at the beginning; moreover, this completion is uniquely determined. The thread so obtained will be called the product $\gamma'\gamma''$.

That the multiplication of threads just defined is associative follows from the associativity of the operations in the groups G_n. The unit element is the thread that consists of the unit elements of all the groups G_n. The inverse thread of (3) is

$$g_k^{-1}, \quad g_{k+1}^{-1}, \ldots, g_n^{-1}, \ldots.$$

The set of all threads is, therefore, a group with respect to multiplication. We denote this group by $\overline{G}$; it is called the (direct) *limit group* for the sequence (1) with the isomorphisms (2). We can also say that the groups (1) form an *ascending sequence* in virtue of the isomorphisms (2) and that $\overline{G}$ is the *union* of this ascending sequence. For, let us collect all the threads that contain an element of G_s, in other words, that begin in the groups G_k with $k \leqq s$. These threads constitute a subgroup $\overline{G}_s$ of $\overline{G}$ which is isomorphic to G_s. The subgroups

$$\overline{G}_1, \overline{G}_2, \ldots, \overline{G}_n, \ldots \tag{5}$$

are embedded in one another in the same way as the groups (1) by the isomorphisms (2); the set-theoretical union of the ascending sequence of subgroups (5) is the whole group $\overline{G}$.[e]

The group $\overline{G}$ is uniquely defined by the groups (1) and the isomorphisms (2). We cannot restrict ourselves to the given groups (1) only. For, the additive group of rational numbers R is the union of a countable ascending sequence of infinite cyclic groups (see above, Example 1). But so is the additive group of dyadic fractions R_2, since it is the sum of an ascending sequence of proper subgroups

$$\{1\} \subset \left\{\frac{1}{2}\right\} \subset \left\{\frac{1}{4}\right\} \subset \ldots \subset \left\{\frac{1}{2^n}\right\} \subset \ldots .$$

The groups R and R_2 are not isomorphic since, for example, there is no element x in R_2 that satisfies the equation

$$3x = 1,$$

while this equation has a solution in R. This shows that the union of an ascending sequence of groups depends not only on the groups themselves, but also on the manner in which each is embedded in the following.

The above construction can easily be extended to the case of an arbitrarily ordered set of groups of arbitrary cardinal number. We need only assume that for each pair of groups of this set, say G_α, G_β, the first of which precedes the second, an isomorphic mapping $\varphi_{\alpha\beta}$ of G_α into G_β is defined, and that if the isomorphisms $\varphi_{\alpha\beta}$ and $\varphi_{\beta\gamma}$ and hence $\varphi_{\alpha\gamma}$ are defined, then $\varphi_{\alpha\gamma}$ coincides with the result of performing the isomorphisms $\varphi_{\alpha\beta}$ and $\varphi_{\beta\gamma}$ in succession. The details of this construction are left to the reader.

Let us use our construction to form a group that will be rather important in the sequel, especially in the theory of abelian groups. If a prime number p is given, then every cyclic group of order p^n has a unique cyclic subgroup of order p^{n-1}. Thus for each n an isomorphic mapping of a cyclic group of order p^{n-1} into a cyclic group of order p^n is defined; we can therefore speak of the ascending sequence of cyclic groups of order p^n, $n = 1, 2, \ldots$. The union of this sequence is called a *group of type* p^∞.[1] It is easy to verify that a group of type p^∞ is isomorphic to the multiplicative group of roots of unity whose degrees are powers of p.

Since a cyclic group $\{a\}$ of order p^n has, for every k less than n, a unique cyclic subgroup of order p^k, namely $\{a^{p^{n-k}}\}$, the group P of type p^∞ also has for each k, $k = 1, 2, \ldots$, a *unique* cyclic subgroup of order p^k and coincides with the union of the ascending sequence of these subgroups. Let these be the subgroups $\{a_k\}$, $k = 1, 2, \ldots$; we also put $\{a_0\} = 1$. Now

[1] Sometimes also called a *quasi-cyclic* group.

if U is an arbitrary proper subgroup of P, then it cannot contain all the a_k. Let a_{n+1} be the first generator that does not lie in U. *Then U coincides with the cyclic subgroup* $\{a_n\}$. For if an element a_k, with $k > n+1$, were contained in U, then U would also contain the cyclic subgroup $\{a_k\}$ and hence the element a_{n+1}. And if U contained an element b not in $\{a_n\}$, then we could find a k, with $k > n$, for which

$$b \notin \{a_{k-1}\}, \qquad b \in \{a_k\}.$$

However, we would then have

$$\{b\} = \{a_k\},$$

so that a_k would lie in U after all. Thus we have proved that *every proper subgroup of a group of type p^∞ is a finite cyclic group of order p^n.*

From results of Chap. VII it will follow that the groups of type p^∞ (for all prime numbers p) are the only infinite abelian groups whose proper subgroups are all finite. The problem, raised by O. J. Schmidt, whether there exist infinite non-commutative groups with this property, is still open.

CHAPTER III

NORMAL SUBGROUPS

§ 8. Decomposition of a group with respect to a subgroup

If two subsets M and N are given in a group G, then we define the *product* MN to be the set of all elements of G that are equal to the product of an element of M by an element of N.[1] If one of the subsets M, N consists of a single element a, then we have the definition of the *product aN of an element by a subset* or *the product Ma of a subset by an element.*

Multiplication of subsets is associative,

$$(MN)P = M(NP),$$

but not, in general, commutative. If for two subsets M and N the equality

$$MN = NM$$

holds (that is, if for any two elements a and b, $a \in M$, $b \in N$, there exist elements a' and a'' in M, b' and b'' in N for which $ab = b'a'$, $ba = a''b''$) then the M and N are called *permutable.* Special cases are *permutability of an element and a subgroup, permutability of two subgroups,* and so on.

We remark that if A and B are subgroups of G, then the subset AB need not be a subgroup, that is, *the product AB is, in general, different from the subgroup $\{A, B\}$ defined in* § 6. We can, however, assert that

$$AB \subseteq \{A, B\}.$$

The subgroup $\{A, B\}$ generated by two subgroups A and B of a group G coincides with the product AB if and only if A and B are permutable.

For if

$$AB = \{A, B\},$$

then for any a in A and b in B the element ba, which is contained in $\{A, B\}$,

[1] An element may be equal to several distinct products of this form; such an element shall not, however, be counted more than once in MN.

must be equal to some element $a'b'$, $a' \epsilon A$, $b' \epsilon B$, so that

$$BA \subseteq AB.$$

We now show that the element ab is, in turn, contained in the product BA. Making use of the above inclusion we obtain

$$(ab)^{-1} = b^{-1}a^{-1} = a''b'', \quad a'' \epsilon A, \quad b'' \epsilon B;$$

and hence $ab = b''^{-1}a''^{-1}$, so that $AB \subseteq BA$, and therefore $AB = BA$.

Conversely, if A and B are permutable, then every product of three elements of the form $a_1 b a_2$ or $b_1 a b_2$ can obviously be written in the form $a'b'$; in the first case, we need only replace ba_2 by some product $a_2'b'$ equal to it (such a product exists, since A and B are permutable) and then put $a_1 a_2' = a'$; in the second case, we replace $b_1 a$ by $a'b_1'$ and then put $b_1' b_2 = b'$. Now if it has already been proved that every product of n factors, $n \geqq 3$, taken alternately from A and B, is contained in AB, and if a product of the same kind but with $n + 1$ factors is given, then we replace the product of the first n factors by a product $a'b'$, equal to it, and again arrive at the case of three factors. It follows that every element of the subgroup $\{A, B\}$ is contained in the subset AB.

Subgroups of an abelian group are, of course, always permutable. So are subgroups A and B of any (finite or infinite) symmetric group provided that every symbol displaced by one of the subgroups A, B remains unaltered under all the permutations of the other group—indeed, in this case each element of A is permutable with every element of B (that is, the subgroups are *element-wise* permutable). We leave it to the reader to show that in the symmetric group of degree 3 the cyclic subgroups generated by the permutations

$$(123) \text{ and } (12)$$

are permutable, but those generated by

$$(12) \text{ and } (23)$$

are not.

We note for later use that if A is a subgroup of a group G, then

$$AA = A.$$

For it is clear that $AA \subseteq A$; but the product of A by 1 already yields the whole of A.

The multiplication of subsets of a group has an important application in the decompositions of a group with respect to a subgroup; these play a fundamental rôle in the whole theory.

Let H be a subgroup of a group G. If a is an arbitrary element of G, then the product aH is called the *left coset of H in G determined by a*. Clearly, a is contained in the coset aH, since H contains the unit element.

If b is an arbitrary element of aH, then the left cosets aH and bH coincide, that is, *every left coset is determined by any of its elements.* For if $b = ah_0$, $h_0 \in H$, then

$$bh' = a(h_0 h') \text{ and } ah'' = b(h_0^{-1} h''), \quad h', \ h'' \in H.$$

We shall also say that an arbitrary element of a left coset is a *representative* of that coset.

It follows that *any two left cosets of H in G are either equal or disjoint*, that is, their intersection is empty. We see that the whole group G is divided into disjoint cosets with respect to a subgroup H. This is called the *left decomposition of G with respect to H*. One of the cosets of this decomposition is H itself: if the element a is contained in H, then $aH = H$.

Note that two elements a and b lie in the same coset of H in G if and only if $a^{-1}b$ is contained in H.

The concept of a left coset is illustrated by the following

Examples. 1. If G is the additive group of integers and H the subgroup of numbers divisible by 4, then two numbers a and b lie in the same left coset of H in G if and only if they leave the same remainder on division by 4. Thus the left decomposition of G with respect to H consists of four cosets: H itself and the sets of numbers which on division by 4 give the remainders 1, 2, and 3, respectively.

2. If G is the symmetric group of degree 3 and $H = \{(12)\}$, then the left decomposition of G with respect to H consists of three cosets; the subgroup H itself, consisting of the elements 1 and (12), the coset $(13) \cdot H$, consisting of the elements (13) and (132), and the coset $(23) \cdot H$, consisting of the elements (23) and (123).

3. If G is the group of non-singular matrices of degree n with real elements, and H the subgroup of matrices with determinant 1, then we obtain the left decomposition of G with respect to H if we collect into one coset all the matrices whose determinants are equal.

If in an arbitrary group G we take G itself as the subgroup H, then the decomposition consists of a single coset, and if H is the unit subgroup E, then every element of the group constitutes a separate coset.

We could have obtained, instead of the left decomposition, the *right decomposition of a group G with respect to a subgroup H* by calling every subset Ha, $a \in G$ a *right coset of H in G*. Everything that has been proved above for left cosets carries over to right cosets. In particular, one of the right cosets is H itself. Two elements a and b lie in the same right coset with respect to H if and only if $ba^{-1} \in H$.

In the case of abelian groups it is, of course, unnecessary to distinguish between the left and right decompositions, but in the non-commutative case these decompositions may turn out to be distinct. For example, the right decomposition of the symmetric group of degree 3 with respect to the subgroup $H = \{(12)\}$ differs from the left decomposition given in Example 2 above, and consists of the following three cosets: H itself, the coset $H \cdot (13)$, containing the elements (13) and (123), and the coset $H \cdot (23)$, consisting of the elements (23) and (132). We can assert, however, that *the two decompositions of a group G with respect to an arbitrary subgroup H consist of the same number of cosets* (in the infinite case this means that *the sets of left and right cosets with respect to a given subgroup have the same cardinal number*). For, the set of inverses of the elements of the left coset aH is the right coset Ha^{-1}

$$(aH)^{-1} = Ha^{-1};$$

thus there is a one-to-one correspondence between the left and right cosets.

The number of cosets in either decomposition of a group G with respect to a subgroup H (in the infinite case, the cardinal number of the sets of these cosets) is called the *index* of H in G. If the number of cosets is finite, then H is called a *subgroup of finite index*.

All the subgroups of a group all have finite index if and only if the group itself is finite; for the index of the unit subgroup of an arbitrary group is the cardinal number of the group. All subgroups other than the unit subgroup of the infinite cyclic group are subgroups of finite index, and the group has for every natural number n one and only one subgroup of index n; the proof of this statement follows from the theorem on subgroups of cyclic groups proved in § 6.

On the other hand, there exist groups in which all the proper subgroups are of infinite index. An example is the additive group of rational numbers R. For if H is a proper subgroup of R, then we can find an element a not in H

which is such that pa is contained in H, where p is a prime number. The numbers

$$a, \quad \frac{1}{p}a, \quad \frac{1}{p^2}a, \ldots, \quad \frac{1}{p^n}a, \ldots$$

all lie outside H and belong to different cosets of H in R. For if

$$\frac{1}{p^n}a = \frac{1}{p^k}a + h, \quad h \in H, \quad n > k,$$

then

$$a = p^{n-k}a + p^n h;$$

that is, a is itself contained in H, contrary to our assumption.

THEOREM OF POINCARÉ. *The intersection of a finite number of subgroups of finite index has itself finite index.*

It is obviously sufficient to prove the theorem for the case of two subgroups. Let H and K be subgroups of finite index in a group G and let D be their intersection. Two elements a and b lie in the same left coset of D if and only if $a^{-1}b \in D$, so that $a^{-1}b \in H$ and $a^{-1}b \in K$. We therefore obtain all the left cosets of D in G if we take all non-empty intersections of the left cosets of H with the left cosets of K. Since the indices of H and K are finite, the number of these intersections, and hence the index of D in G, is finite. We see, moreover, that *the index of D in G is not greater than the product of the indices of H and K.*

In the case of finite groups the concept of the decomposition of a group with respect to a subgroup leads to the following important theorem:

THEOREM OF LAGRANGE. *The order and the index of a subgroup of a finite group are divisors of the order of the group.*

For if a finite group G is of order n and if H is a subgroup of order h and index j, then each left coset of G with respect to H consists of h elements, and therefore

$$n = hj.$$

Since the order of an element is equal to the order of its cyclic subgroup, it follows from the theorem of Lagrange that *the order of each element of a finite group is a divisor of the order of the group.*

It also follows from the theorem of Lagrange that *every group whose order is a prime number is cyclic.* For the group must be the cyclic subgroup generated by any of its elements other than 1.

The Theorem of Lagrange is a special case of the following theorem, which refers to arbitrary groups:

If H and K are subgroups of a group G, of finite index j and n respectively, and if K is contained in H, then the index h of K in H is also finite and

$$n = hj.$$

For if two elements lie in the same left coset of K in G, then *a fortiori* they lie in the same left coset of H. Every left coset of H in G therefore splits into several complete left cosets of K in G. From this it already follows that the index of K in H is finite. Now if K has h left cosets in H, then every coset aH, $a \in G$, also consists of h such cosets; we obtain them when all the left cosets of K occurring in H are multiplied on the left by a. This completes the proof of the theorem.

If G is a finite group and $K = E$, then we obtain the theorem of Lagrange.

In certain group-theoretical problems use is made of *the decomposition of a group with respect to a double module*, which is a generalization of the decomposition of a group into cosets. Let H and K be arbitrary subgroups of a group G. If a is an element of G, then the product HaK obviously contains a; we shall call this product the double coset modulo (H, K) generated by a. If b is contained in HaK, so that $b = hak$, then $a = h^{-1}bk^{-1}$, that is, $a \in HbK$. Finally, it follows from $b \in HaK$, $c \in HbK$ that $c \in HaK$. This shows that G is divided into disjoint double cosets modulo (H, K). When $K = E$, the decomposition of G thus obtained obviously becomes the right decomposition of G with respect to H, and when $H = E$, the left decomposition of G with respect to K.

Clearly, the double coset HaK contains, with each one of its elements, the entire right coset with respect to H generated by that element. We can now establish a one-to-one correspondence between the right cosets of H which are contained in HaK and the right cosets of the intersection $D = a^{-1}Ha \cap K$ in K as follows: With the coset Hak_0, $k_0 \in K$ we associate the coset Dk_0. For if $Hak_0 = Hak_1$, $k_1 \in K$, then $k_1 = a^{-1}ha \cdot k_0$, $h \in H$ and hence $a^{-1}ha \in D$, so that $k_1 \in Dk_0$. On the other hand, if $k' \in K$, then Dk' corresponds to the coset Hak' in HaK. Further, if $Dk' = Dk''$, then there exists an element $h \in H$ for which

$$k'' = a^{-1}ha \cdot k',$$

so that $ak'' = hak'$ and hence $Hak'' = Hak'$. Therefore *if the index of the subgroup $a^{-1}Ha \cap K$ in K is finite, then the number of right cosets of H*

that are contained in the double coset HaK is also finite, and conversely. Moreover these two numbers are equal.

§ 9. Normal subgroups

We know from the preceding section that non-commutative groups may possess subgroups for which the left and right decompositions differ. But in any group the two decompositions with respect to the unit subgroup (and those with respect to the group itself) coincide. Example 3 of the preceding section presents a less trivial case in which, as can easily be verified, the two decompositions coincide.

A subgroup H of a group G is called a *normal* (or *invariant* or *self-conjugate*) subgroup if the left and right decompositions of G with respect to H coincide. In other words, H is a normal subgroup of G if for each element a of H its left and right cosets in G coincide:

$$aH = Ha.$$

This shows that a subgroup H of a group G is normal if and only if it is permutable with every element of the group, that is, if for every a in G and every h in H we can find elements h' and h'' in H for which

$$ah = h'a, \qquad ha = ah''. \tag{1}$$

The concept of a normal subgroup can also be defined in many other ways; we shall each time use the definition most convenient in the context. We have just given two; others will be given later.

Two elements a and b of a group G are called *conjugate* in G if we can find an element g for which

$$b = g^{-1}ag.$$

We shall also say that b is obtained from a by *transformation* by g.

Since the second equation (1) can be written in the form

$$a^{-1}ha = h'',$$

and since a and h are arbitrary elements of G and H respectively, we obtain the following property of normal subgroups:

If a normal subgroup H of a group G contains an element h, it also contains all the elements that are conjugate to h in G.

This property could be taken as the definition of a normal subgroup; it is often convenient to use it in the following more general form:

Let G be a group with a system of generators M, and H a subgroup generated by a set of elements N. If the process of transforming the elements of N by the elements of M and their inverses does not lead outside of H, then H is a normal subgroup of G.

For it is easy to verify that

$$g^{-1}(h_1^{\alpha_1}h_2^{\alpha_2}\dots h_n^{\alpha_n})g=(g^{-1}h_1g)^{\alpha_1}(g^{-1}h_2g)^{\alpha_2}\dots(g^{-1}h_ng)^{\alpha_n},$$

$$(g_1g_2)^{-1}h(g_1g_2)=g_2^{-1}(g_1^{-1}hg_1)g_2.$$

However, every element of G has the form

$$g=g_1g_2\cdots g_k,$$

where $g_i\in M$ or $g_i^{-1}\in M$ $(i=1,2,\dots,k)$, and every element of H has the form

$$h=h_1^{\alpha_1}h_2^{\alpha_2}\dots h_n^{\alpha_n},$$

where $h_i\in N$ $(i=1,2,\dots,n)$. Therefore we always have $g^{-1}hg\in H$, and this is what we had to prove.

The reference to the inverses of the elements of M in this formulation of the theorem is, of course, superfluous when all the elements of M are of finite order.

Let U be any subgroup and g an arbitrary element of a group G. Then the subset $g^{-1}Ug$ (which consists, obviously, of all the elements obtained from the elements of U by transforming them with g) is itself a subgroup. For if u_1 and u_2 belong to U, then

$$(g^{-1}u_1g)(g^{-1}u_2g)=g^{-1}(u_1u_2)g \tag{2}$$

and

$$(g^{-1}u_1g)^{-1}=g^{-1}u_1^{-1}g.$$

The subgroup $g^{-1}Ug$ is said to be *conjugate* to U in G. We shall also say that it is obtained from U by *transformation* by g. Since

$$g^{-1}u_1g=g^{-1}u_2g$$

implies that $u_1=u_2$, we see from (2) that the mapping

$$u\to g^{-1}ug,\ u\in U$$

is an *isomorphic mapping* of U onto $g^{-1}Ug$.

From what we have proved above about the conjugates of the elements of a normal subgroup it follows that *all the subgroups of a group G that are conjugate to a normal subgroup H of G must be entirely contained in H.* In fact, we can assert a little more. If the subgroup $g^{-1}Hg$ is a proper subgroup of the normal subgroup H, that is, if H contains an element h_0 not contained in $g^{-1}Hg$, then gh_0g^{-1} is conjugate to h_0 but is not in H; and this is a contradiction. On the other hand, since every subgroup of G that coincides with its conjugate subgroups must obviously contain all the conjugates of each of its elements, we arrive at the following result:

The normal subgroups of a group G are precisely those subgroups which coincide with all their conjugates in G.

We now pass on to some simple consequences of the definition of a normal subgroup.

Every subgroup of index 2 is a normal subgroup, since both decompositions of the group with respect to this subgroup coincide. Thus, the alternating group of degree n is a normal subgroup of the symmetric group of degree n, in which it has index 2.

The intersection of any set of normal subgroups of a group G is itself a normal subgroup.

For if D is the intersection of the given normal subgroups, then every conjugate of an element of D must be contained in all these normal subgroups and hence in their intersection.

This property of normal subgroups allows us, just as in § 6 in the case of subgroups, to speak of the normal subgroup of a group G *generated* by a given subset M; it is the intersection of all the normal subgroups containing M.

The normal subgroup generated by any set of normal subgroups of a group G coincides with the subgroup generated by this set of subgroups.

For if normal subgroups H_α are given (α ranging over some index set) then every element of the subgroup $\{H_\alpha\}$ can be written in the form

$$h_1 h_2 \dots h_k,$$

where each h_i is contained in some H_{α_i}, $i = 1, 2, \dots, k$. If $g \in G$, then

$$g^{-1}(h_1 h_2 \dots h_k)\, g = (g^{-1}h_1 g)(g^{-1}h_2 g)\dots(g^{-1}h_k g);$$

but since

$$g^{-1}h_i g \in H_{\alpha_i}, \quad i = 1, 2, \dots, k,$$

we find that every conjugate of an element of $\{H_\alpha\}$ is contained in this group.

It follows that *the union of an ascending sequence of normal subgroups of a group G is itself a normal subgroup of G.* The proof is immediate.

A normal subgroup, being permutable with every element of the group, is *a fortiori* permutable with every subgroup. Hence it follows, by § 8, that *the subgroup $\{H, K\}$ generated by a normal subgroup H and an arbitrary subgroup K of a group G coincides with the product HK.* In other words, every element of $\{H, K\}$ can be written as a product hk, where $h \in H$, $k \in K$. $\{H, K\}$ then coincides also with KH.

If H is a normal subgroup of a group G and if it is contained in a subgroup F of G,

$$H \subset F \subset G,$$

then *H is a normal subgroup of F.* For, every element of the form $f^{-1}hf$, where $h \in H, f \in F$, belongs to H. We note, however, that if H is a normal subgroup of G, and K a normal subgroup of H, then while K is certainly a subgroup of G, it need not be normal in G; that is, *the property of being a normal subgroup is not transitive.* Later on we shall meet several relevant examples of this.

In an abelian group every subgroup is normal. But there also exist non-commutative groups in which every subgroup is normal. Such non-commutative groups are called *hamiltonian* (after W. R. Hamilton); a complete description of them can be found in a paper by Baer [2]. It has been proved, in particular, that every hamiltonian group contains a subgroup isomorphic to the following group Q which is known as the *quaternion group* and is itself hamiltonian. We denote by Q the subgroup of the symmetric group of degree 8 that is generated by the permutations

$$a = (1234)(5678), \quad b = (1537)(2846).$$

The following relations are easily verified:

$$a^4 = 1, \tag{3}$$
$$b^4 = 1, \tag{4}$$
$$a^2 = b^2, \tag{5}$$
$$aba = b. \tag{6}$$

Hence we have

$$bab = a^3(aba)b = a^3b^2 = a^5 = a, \tag{7}$$
$$a^3b = b^2ab = ba, \tag{8}$$
$$b^3a = a^2ba = ab.$$

Since $a^2 \cdot a = a \cdot a^2$ and $b^2 \cdot b = b \cdot b^2$, we can represent every product of powers of a and b as an alternating product of first powers of these elements, possibly multiplied on the left by a^3 or b^3; this can be done by the use of (5) and by means of re-arrangements (that is, without changing the number of factors). However, by using (6), (7), (8), or (9) we can decrease the number of factors in every such product until it coincides with one of the following eight:

$$1,\ a,\ b,\ ab = (1836)(2745),\quad ba = (1638)(2547),$$

$$a^2 = b^2 = (13)(24)(57)(68),\quad a^3 = (1432)(5876),\quad b^3 = (1735)(2648);$$

and these products are all distinct. Thus Q is a non-commutative group of order eight.

Every subgroup of Q, other than E and Q itself, must be of order 2 or 4. Actually, Q has a single subgroup of order 2, namely $\{a^2\}$, and three subgroups of order 4, namely $\{a\}$, $\{b\}$, and $\{ab\}$. Transforming the generators of all these cyclic subgroups by a and by b we can verify by using (3)-(7) that all these subgroups are normal in Q.[1]

Simple Groups. Every group has two normal subgroups, the group itself and the unit subgroup. A group that has no other normal subgroups is called *simple*. Simple groups are in a certain sense the very opposite to hamiltonian groups.

An abelian group is simple if and only if it is cyclic and every element other than 1 is a generator. The remark in § 6 on generators of cyclic groups allow us, therefore, to state that *an abelian group is simple if and only if it is cyclic and its order is a prime number.*

There also exist non-commutative simple groups, finite as well as infinite. We have, for example, the following theorem, which plays an important rôle in Galois theory:

The alternating group A_n of degree n for $n \geqq 5$ is simple.

First of all, we prove two lemmas.

LEMMA 1. *If $n \geqq 3$, then A_n is generated by the cycles of length* 3.

---

[1] The reader who is familiar with quaternions can verify that the mapping

$$a \to i,\ b \to j$$

establishes an isomorphism between the group Q and the multiplicative group of the eight quaternions ± 1, $\pm i$, $\pm j$, $\pm k$. [*Trans.*]

For, every even permutation is the product of an even number of transpositions; but the product of two distinct transpositions is equal either to a cycle of length 3 or to the product of two such cycles: if $\alpha, \beta, \gamma, \ldots$ are the permuted symbols, then

$$(\alpha\beta)(\alpha\gamma) = (\alpha\beta\gamma),$$
$$(\alpha\beta)(\gamma\delta) = (\alpha\beta\gamma)(\alpha\delta\gamma).$$

Every cycle of length 3 is obviously an even permutation.

LEMMA 2. *If a normal subgroup of A_n, $n \geqq 5$, contains a cycle of length 3, then it is the whole group A_n.*

Suppose H is a normal subgroup of A_n and contains the cycle $(\alpha\beta\gamma)$; and let $(\bar{\alpha}\bar{\beta}\bar{\gamma})$ be any other cycle of length 3 in A_n. If the symbols δ and ε are different from α, β, and γ, then the permutation of degree n

$$a = \begin{pmatrix} \ldots\alpha\ldots\beta\ldots\gamma\ldots\delta\ \ldots\varepsilon\ldots \\ \ldots\bar{\alpha}\ldots\bar{\beta}\ldots\bar{\gamma}\ldots\delta'\ldots\varepsilon'\ldots \end{pmatrix}$$

(which we can make even by transposing, if necessary, the symbols δ' and ε' in the second row) is such that

$$a^{-1}(\alpha\beta\gamma)a = (\bar{\alpha}\bar{\beta}\bar{\gamma}).$$

The normal subgroup H therefore contains all the cycles of length 3 in A_n and, by Lemma 1, coincides with A_n.[1]

We now proceed to the

Proof of the Theorem: Suppose A_n has a normal subgroup H, different from E, and suppose that among the elements of H there are some whose decomposition into cycles contains one cycle of length at least 4. Let h be one of these elements,

$$h = (\alpha\beta\gamma\delta\ldots)\ldots,$$

where the dots outside the parenthesis represent all the remaining cycles. Then H also contains the following element, which is conjugate to h in A_n:

$$h' = (\alpha\gamma\beta)\,h\,(\alpha\beta\gamma) = (\beta\gamma\alpha\delta\ldots)\ldots,$$

[1] Clearly, Lemma 2 holds for $n < 5$ as well.

and hence H contains the element

$$h^{-1}h' = (\alpha\beta\delta).$$

Therefore, by Lemma 2, $H = A_n$.

Now suppose that in the decomposition of an element h of H there occur only cycles of length 3 and, possibly, 2. We can assume that there are at least two cycles of length 3, since otherwise h^2 would be simply one cycle of length 3 and we could apply Lemma 2 immediately. If

$$h = (\alpha\beta\gamma)(\alpha'\beta'\gamma')\ldots,$$

then H also contains the element

$$h' = (\beta'\alpha'\gamma)\,h\,(\gamma\alpha'\beta') = (\alpha\beta\alpha')(\gamma\gamma'\beta')\ldots,$$

and therefore also the element

$$hh' = (\alpha\alpha'\gamma\beta\gamma')\ldots,$$

which contains a cycle of length 5, and we again have the previous case.

Suppose, finally, that the decomposition of an element h of H consists only of cycles of length 2; obviously there is then an even number of them. If $h = (\alpha_1\beta_1)(\alpha_2\beta_2)$, then H also contains the element

$$h' = (\gamma\beta_1\alpha_1)\,h\,(\alpha_1\beta_1\gamma) = (\beta_1\gamma)(\alpha_2\beta_2),$$

where γ is an arbitrary symbol, different from the symbols that are actually affected by h. H must also contain the element

$$hh' = (\alpha_1\gamma\beta_1),$$

and hence $H = A_n$. If

$$h = (\alpha_1\beta_1)(\alpha_2\beta_2)(\alpha_3\beta_3)(\alpha_4\beta_4)\ldots,$$

then H also contains the element

$$h' = (\beta_1\alpha_2)(\beta_2\alpha_3)\,h\,(\beta_2\alpha_3)(\beta_1\alpha_2) = (\alpha_1\alpha_2)(\beta_1\alpha_3)(\beta_2\beta_3)(\alpha_4\beta_4)\ldots,$$

and hence the element

$$hh' = (\alpha_1\alpha_3\beta_2)(\alpha_2\beta_3\beta_1);$$

this brings us back to the case considered above. This completes the proof of the theorem.[1]

[1] Some proofs of this theorem, essentially rather similar to the one given in the text, begin by choosing an element of H, other than the unit element, that leaves the largest possible number of symbols in place. The simplest proof of this kind can be found in a paper by Bauer [1].

The assumption $n \geqq 5$ is essential. True, the alternating group of degree 3 is a cyclic group of order 3 and is therefore simple; but *the alternating group of degree* 4 *is not simple*: it is easy to verify that the permutations (12)(34), (13)(24), and (14)(23) which are contained in it form, together with 1, a normal subgroup V of A_4. This group V of order 4, which is also called Klein's *four-group*, is abelian but not cyclic.

The above theorem shows that there exist infinitely many simple non-commutative finite groups. But the alternating groups are by no means the only ones. In § 61 we shall give some results bearing on the problem of a complete classification of all finite simple groups; this problem is still far from a complete solution.

In the proof of the theorem we have nowhere made use of the finiteness of the group A_n. We see, therefore, that *the countable alternating group and, more generally, the alternating groups of any infinite cardinal number* (see § 4, Example 4) *are simple*. This shows that there exist simple groups of any infinite cardinal number.

§ 10. The connection between normal subgroups, homomorphisms, and factor groups

It follows from the definition of a normal subgroup that the left cosets of a normal subgroup H in a group G are also right cosets and conversely. We can therefore speak simply of the cosets of H in G and of the *decomposition of* G *into cosets* with respect to a normal subgroup.

The decomposition of a group G *into cosets of a normal subgroup* H *is a regular partition* (see § 2) *of* G.

For let two cosets of a normal subgroup H in G be given. If *arbitrary* representatives a and b are chosen in these cosets, that is, if the cosets can be written in the form aH and bH, then the associative law for multiplication of subsets and the basic equations $Hb = bH$ and $HH = H$ yield

$$aH \cdot bH = abHH = abH.$$

The converse is also true.

If a regular partition of a group G *is given, then the class that contains the unit element is a normal subgroup of* G, *and all the other classes are cosets of this normal subgroup in* G.

Let A be the class of the given regular partition that contains the element 1. If a_1 and a_2 are two elements of A, then the product $a_1 a_2$ must lie in the same class as $1 \cdot 1 = 1$ (by the definition of a regular partition), and therefore

$$a_1 a_2 \in A.$$

Furthermore, if a is an element of A, then the product $a a^{-1} = 1$ must lie in the same class as $1 \cdot a^{-1} = a^{-1}$; hence

$$a^{-1} \in A.$$

We have thus shown that A is a subgroup. If a is now an element of A and b an element of G, then the product $b^{-1} a b$ must lie in the same class as $b^{-1} \cdot 1 \cdot b = 1$, so that

$$b^{-1} a b \in A.$$

The class A is therefore a normal subgroup of G.

Finally, let B be an arbitrary class of the given regular partition. If b is an element of B, then for any element a of A the product ba must lie in the same class as $b \cdot 1 = b$; that is, the whole coset bA is contained in B. If c is any other element of B, then since b and c lie in the same class of the regular partition, this must also be true for the products $b^{-1} c$ and $b^{-1} b = 1$, so that

$$b^{-1} c \in A;$$

and hence

$$c \in bA,$$

so that

$$B = bA.$$

This completes the proof.

These results establish a *one-to-one correspondence between the regular partitions of a group G and the normal subgroups of G*. Thus we may abandon the distinction between regular partitions of a group and its decompositions into cosets with respect to a normal subgroup. In particular, if A is that class of a given regular partition of G which contains the unit element, then we shall no longer speak of the factor groups of G with respect to this regular partition, but of the *factor group of the normal subgroup A*. We shall denote it by the symbol G/A.

We leave it to the reader to re-formulate the *homomorphism theorem* for groups (§ 3) correspondingly. This theorem now establishes a close link between the normal subgroups of a group and its homomorphic mappings.

Indeed this link with the homomorphisms of a group makes the concept of a normal subgroup one of the most fundamental in the theory of groups. In particular, we have a new definition of a normal subgroup. Let us define the *kernel* of a homomorphic mapping φ of a group G onto a group G' as the totality of all elements of G that are mapped by φ onto the unit element of G'. From the homomorphism theorem and the results of the present section we obtain the following result:

The normal subgroups of a group G, and they only, are the kernels of the homomorphisms of G.

If a group G is mapped homomorphically onto a group G', and if U is a subgroup of G, then it also undergoes a homomorphic mapping, and therefore its image under this mapping is a subgroup of G'. Conversely, if U' is any subgroup of G', then its *complete inverse image U in G*, that is, the set of all the elements of G that are mapped under φ into the subgroup U', *is a subgroup of G*. For if a and b are elements of U, and

$$a\varphi = a' \in U', \quad b\varphi = b' \in U',$$

then

$$(ab)\varphi = a'b';$$

and since $a'b' \in U'$, ab must lie in U. Further,

$$(a^{-1})\varphi = a'^{-1},$$

but $a'^{-1} \in U'$, and hence $a^{-1} \in U$. Our statement is proved. We also note that, because U' contains the unit element of G', *its complete inverse image contains the whole kernel of the homomorphism φ*. This correspondence between the subgroups of G and G' has a number of important additional properties which are incorporated in the following *theorem on the correspondence between subgroups under homomorphic mappings*; by virtue of the homomorphism theorem we can use the terms factor group and natural homomorphism of a group onto its factor group in the statement of the theorem.

Theorem: *The relation that assigns to every subgroup of the factor group $\overline{G} = G/H$ its complete inverse image in G under the natural homomorphism of G onto $\overline{G}$ is a one-to-one correspondence between all the subgroups of $\overline{G}$ and those subgroups of G that contain the normal subgroup H. Corresponding subgroups have equal indices in their respective groups. Finally, if one of the subgroups is normal, then the other one is also normal, and the factor groups of G and $\overline{G}$ with respect to these normal subgroups are isomorphic.*

Proof. If $\overline{U}_1$ and $\overline{U}_2$ are distinct subgroups of $\overline{G}$, then we can find in one of them, say in $\overline{U}_1$, an element $\overline{a}$ that does not lie in the other. Under the natural homomorphism some elements of G are mapped onto $\overline{a}$, and hence the complete inverse images of these two subgroups in G cannot coincide. On the other hand, let U be an arbitrary subgroup of G containing H, $\overline{U}$ its image in $\overline{G}$, and U_0 the complete inverse image of $\overline{U}$ in G. It is clear that $U \subseteq U_0$. However, if a_0 is an element of U_0, then U contains an element a which is such that a_0 and a lie in the same coset with respect to H, and since $H \subset U$ we have $a_0 \in U$, so that $U_0 = U$. Thus we have proved that the correspondence is one to one.

If U (containing H) and $\overline{U}$ are now arbitrary corresponding subgroups of G, and $\overline{G} = G/H$, then for a and b in G the element $a^{-1}b$ lies in U if and only if the coset

$$a^{-1}bH = a^{-1}H \cdot bH$$

belongs to $\overline{U}$. This shows that the left cosets of U in G stand in one-to-one correspondence with the left cosets of $\overline{U}$ in $\overline{G}$, so that the subgroups U and $\overline{U}$ have equal indices in G and $\overline{G}$, respectively.

If $\overline{U}$ is now a normal subgroup of $\overline{G}$, then the natural homomorphisms of G onto $\overline{G}$ and of $\overline{G}$ onto $\overline{G}/\overline{U}$ carried out in succession give a homomorphic mapping of G onto the latter factor group. The kernel of this homomorphism consists of those elements of G that are mapped into $\overline{U}$ under the mapping of G onto $\overline{G}$, that is, the elements of U. Hence it follows that U is a normal subgroup of G and that

$$G/U \simeq \overline{G}/\overline{U}.$$

If, conversely, U is a normal subgroup of G containing H, and $\overline{U}$ the corresponding subgroup of $\overline{G}$, then for any $\overline{u} \in \overline{U}$ and $\overline{g} \in \overline{G}$ the element (that is, the coset of H) $\overline{g}^{-1}\overline{u}\,\overline{g}$ consists of elements of G belonging to U and is therefore contained in $\overline{U}$. It follows that $\overline{U}$ is a normal subgroup of $\overline{G}$. This completes the proof of the theorem.

In § 4 we gave a number of examples of homomorphic mappings of groups. The reader will easily find the kernels of these homomorphisms and construct the corresponding factor groups. We shall now investigate the factor groups of the finite and infinite cyclic groups.

Let φ be a homomorphic mapping of a cyclic group $A = \{a\}$ onto a group B. If

$$a\varphi = b,$$

then obviously all the elements of B are powers of b, so that $B = \{b\}$. In other words, *all the factor groups of cyclic groups are themselves cyclic groups.*

In particular, let A be an infinite cyclic group represented as the additive group of integers. We obtain a homomorphic mapping of A onto a cyclic group B of order n with generator b if we assign to the integer k the element b^k as its image. The numbers k and l are mapped onto the same element of the cyclic group B if and only if $k - l$ is divisible by n, that is, if in the usual terminology k and l are *congruent modulo* n (in symbols: $k \equiv l \pmod{n}$). In the additive group of integers there corresponds to this homomorphic mapping the decomposition into classes with respect to the subgroup consisting of the multiples of n; these are the *residue classes modulo* n.[1] Making use of the result of § 6 on subgroups of cyclic groups and letting n run through all the natural numbers we find that *all the cyclic groups and no other groups occur as factor groups of the infinite cyclic group* (that is, the additive group of integers), and factor groups with respect to distinct subgroups of this group are not isomorphic.[2]

If $A = \{a\}$ is now a finite cyclic group of order s and if t is a divisor of s,

$$s = tq,$$

then the subgroup $\{a^t\}$ has order q, and therefore its factor group is cyclic of order t. Conversely, since *the order of a factor group of a finite group is equal to the index of the corresponding normal subgroup and therefore divides the order of the group,* we find that *the factor groups of a finite cyclic group of order s are the cyclic groups whose order divides s, and no others.*

Let us now investigate *the factor groups of a group P of type* p^∞. We have seen in § 7 that the proper subgroups of P form an ascending sequence

$$E \subset \{a_1\} \subset \{a_2\} \subset \ldots \subset \{a_n\} \subset \ldots,$$

where these subgroups are of orders $1, p, p^2, \ldots, p^n, \ldots$ respectively. We consider the factor group of $\{a_n\}$ in P. It is the union of the ascending sequence of factor groups $\{a_k\}/\{a_n\}$, $k = n+1, n+2, \ldots$, which, from the above, are cyclic groups of order p^{k-n}. The factor group $P/\{a_n\}$ is therefore itself a group of type p^∞. We see that *a group of type* p^∞ *is isomorphic to all the factor groups of its proper subgroups.*

---

[1] See § 8, Example 1, for the special case $n = 4$.

[2] We speak of subgroups rather than normal subgroups because the group is abelian.

Let two groups A and B be given. A group G is called an *extension* of A by B if G contains a normal subgroup A', isomorphic to A, whose factor group is isomorphic to B,

$$A' \simeq A, \quad G/A' \simeq B.$$

Note that the extension G is not uniquely determined by giving the groups A and B, as the following examples show.

Examples. 1. In the cyclic group $\{a\}$ of order 4, the subgroup $\{a^2\}$ is cyclic of order 2, and its factor group is also cyclic of order 2. If we now take the non-cyclic abelian group V of order 4 that is contained in the alternating group A_4 (as we have seen in the preceding section), then every one of its cyclic subgroups is of order 2. We have, therefore, two non-isomorphic extensions of a cyclic group of order 2 by another such group.

2. The cyclic group of order 6 has a unique cyclic subgroup of order 3, and its factor group is cyclic of order 2; but S_3, the symmetric group of degree 3, has the normal subgroup A_3 which is also a cyclic group of order 3, and the factor group S_3/A_3 is also cyclic of order 2.

Extensions of groups will be studied in detail in Chap. XII.

The following theorem plays an important rôle in the sequel:

THE ISOMORPHISM THEOREM. *If A and B are subgroups of a group G, and A is a normal subgroup of* $\{A, B\}$, *then the intersection* $A \cap B$ *is a normal subgroup of B and*

$$\{A, B\}/A \simeq B/(A \cap B).$$

For $\{A, B\} = AB$, because A is normal in $\{A, B\}$. Every coset of A in AB therefore contains elements of B, that is, has a non-empty intersection with B. Hence it follows that in the natural homomorphic mapping of $\{A, B\}$ onto the factor group $\{A, B\}/A$ the subgroup B is mapped onto this whole factor group. Therefore, by the homomorphism theorem the factor group $\{A, B\}/A$ is isomorphic to the factor group of B with respect to the normal subgroup consisting of all the elements of B that are mapped onto the unit element. However, these are precisely the elements of $A \cap B$. This concludes the proof.

The isomorphism theorem contains the following result, which could easily be proved independently:

The intersection of a normal subgroup A and a subgroup B is normal in B.

We shall use this for the proof of the following theorem:

The union of an ascending sequence of simple groups is itself a simple group.

For if a group G is the union of an ascending sequence

$$U_1 \subset U_2 \subset \ldots \subset U_n \subset \ldots$$

of proper subgroups which are simple and if H is a proper normal subgroup of G, different from E, then there exists an index k for which the intersection $H \cap U_k$ differs from E as well as from U_k itself. By the above remark this intersection is, however, a normal subgroup of U_k; this contradicts the assumption that U_k is simple.[f]

The isomorphism theorem is a special case of the following theorem which is known as

Zassenhaus' Lemma [1]: *If A, A', B, and B' are subgroups of a group G, and if A' is normal in A, B' normal in B, then $A'(A \cap B')$ is normal in $A'(A \cap B)$, and $B'(B \cap A')$ is normal in $B'(B \cap A)$, and the corresponding factor groups are isomorphic.*

$$A'(A \cap B)/A'(A \cap B') \simeq B'(B \cap A)/B'(B \cap A').$$

Proof. If we write

$$C = A \cap B,$$

and

$$D = (A \cap B')(B \cap A').$$

then clearly $D \subseteq C$. Moreover, since B' is normal in B and since C is a subgroup of B, we see that

$$C \cap B' = A \cap B \cap B' = A \cap B'$$

is a normal subgroup of C. By the symmetry of the assumptions on A and B, this also holds for the intersection $B \cap A'$ and therefore also for D, since the product of normal subgroups is itself a normal subgroup. We can therefore speak of the factor group of D in C; we denote it by H,

$$H = C/D.$$

On the other hand, A' is a normal subgroup of A, so that the product $A'(A \cap B) = A'C$ is a subgroup. Every element of this product has the form $a'c$, where $a' \in A$, $c \in C$. Let us associate it with the coset Dc (that is, with an element of H). If $a'c$ has another representation in the same form

$$a'c = a_1'c_1,$$

then

$$a_1'^{-1}a' = c_1c^{-1} \in (A' \cap C) \subseteq (A' \cap B) \subseteq D,$$

and hence

$$c_1 = (a_1'^{-1}a')\, c \in D\, c.$$

We obtain a single-valued mapping of the group $A'C$ into the group H, and in fact onto the whole group H, since every element $c \in C$ is mapped onto its coset Dc. This mapping is homomorphic: since A' is normal in $A'C$, we have

$$a_1'c_1 \cdot a_2'c_2 = a_3'(c_1c_2), \quad \text{where} \quad a_3' \in A'.$$

The kernel of this homomorphism clearly must contain the subgroup $A'(A \cap B')$; we know that $A \cap B' \subseteq D$. On the other hand, if an element $a'c$ is mapped by this homomorphism into D, then $c \in D$, i.e.

$$c = uv, \qquad \text{where} \quad u \in (B \cap A'), \quad v \in (A \cap B'),$$

and then

$$a'c = (a'u)v = a_1'v \in A'(A \cap B').$$

The kernel of the homomorphism in question is therefore the subgroup $A'(A \cap B')$. By the homomorphism theorem this leads to the isomorphism

$$A'(A \cap B)/A'(A \cap B') \simeq H.$$

By symmetry we also have the isomorphism

$$B'(B \cap A)/B'(B \cap A') \simeq H.$$

Every statement in the theorem is now proved.

The isomorphism theorem arises from Zassenhaus'Lemma when $A \supseteq B$, $B' = E$.

If A and B are subgroups of G, but neither is assumed to be normal in $\{A, B\}$, then the isomorphism theorem can be replaced by a statement regarding the indices of A in $\{A, B\}$ and of $A \cap B$ in B. In the general case we can only assert that *the first of these indices is not less than the second.* For by repeating the arguments that led to the proof of the isomorphism theorem we see that every right coset of $A \cap B$ in B is the intersection with B of a right coset of A in $\{A, B\}$, but it can happen that some right cosets of A in $\{A, B\}$ have an empty intersection with B. This is illustrated by the example of the symmetric group of degree 3, if A and B

are chosen as two of the cyclic subgroups of order 2. Bearing in mind the result of § 8 to the effect that $\{A, B\} = AB$ if and only if A and B are permutable, we can now prove at once that every coset of $\{A, B\}$ with respect to A has a non-empty intersection with B if and only if A and B are permutable. In other words, assuming that the indices are *finite*, we obtain the theorem:

The indices of A in $\{A, B\}$ and of $A \cap B$ in B are equal if and only if A and B are permutable.

§ 11. Classes of conjugate elements, and conjugate subgroups

If M is a subset of a group G, then the set of all elements of G that are permutable with M constitutes a subgroup which is called *the normalizer* of M in G. For if $aM = Ma$ and $bM = Mb$, then

$$(ab)M = aMb = M(ab);$$

multiplying both sides of the equation $aM = Ma$ on the left and on the right by a^{-1} we obtain further

$$Ma^{-1} = a^{-1}M.$$

This general definition allows us, in particular, to speak of the normalizer of a subgroup or of a single element. From the fact that an element is permutable with itself and a subgroup permutable with each of its elements it follows that *the normalizer of the element a (of the subgroup A) contains the element a (the subgroup A)*. The normalizer of a subgroup A is obviously the maximal subgroup of G in which A is normal. It follows that *the normalizer of a subgroup A is the whole group G if and only if A is normal in G*. By contrast, it can happen that a subgroup coincides with its own normalizer; this is true, for example, for the cyclic subgroup generated by the element (12) in the symmetric group of degree 3.

The normalizer of an element a of G is obviously contained in the normalizer of the cyclic subgroup $\{a\}$, but need not coincide with it. An example is the element (123) in the symmetric group of degree 3. In either case, the normalizer of a contains the subgroup $\{a\}$ as a normal subgroup.

The concept of a normalizer will help to establish some very important properties of conjugate elements and conjugate subgroups which form the substance of the present section.

If an element b of a group G is conjugate to an element a, that is $b = g^{-1}ag$, then $a = gbg^{-1}$; that is, a is obtained from b by transforming by g^{-1}. Each element a is conjugate to itself, since $a = 1^{-1}a1$. Finally, if $b = g_1^{-1}ag_1$, $c = g_2^{-1}bg_2$, then

$$c = (g_1g_2)^{-1}a(g_1g_2);$$

that is, the property of conjugacy of elements is transitive. It follows that the whole group G is partitioned into disjoint sets, the so-called *classes of conjugate elements*. All the elements in one class of conjugates obviously have the same order.

One of the definitions of a normal subgroup given in § 9 can now be expressed in the following form: A subgroup of a group G is normal if it contains the whole class of conjugates of each of its elements, that is, consists of complete classes of conjugate elements of G. We mention that every subset of a group that consists of complete classes of conjugate elements is called a *normal* (or *invariant*) *subset* of the group.

We shall now list a few basic properties of classes of conjugate elements.

The number of conjugates of an element a in a group G is equal to the index of the normalizer N of the element a in G.

For if $b = g^{-1}ag$, then for each n of N we have $(ng)^{-1}a(ng) = b$. Conversely, if $g_1^{-1}ag_1 = b$, then $(gg_1^{-1})^{-1}a(gg_1^{-1}) = a$, that is, $gg_1^{-1} \subset N$, and therefore the elements g and g_1 lie in the same right coset of N. There exists, then, a one-to-one correspondence between the right cosets of N in G and the conjugates of a.

It follows, in particular, that *the class of conjugates of an element a in G is finite if and only if the normalizer of a is of finite index in G.* Since the index of a subgroup of a finite group divides the order of the group (Theorem of Lagrange, see § 8) it also follows from the above theorem that *the number of elements in a class of conjugates of a finite group divides the order of the group.*

The following statement is a special case of the theorem proved at the beginning of § 9.

The subgroup generated by some classes of conjugate elements of a group G or, more generally, by some normal subset is a normal subgroup of G.

Hence it follows easily that the normal subgroup generated in a group G by a subset M is the subgroup generated in G by the subset $\overline{M}$ that consists of all the elements conjugate to elements of M.

The product K_1K_2 of two classes of conjugate elements K_1 and K_2 in a group G consists of a number of classes of conjugate elements, that is, is a normal subset. For if $a_1 \in K_1$, $a_2 \in K_2$, then

$$g^{-1}(a_1a_2)g = (g^{-1}a_1g)(g^{-1}a_2g);$$

that is, every conjugate to an element of the product K_1K_2 is also contained in this product.

We remark, finally, that *if K is a class of conjugate elements of a group G, then K^{-1}* (i.e. the totality of the inverses of elements of K) *is also a class of conjugate elements* and that, more generally, *the set of s-th powers, for any s, of all elements of K is a class of conjugate elements in G.* For if $a_2 = g^{-1}a_1g$, then $a_2^s = g^{-1}a_1^sg$, and from $b = g_1^{-1}a_1^sg_1$ it follows that $b = (g_1^{-1}a_1g_1)^s$, that is, b is the s-th power of an element conjugate to a_1.

In every group G the element 1 by itself forms a class of conjugate elements. A group may also have other elements that singly form classes of conjugates; these obviously will be the elements that are permutable with all the elements of the group, the so-called *central* elements (or *invariant* elements) of the group. A central element can also be defined as an element whose normalizer coincides with the whole group.

The set Z of all central elements of a group G is easily seen to be a subgroup of G. This subgroup, which is called the *center* of G, is normal in G, since every one of its elements forms a separate class of conjugates in G. Every subgroup of the center is also normal in G. A group coincides with its center if and only if it is abelian. On the other hand, there are groups whose center consists of 1 only. Such groups are called *groups without center*, a name that, while not quite accurate, is very convenient. Examples are: the symmetric groups S_n for $n \geqq 3$ and, of course, all the non-commutative simple groups.

A well-known theorem in higher algebra states that the center of the group of non-singular matrices of order n with elements in a field consists of all the *scalar* matrices of order n, that is, of matrices whose elements outside the main diagonal are zero while those in the main diagonal are all equal.

The factor group of a group G with respect to its center need not be a group without center. Thus, the center of the quaternion group (see § 9) is the cyclic group of order 2, and its factor group is abelian. We mention, however, that *the factor group of a non-commutative group with respect to its center cannot be cyclic.* For if the factor group G/Z were cyclic, then we take an element a_0 from a coset of Z which generates that

cyclic group. The subgroup generated by this element together with the elements of Z is the whole group G. But since all the elements mentioned are permutable, the group G is commutative.

Just as we have partitioned a group into classes of conjugate elements, so we can divide the set of all subgroups of a group G into disjoint *classes of conjugate subgroups.*

If K is a class of conjugate elements of a group G, then the set of normalizers of the elements of K is a class of conjugate subgroups.[1]

For if a and b are elements of K, and N_a and N_b are their normalizers in G, then from $b = g^{-1}ag$ and $x \in N_a$, that is, $xa = ax$, it follows that

$$b(g^{-1}xg) = g^{-1}(ax)\,g = (g^{-1}xg)\,b,$$

that is,

$$g^{-1}N_a g \subset N_b. \tag{1}$$

But from $a = gbg^{-1}$ we obtain in the same way

$$gN_b g^{-1} \subset N_a,$$

i.e.

$$N_b \subset g^{-1}N_a g. \tag{2}$$

From (1) and (2) it follows that

$$N_b = g^{-1}N_a g.$$

Now if any subgroup F is conjugate to N_a,

$$F = {g_1}^{-1}N_a g_1,$$

then F is the normalizer of the element $g_1^{-1}ag_1$. This proves the theorem.

We proceed to establish some basic properties of classes of conjugate subgroups.

The number of distinct subgroups that are conjugate to a subgroup A of a group G (that is, the cardinal number of the set of these subgroups) is equal to the index of the normalizer N of A in G. For just as in the case of conjugate elements, the transformation of A by two distinct elements of G leads to the same conjugate subgroup of A if and only if these elements lie in the same right coset of N.

It follows, in particular, that the normalizers of all the subgroups con-

[1] The normalizers of two distinct elements of K may, of course, turn out to be equal.

jugate to A have the same index in G. Moreover, since for $B = g^{-1}Ag$ the normalizer of B is the subgroup $g^{-1}Ng$, and since the mapping $x \to g^{-1}xg$, $x \in N$, is an isomorphism of N onto $g^{-1}Ng$ in which A is mapped onto B, the indices of A in N and of B in $g^{-1}Ng$ are equal. These two remarks allow us to state that the indices of A and B in G are equal; that is, *conjugate subgroups have equal indices* in the whole group. If these indices are finite, then no subgroup can contain properly another conjugate to it. This may very well occur, however, in the general case: If $g^{-1}Ag$ is distinct from A and contained in A, then $g^{-2}Ag^2$ is a proper subgroup of $g^{-1}Ag$, $g^{-3}Ag^3$ a proper subgroup of $g^{-2}Ag^2$, and so on. On the other hand, A is in that case a proper subgroup of gAg^{-1}, the latter a proper subgroup of g^2Ag^{-2}, and so on.

Consider, for example, the group G of all one-to-one mappings of the set of all (positive and negative) integers onto itself.

In this group we take the set M consisting of the transpositions

$$(12),\ (23),\ \ldots,\ (n,\ n+1),\ \ldots,\ n > 0,$$

and we denote by A the subgroup generated by these transpositions. If g is now the mapping that carries every integer k into $k+1$, that is, in cycle notation,

$$g = (\ldots,\ -k,\ \ldots,\ -2,\ -1,\ 0,\ 1,\ 2,\ \ldots,\ k,\ \ldots),$$

then

$$g^{-1}(n,\ n+1)g = (n+1,\ n+2),$$

so that the subgroup A is conjugate in G to a proper subgroup generated by all the elements of the set M except (12).

The intersection of all the subgroups in a complete class of conjugate subgroups in a group G is a normal subgroup.

For by transforming all the subgroups of the given conjugate class by an element g we also transform this intersection D. However, the transformation of a class of conjugate subgroups only permutes these subgroups among themselves, that is, for every g of G the subgroup $g^{-1}Dg$ coincides with D, which proves the theorem. Note that the intersection D may, of course, turn out to be the unit subgroup E.

The theorem just proved leads to the following important result:

If a group G has a subgroup of finite index, then it also has a normal subgroup of finite index.

Proof. If the subgroup H has finite index in G, then as we have shown

above, all the subgroups conjugate to H also have finite index. Now if the index of H is finite, it follows that the index of its normalizer, and therefore the number of conjugates of that subgroup, is also finite. The intersection of all these subgroups is, as we have just shown, a normal subgroup of G, and moreover has finite index in G, by the theorem of Poincaré (see § 8).

We end the present section by introducing a concept very similar to that of the normalizer. If M is a subset of a group G, then the set of all elements that are permutable with *every element* of M is a subgroup of G which is called the *centralizer of M in G*. The centralizer of a single element coincides with its normalizer, and—more generally—the centralizer of a subset M is contained in the normalizer of M. The centralizer of a subgroup need not, of course, contain that subgroup. The centralizer of the set of all elements of a group is the center of the group.

The centralizer of a subset M obviously coincides with the intersection of the normalizers of all the elements of M. Hence it follows easily that *the centralizer of a normal subgroup and, more generally, of a normal subset of a group is a normal subgroup*. For the normalizers of all the elements of a normal subgroup constitute some complete classes of conjugate subgroups,[1] and therefore the intersection of these normalizers must itself be a normal subgroup. Applying this fact to an arbitrary subgroup and its normalizer we see that *the centralizer of every subgroup is a normal subgroup of its normalizer*.

[1] See the theorem on the connection between classes of conjugate elements and conjugate subgroups that has been proved in this section.

CHAPTER IV

ENDOMORPHISMS AND AUTOMORPHISMS GROUPS WITH OPERATORS

§ 12. Endomorphisms and automorphisms

A homomorphic mapping of a group G into itself, that is, onto one of its subgroups, is called an *endomorphism* of G. Among the endomorphisms of a group are its *automorphisms*, that is, the isomorphic mappings onto itself. A trivial example of an automorphism is the identity mapping of a group onto itself, the so-called *identity automorphism*, in which every element of the group remains in place. The mapping of the additive group of the integers onto itself which carries the number n into $-n$ is an example of a non-identity automorphism.

Every group has a *null endomorphism* which maps each element onto the unit element. Among the endomorphisms of a group there may be some that map the group onto itself, although they are not automorphisms. This will always occur in groups that are isomorphic to one of their proper factor groups—the existence of such groups was shown in § 11. Of course, they have to be infinite. Every isomorphism between a group and one of its proper subgroups is also an endomorphism of the group; examples of such endomorphisms which are not automorphisms can be found in the additive group of integers.

If H is a subgroup of a group G, then an endomorphism of G induces a homomorphic mapping in H; if the endomorphism is an automorphism, then the induced mapping is isomorphic. It follows that the image of H under an endomorphism (and in particular, under an automorphism) χ is also a subgroup of G, which we shall denote by $H\chi$. The image of G itself under the endomorphism χ is therefore the subgroup $G\chi$.

If a group G is given by a system of generators $M = \{a_\alpha\}$, then every endomorphism χ of G is completely determined by the images $a_\alpha\chi$ of all the generators. If, in particular, χ is an automorphism of G, then the set of images of all the elements of M under the automorphism χ is also a set of generators for G.

If an element a is chosen in a group G, then the mapping that carries every element x of G into the element $a^{-1}xa$, that is, the transformation

of the whole group by a, is an automorphism of G. For $a^{-1}xa = a^{-1}ya$ implies $x = y$, i.e. the mapping is one to one. The equation

$$x = a^{-1}(axa^{-1})a$$

shows that every element of G appears in this mapping as the image of some element. Finally, from

$$a^{-1}xa \cdot a^{-1}ya = a^{-1}(xy)a$$

it follows that this mapping is isomorphic. Such an automorphism of G is called an *inner* automorphism. All other automorphisms of G are called *outer* automorphisms. The identity automorphism belongs to the inner automorphisms—one can consider it as obtained by the transformation of the group by the unit element. In the case of an abelian group, this is the only inner automorphism. In the general case, the inner automorphism induced by the element a coincides with the identity automorphism if and only if a belongs to the center of the group, since the equation

$$a^{-1}xa = x$$

for all x in G is equivalent to the permutability of a with all the group elements.

Under an inner automorphism of a group every class of conjugate elements is mapped onto itself. There exist, however, groups (and even finite ones) that have outer automorphisms with the same property (for a simple example, see Wall [1]).

The cyclic group of order 2 has only one automorphism, namely the identity. *This group is, however, the only one having no automorphism other than the identity.* For, every non-commutative group obviously has non-identity inner automorphisms. If the group G is abelian and if its elements, except the unit element,are not all of order 2, then the mapping that carries every element a of G into its inverse element a^{-1} is a non-identity

automorphism, since the commutative law implies the equation

$$(ab)^{-1} = a^{-1} b^{-1}.$$

Finally, the existence of non-identity automorphisms in non-cyclic abelian groups with elements of order 2 only follows from the complete description of the structure of such groups which will be given in § 24.

Groups of automorphisms

The endomorphisms of a group G are mappings of the group into itself. We can therefore speak of the *multiplication* of endomorphisms in the sense that they are performed in succession: If two endomorphisms χ and η of a group G are given, then their *product* $\chi\eta$ is that mapping which yields for every a in G

$$a(\chi\eta) = (a\chi)\eta.$$

The product of two endomorphisms is itself an endomorphism. For

$$(ab)(\chi\eta) = [(ab)\chi]\eta = (a\chi \cdot b\chi)\eta = (a\chi)\eta \cdot (b\chi)\eta = a(\chi\eta) \cdot b(\chi\eta).$$

The product of two automorphisms is obviously itself an automorphism.

The associative law for the multiplication of endomorphisms follows from results in § 1. The identity automorphism introduced above plays the rôle of the unit element; but it would be wrong to think that the endomorphisms of a group G constitute a group with respect to the multiplication so defined. For we cannot define the inverse of every endomorphism, because under a homomorphic mapping the original need not be single-valued. *The inverse mapping exists only for automorphisms,* and obviously it is then itself an automorphism.[9]

We see then that the set Φ of all automorphisms of a group G is itself a group. This *group of automorphisms* of G is a subgroup of the group $S(G)$ of all one-to-one mappings of G onto itself.

The inner automorphisms of a group G form a subgroup of the group of all automorphisms, since the successive transformation of G by a and b is equivalent to the transformation by ab. Moreover, we obtain a homomorphic mapping of G onto the group Φ' of its inner automorphisms if we associate with each element of G the inner automorphism induced by it. As we have mentioned above, it is precisely the elements of the center Z of G that are mapped onto the unit element of Φ', in other words, *the group of inner automorphisms of a group G is isomorphic to the factor group of its center,*

$$\Phi' \simeq G/Z.$$

It follows, in particular, that *two elements a and b of G induce the same inner automorphism if and only if they belong to the same coset of the center of G.*

The group of inner automorphisms is normal in the group of all automorphisms. For let φ be an automorphism of a group G and α the inner automorphism induced by the element a. Then for every element x of G we have

$$x(\varphi^{-1}\alpha\varphi) = [a^{-1}(x\varphi^{-1})a]\varphi = (a^{-1})\varphi \cdot (x\varphi^{-1})\varphi \cdot a\varphi = (a\varphi)^{-1}x(a\varphi),$$

that is, $\varphi^{-1}\alpha\varphi$ is itself an inner automorphism and is induced by the element $a\varphi$.

The investigation of the group of all automorphisms of a given group G is usually very difficult. In most cases the properties of a group do not carry over to its group of automorphisms. Thus, *the group of automorphisms* of an abelian group may turn out to be non-commutative—for example, the group of automorphisms of the non-cyclic group V of order 4, which we met in § 9, is the symmetric group of degree 3. On the other hand, *there exist non-commutative groups whose groups of automorphisms are abelian* (C. Hopkins [1]). However, *the group of automorphisms of a non-commutative group G cannot be cyclic,* since even the group of inner automorphisms, which is isomorphic to the factor group of G with respect to its center, cannot be cyclic (see § 11), whereas all subgroups of cyclic groups are cyclic (see § 6).

We can assert, of course, that *the group of automorphisms of a finite group of order n is itself finite.* It is a subgroup of the symmetric group of degree n and its order is therefore a divisor of $n!$ and even of $(n-1)!$, since the unit element of the group remains in place under all the auto-

morphisms of the group. Narrower bounds for the order of the group of automorphisms of a finite group may be found in papers by Birkhoff and Hall [1] and Lyapin [1].

The group of automorphisms of an infinite group may be finite—in the infinite cyclic group a generator can only be chosen in two ways, and since the property of being a generator of a cyclic group is preserved under automorphisms, it turns out that the group of automorphisms of the infinite cyclic group is finite and of order 2. But the group of automorphisms of the multiplicative group of positive rational numbers has the cardinal number of the continuum—any one-to-one mapping of the set of all prime numbers onto itself leads to an automorphism of this group.

The groups of automorphisms of non-isomorphic groups may be isomorphic. Thus, we have shown above that the group of automorphisms of the infinite cyclic group is cyclic and of order 2; but this also holds for the group of automorphisms of the cyclic group of order 3, as one can easily see. Other examples are the four-group V and the symmetric group of degree 3: both have S_3 as their groups of automorphisms (see § 13). Furthermore, there exist groups that cannot be the groups of automorphisms of any group. This is true, for example, of all *finite cyclic groups of odd order.* As we have seen above, they cannot be the group of automorphisms of non-commutative groups; but abelian groups, except the cyclic group of order 2, must always have automorphisms of order 2, so that their groups of automorphisms, if finite, are of even order.

Among the properties of a group that are preserved in its group of automorphisms is the absence of a (non-trivial) center.

If G is a group without center, then its group of automorphisms Φ also has no center.

For let φ be an automorphism of G other than the identity and let a be an element of G for which $a\varphi = a' \neq a$. If φ were in the center of Φ, then it would be permutable with the inner automorphism induced in G by a, that is, for any element g of G we would have

$$a^{-1}(g\varphi)\,a = (a^{-1}ga)\,\varphi = a'^{-1}(g\varphi)\,a'.$$

Since the element $g\varphi$ ranges over the whole of G as g does, we see that the elements a and a' induce the same inner automorphism of G and this contradicts the assumption that the center of G is trivial.

§ 13. The Holomorph. Complete groups

The transformation of a group G by one of its elements a carries every subgroup H of G into a conjugate subgroup $a^{-1}Ha$ (see § 9) and therefore maps every normal subgroup onto itself. This invariance under all inner automorphisms of the group could be used as yet another definition of a normal subgroup. The mapping onto itself which the transformation of G by an element a induces in a normal subgroup H is an automorphism of H, but in general is an outer automorphism. In other words, if one group is a normal subgroup of another, then every inner automorphism of the larger group induces some automorphism in the smaller one. The question arises whether it is possible to embed an arbitrary group G as a normal subgroup in another group such that *all* the automorphisms of G are induced by *inner* automorphisms of the larger group. We now proceed to show that the answer to this question is in the affirmative.

In § 5 we have shown that we obtain an isomorphic mapping of G into $S(G)$ (the unrestricted symmetric group) if we associate with every element a of G the mapping that carries each element x of G into xa. The subgroup $\overline{G}$ of $S(G)$ onto which G is isomorphically mapped in this way can be identified with G itself. We must distinguish, however, between the elements of G $qu\hat{a}$ symbols to be permuted and $qu\hat{a}$ elements of $S(G)$; we shall therefore denote by $\bar{a}$ the element of $\overline{G}$ that corresponds to the element a of G.

The normalizer Γ of the subgroup $\overline{G}$ in the group $S(G)$ is called the *holomorph* of the group G. From the definition of the normalizer it follows that Γ contains $\overline{G}$ as a normal subgroup. We wish to prove now that all the automorphisms of $\overline{G}$ are induced by inner automorphisms of Γ.

We know that Φ, the group of automorphisms of G, is a subgroup of $S(G)$. We now show that Φ *is contained in* Γ, that is, every automorphism φ, considered as an element of $S(G)$, is permutable with $\overline{G}$. Let $\bar{a}$ be an arbitrary element of $\overline{G}$ and consider the mapping of G obtained from the product $\varphi^{-1}\bar{a}\varphi$. Under the automorphism φ^{-1} an element x of G goes into $x\varphi^{-1}$; the mapping $\bar{a}$ now carries this element into the product $x\varphi^{-1} \cdot a$; and the automorphism φ yields

$$(x\varphi^{-1} \cdot a)\varphi = (x\varphi^{-1})\varphi \cdot a\varphi = x \cdot a\varphi.$$

So we see that the product $\varphi^{-1}\bar{a}\varphi$ coincides with the element $\overline{a\varphi}$ of $\overline{G}$; this shows that the automorphism φ belongs to the holomorph Γ.

At the same time we see, by letting $\bar{a}$ range over all the elements of $\overline{G}$,

that the transformation of $\overline{G}$ by the element φ results in that mapping of $\overline{G}$ which coincides with the automorphism φ of G: *All the automorphisms of $\overline{G}$ are induced by inner automorphisms of the holomorph* Γ.[1]

We shall now find the centralizer Z of $\overline{G}$ in $S(G)$. Suppose the mapping ζ belongs to Z, that is, for every $\bar{a}$ of $\overline{G}$

$$\bar{a}\zeta = \zeta\bar{a}. \tag{1}$$

The image of the unit element of G under the mapping ζ is an element of G which we shall denote by s^{-1}

$$1\zeta = s^{-1}.$$

Since

$$1(\bar{a}\zeta) = (1 \cdot a)\zeta = a\zeta,$$

$$1(\zeta\bar{a}) = (s^{-1})\bar{a} = s^{-1}a,$$

we have in virtue of (1)

$$a\zeta = s^{-1}a \tag{2}$$

for all a of G.

Conversely, for any s of G the mapping ζ of G onto itself defined by the equation (2) belongs to Z. For it is obviously one-to-one. If b is any element of G, then

$$a(\bar{b}\zeta) = (ab)\zeta = s^{-1}(ab),$$

$$a(\zeta\bar{b}) = (a\zeta)b = (s^{-1}a)b,$$

that is,

$$\bar{b}\zeta = \zeta\bar{b}.$$

Hence the elements of Z are of the form (2) for all elements s of G. Different mappings ζ correspond here to different elements s; that is, the correspondence between the groups G and Z is one to one. *It is indeed an isomorphism*: If ζ and η are elements of Z, s and t the corresponding elements of G, i.e. if for all a in G

$$a\zeta = s^{-1}a, \qquad a\eta = t^{-1}a,$$

then

[1] This gives us the solution of the problem raised above. The reader who would prefer to deal with the original group G rather than with $\overline{G}$ can replace in the set Γ the elements of $\overline{G}$ by the corresponding elements of G and re-define the group operation of Γ in the newly obtained set.

$$a(\zeta\eta) = (a\zeta)\eta = (s^{-1}a)\eta = t^{-1}s^{-1}a = (st)^{-1}a.$$

The subgroup Z is contained in the holomorph Γ of G and is, in fact, a normal subgroup of Γ; this follows from the remark at the end of § 11. But $\overline{G}$ is also normal in Γ. Hence

$$\{Z, \overline{G}\} = Z\overline{G}.$$

The subgroup $Z\overline{G}$ of Γ contains the whole group Φ' of inner automorphisms of G. For, the trivial equation

$$s^{-1}as = (s^{-1}a)s \tag{3}$$

shows that the transformation of G by s is equal, as an element of $S(G)$, to the product of the element of Z corresponding to s by the element $\bar{s}$ of $\overline{G}$. It also follows from equation (3) that *the subgroup Z is contained in the product of the subgroups Φ' and $\overline{G}$,* so that

$$Z\overline{G} = \Phi'\overline{G}. \tag{4}$$

The holomorph Γ coincides with the product of the subgroups Φ and $\overline{G}$ of $S(G)$,

$$\Gamma = \Phi\overline{G}.$$

For let τ be an arbitrary element of Γ. Since τ is permutable with $\overline{G}$, the transformation of $\overline{G}$ by τ induces an automorphism of $\overline{G}$ which could also be obtained, as we have shown above, by the transformation by an element φ of Φ. The element $\tau\varphi^{-1}$ is therefore permutable with every element of $\overline{G}$; that is, it belongs to Z and so, by (4), to $\Phi'\overline{G}$. The element τ therefore lies in the product $(\Phi'\overline{G})\Phi = \Phi\overline{G}$.

Complete groups. A group G is called *complete* if it has no center and no outer automorphisms. A complete group is therefore isomorphic to its group of automorphisms. The following theorem (Hölder [2]) provides important examples of complete groups.

The finite symmetric group S_n is complete when $n \geqq 3$ and $n \neq 6$.

Proof. It is clear that S_n is for $n \geqq 3$ a group without center. Let us consider its automorphisms. We begin with the remark that the elements of order 2 in S_n are precisely those that decompose into the product of disjoint cycles of length 2, i.e. into the product of independent transpositions. Let

$$a = (\alpha_1\alpha_2)(\alpha_3\alpha_4)\ \ldots\ (\alpha_{2k-1}\alpha_{2k}), \qquad 2 \leqq 2k \leqq n,$$

be one of these elements; all the α_i, $i = 1, 2, \ldots, 2k$, are distinct. We now show that *the class of conjugates of a in S_n consists of all permutations that decompose into a product of k independent transpositions.*

For if

$$b = (\beta_1\beta_2)(\beta_3\beta_4)\ldots(\beta_{2k-1}\beta_{2k})$$

is any such permutation (all the $\beta_i, i = 1, 2, \ldots, 2k$, are also distinct), then b is obtained by transforming a by an arbitrary permutation of the form

$$\begin{pmatrix} \alpha_1\alpha_2 \ldots \alpha_{2k} \ldots \\ \beta_1\beta_2 \ldots \beta_{2k} \ldots \end{pmatrix}. \tag{5}$$

Conversely, any permutation of S_n can be written in the form (5), and the transformation of a by this permutation therefore leads to an element of the form b.

We denote by C_k the class of conjugate elements of order 2 that are products of k independent transpositions. In particular, the class C_1 consists of all the transpositions $(\alpha_1\alpha_2)$.

Every automorphism of a group preserves the orders of the elements and maps a class of conjugate elements onto a complete class of conjugate elements. Therefore, if φ is an arbitrary automorphism of S_n, then it must map the class C_1 onto one of the classes $C_k, k \geqq 1$. We shall now show that *when $n \neq 6$, then the class C_1 can be mapped by the automorphism φ only onto itself.*

This is obvious for $n = 3$, because then the class C_1 contains all the elements of order 2 in the group S_3. Let $n \geqq 4$. The class C_1 consists of

$$\frac{n(n-1)}{2} \tag{6}$$

distinct elements. If now $k \geqq 2$, then the class C_k, consisting of all the elements of the form

$$(\alpha_1\alpha_2)(\alpha_3\alpha_4)\ldots(\alpha_{2k-1}\alpha_{2k}),$$

contains exactly

$$\frac{n(n-1)\ldots(n-2k+2)(n-2k+1)}{k!\,2^k} \tag{7}$$

elements: The number 2^k appears in the denominator because we can permute the symbols in each transposition, and the number $k!$ because we can permute the transpositions arbitrarily. If the class C_1 is mapped by φ

onto the class C_k, $k \geqq 2$, then these classes must consist of the same number of elements. Equating the numbers (6) and (7) we obtain the equation

$$(n-2)(n-3)\ldots(n-2k+2)(n-2k+1) = k!\,2^{k-1}. \qquad (8)$$

Since $n \geqq 2k$, this equation cannot hold for $k = 2$ and any n. *For* $k = 3$ *it is satisfied when* $n = 6$. But when $k \geqq 4$, then the left-hand side of (8) is always greater than the right-hand side; it is sufficient to verify this for $n = 2k$, which gives the smallest value to the left-hand side.

We shall assume from now on that $n \neq 6$. *If* α *is one of the permuted symbols, then there exists a symbol* α' *which is such that all the transpositions containing* α *are mapped by* φ *onto the set of all the transpositions containing* α'.

For we have shown above that the image of a transposition under φ is itself a transposition. If

$$(\alpha\beta)\varphi = (\beta'\beta''),$$
$$(\alpha\gamma)\varphi = (\gamma'\gamma''),$$

then the symbols β', β'', γ', γ'' cannot all be distinct, because then the product of the transpositions $(\alpha\beta)$ and $(\alpha\gamma)$ would be the element $(\alpha\beta\gamma)$ of order 3, while the product of their images would be of order 2.

With any four symbols the following could happen:

$$(\alpha\beta)\varphi = (\alpha'\beta'),$$
$$(\alpha\gamma)\varphi = (\alpha'\gamma'),$$
$$(\alpha\delta)\varphi = (\beta'\gamma').$$

However, the product

$$(\alpha\beta)(\alpha\delta)(\alpha\gamma) = (\alpha\beta\delta\gamma)$$

is then of order 4, while the product of the images

$$(\alpha'\beta')(\beta'\gamma')(\alpha'\gamma') = (\beta'\gamma')$$

is of order 2. This shows that the images under φ of all the transpositions of the form $(\alpha\beta)$ for given α contain a common permuted symbol α'. These images exhaust all the transpositions containing the symbol α', since otherwise the inverse automorphism φ^{-1} would lead to a contradiction to the above result.

The mapping $\alpha \to \alpha'$ is therefore a *one-to-one mapping of the set of all*

permuted symbols onto itself, that is, *it is an element of the group* S_n. We denote it by s, so that

$$\alpha' = \alpha s.$$

If $(\alpha\beta)$ is now an arbitrary transposition, then its image under φ must be a transposition that contains both the symbols αs and βs, so that

$$(\alpha\beta)\varphi = (\alpha s,\ \beta s).$$

However, on the right-hand side we have the image of the transposition $(\alpha\beta)$ under the transformation by the permutation s. Thus we have shown that *the automorphism* φ *coincides with the inner automorphism induced by the element* s; this is true for all transpositions and therefore for all the elements of S_n, which are of course products of transpositions. This completes the proof of the theorem.

In the group of automorphisms of the symmetric group S_6 the outer automorphisms form a single coset of the normal subgroup of inner automorphisms, so that the order of the group is $2 \cdot 6! = 1440$ (see Hölder [2], p. 343).

In the paper by Schreier and Ulam [3] it is shown that for any infinite set M the unrestricted symmetric group S_M is complete. Further examples of complete groups can be found in the paper by Golfand [3] in which the automorphisms of the holomorph of certain groups are studied.

The question whether non-isomorphic groups may have isomorphic holomorphs is studied by Mills [1], [2].

§ 14. Characteristic and fully invariant subgroups

Two elements a and b of a group G are said to be *of equal type* if there is an automorphism φ of G carrying a into b:

$$a\varphi = b.$$

Elements of equal type obviously have the same order. The whole group splits into disjoint *classes of elements* of equal type, each of which is a normal subset of G. A class of elements of equal type in G is a class of conjugate elements in the holomorph of G. This enables us to carry over to classes of elements of equal type many of the results that have been obtained in § 11 for classes of conjugate elements.

Subgroups and *classes of subgroups of equal type* in a group G are defined similarly. *Subgroups of equal type are clearly isomorphic and moreover*

have equal indices: If A and B are subgroups and if φ is an automorphism for which $A\varphi = B$, then for every element g of G the coset Ag is mapped by φ onto the coset $B(g\varphi)$. Since $g\varphi$ is an arbitrary element of G, this establishes a one-to-one correspondence between the right cosets of A and those of B. Our result also follows easily from the remark that a class of subgroups of equal type in G is a class of conjugate subgroups in the holomorph of G.

Just as we singled out normal subgroups as those that coincide with all their conjugate subgroups, so we shall now select subgroups that coincide with all their subgroups of equal type, i.e. that are mapped onto themselves under *all* the automorphisms of the group. Such subgroups are called *characteristic*. They are obviously normal subgroups.

A characteristic subgroup H of a group G is normal in any group $\overline{G}$ in which G is normal. For, every inner automorphism of $\overline{G}$ induces some automorphism in G and therefore maps H onto itself. Conversely, it follows immediately from the definition of the holomorph that *a subgroup H of a group G which is normal in the holomorph of G is a characteristic subgroup of G.*

The subgroups H of a group G that are mapped into themselves (that is, onto themselves or onto a proper subgroup) under *all* the endomorphisms χ of G,

$$H\chi \subseteq H,$$

are called *fully invariant* (or *fully characteristic*); they play the same rôle with respect to endomorphism as characteristic subgroups do with respect to automorphisms and normal subgroups with respect to inner automorphisms.

Every fully invariant subgroup is characteristic.

For if a subgroup A is fully invariant in G, then it is mapped into itself by all the automorphisms of G. But if an automorphism φ maps A onto a proper subgroup, then φ^{-1} maps this proper subgroup onto a subgroup properly containing it, and this contradicts the assumption.

The property of being characteristic and that of being invariant are *transitive* (in contrast to the property of being normal): *If A is characteristic (fully invariant) in B, and B in C, then A is characteristic (fully invariant) in C.* For every automorphism (endomorphism) of the group C maps B isomorphically onto itself (homomorphically into itself) and therefore maps A onto itself (into itself).

Note, however, that if

$$A \subset B \subset C$$

and if A is characteristic (fully invariant) in C, then it need not be characteristic (fully invariant) in B.

The intersection of any set of characteristic (fully invariant) subgroups of a group G and the subgroup generated by such a set are themselves characteristic (fully invariant) subgroups of G.

The first of these statements is obvious, and the second is proved as follows: If the subgroups A_α are fully invariant (α runs through some index set) and if they generate the subgroup B, then every element b of B is of the form

$$b = a_{\alpha_1} a_{\alpha_2} \dots a_{\alpha_k}, \quad a_{\alpha_i} \in A_{\alpha_i}.$$

Now if χ is an arbitrary endomorphism of G, then

$$b\chi = a_{\alpha_1}\chi \cdot a_{\alpha_2}\chi \dots a_{\alpha_k}\chi;$$

but since $a_{\alpha_i}\chi \in A_{\alpha_i}$, $b\chi \in B$. If the A_α are characteristic subgroups and χ is an automorphism, then we again obtain that $B\chi \subseteq B$. This cannot be a strict inclusion, for then χ^{-1} would map this proper subgroup onto a subgroup properly containing it.

Every group has two fully invariant, and therefore characteristic, subgroups: the group itself and the unit subgroup. Groups that have no other characteristic subgroups are called *elementary*. All simple groups, of course, are of this kind. Another example of an elementary group is the four-group V of order 4.

All subgroups of a cyclic group are fully invariant. For if the endomorphism χ maps the generator a of the cyclic group into a^k, $a\chi = a^k$, then

$$(a^s)\chi = (a\chi)^s = a^{ks},$$

so that the cyclic group of the element a^s is mapped into itself.

The center of a group is a characteristic subgroup, because if an element is permutable with all the group elements then so is its image under an automorphism: If

$$ax = xa \text{ for all } x \in G,$$

then for every automorphism φ we have

$$a\varphi \cdot x\varphi = x\varphi \cdot a\varphi,$$

but $x\varphi$ ranges over the whole of G as x does.

It should be noted, however, that *the center of a group is not always fully invariant.* Let us consider, for example, the group G of all non-singular matrices of order 2 with *rational* elements. If a is such a matrix, then its determinant is a rational number different from zero and can therefore be written in the form $(s/t) \cdot 2^{n(a)}$, where the numbers s and t are odd and n is an integer. Since the determinant of a product of matrices is equal to the product of their determinants, we have

$$n(ab) = n(a) + n(b).$$

We now define a mapping φ of G into itself by associating with every matrix a of G the matrix

$$a\varphi = \begin{pmatrix} 1 & n(a) \\ 0 & 1 \end{pmatrix},$$

which also belongs to G. The equations

$$(ab)\varphi = \begin{pmatrix} 1 & n(ab) \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n(a)+n(b) \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n(a) \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & n(b) \\ 0 & 1 \end{pmatrix} = a\varphi \cdot b\varphi$$

show that φ is an endomorphism of G. However,

$$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}\varphi = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix},$$

so that a matrix belonging to the center of G goes over into one outside the center.

As examples of fully invariant subgroups of an arbitrary group G we can take *the subgroup generated by the n-th powers of all the group elements* or *the subgroup generated by all elements of finite order.* For, the image of the n-th power of an element a under any endomorphism is the n-th power of the image of a, and every element of finite order is mapped into an element of finite order.

Commutators. Important examples of fully invariant subgroups arise from the following concept, which is also of great interest in its own right: If a and b are elements of an arbitrary group G, then the element

$$[a, b] = a^{-1}b^{-1}ab$$

is called the *commutator* of a and b. The commutator is equal to the unit element if and only if a and b are permutable, and in a certain sense it is a measure of the non-permutability of these elements, since

$$ab = ba \cdot [a, b].$$

The following properties of commutators are verified by an immediate calculation (a, b, c are arbitrary group elements):

$$[a, b][b, a] = 1; \quad \text{hence} \quad [a, b]^{-1} = [b, a]. \tag{1}$$

$$[a, b^{-1}] = b[b, a]b^{-1}, \quad [a^{-1}, b] = a[b, a]a^{-1}. \tag{2}$$

$$[ab, c] = b^{-1}[a, c]b[b, c]. \tag{3}$$

$$[a, bc] = [a, c]c^{-1}[a, b]c. \tag{4}$$

We can regard the formation of the commutator as a new operation defined in the set of group elements. This operation is not, in general, associative; that is, the equation

$$[[a, b], c] = [a, [b, c]] \tag{5}$$

does not always hold. In order to give an answer to the question of when equation (5) is satisfied in a group G, we define the following class of groups, which is much wider than that of the abelian groups.

A group G is said[h] to be *nilpotent of class* 2 if the commutator of any pair of its elements lies in the center.

Nilpotent groups will be studied in Chapter XV. Their fundamental rôle in connection with the operation of forming commutators is made clear by the two following theorems (Levi [6]).

I. *The operation of forming commutators is associative in nilpotent groups of class* 2, *and in them only.*

Equation (5) is always satisfied in a nilpotent group of class 2, since both sides are equal to the unit element. Conversely, let G be a group in which equation (5) holds for all elements a, b, c. Putting $c = b$ we obtain

$$[[a, b,], b] = 1;$$

hence by (2) and (1)

$$[a, b]^{-1} = [a, b^{-1}]. \tag{6}$$

Since a and b are arbitrary elements, we replace them in (6) by b and a^{-1} respectively and then apply (1). We obtain

$$[a, b]^{-1} = [a^{-1}, b]. \tag{7}$$

From equations (6) and (7) it follows, finally, that

$$[a, b] = [a^{-1}, b^{-1}]. \tag{8}$$

Now we again consider arbitrary elements a, b, c and change the left-hand and right-hand sides of equation (5), applying formulas (6), (7), (8), and (1), where necessary:

$$[[a, b], c] = [[a, b]^{-1}, c^{-1}] = [a, b]c\,[a, b]^{-1}c^{-1} = [a^{-1}, b^{-1}]\,c\,[a^{-1}, b]\,c^{-1};$$

$$[a, [b, c]] = [a^{-1}, [b, c]^{-1}] = a[b, c]\,a^{-1}[b, c]^{-1} = a\,[c^{-1}, b]\,a^{-1}\,[b, c^{-1}].$$

We equate the results thus obtained and after some simple manipulations arrive at the equation

$$ba^{-1}b^{-1}cab^{-1}a^{-1}c^{-1}bab^{-1}cbc^{-1} = 1.$$

Hence

$$[b^{-1}c, a]\,b^{-1}\,[a, b^{-1}c]\,b = 1$$

or in view of (1),

$$[[a, b^{-1}c], b] = 1.$$

However, $a, b^{-1}c, b$ are arbitrary elements of the group, since a, b, c are. We have thus proved that the commutator of any pair of elements of G is permutable with all the elements of the group or, in other words, that G is nilpotent of class 2.

II. *In nilpotent groups of class 2, and in them only, is the operation of forming commutators linked with multiplication by distributive laws,*

$$[ab,\ c] = [a,\ c]\,[b,\ c], \tag{3'}$$

$$[a,\ bc] = [a,\ b]\,[a,\ c]. \tag{4'}$$

For, the right-hand sides of the equations (3) and (3') are equal to each other if and only if

$$b^{-1}[a,\ c]\,b = [a,\ c]$$

for arbitrary a, b, c, that is, if the group G is nilpotent of class 2.

The derived group

The subgroup G' of a group G generated by the set of commutators of every pair of elements of G is called the *derived group* (or *commutator group*) of G. *The derived group is a fully invariant, and therefore a characteristic, subgroup.* For, any endomorphism χ of G maps the commutator $a^{-1}b^{-1}ab$ of two elements a, b into the element

$$(a^{-1}b^{-1}ab)\,\chi = (a\chi)^{-1} \cdot (b\chi)^{-1}\, a\chi \cdot b\chi,$$

which is also a commutator.

The significance of the derived group is brought out by the following theorem.

The factor group of the derived group is abelian; conversely, the derived group is contained in any normal subgroup whose factor group is abelian.

For if a and b are arbitrary elements of G, then

$$aG' \cdot bG' = abG' = ba\,[a,\ b]\,G' = baG' = bG' \cdot aG',$$

since $[a, b]$ is contained in G'. On the other hand, if the factor group G/N is abelian, then the commutator of any pair of elements of G is contained in N, that is, $G' \subseteq N$.

By virtue of the connection between normal subgroups and factor groups which was established in § 10, we deduce from the first part of this theorem that *every subgroup of a group G that contains the derived group G' of G is normal in G.*

The definition of the derived group and the above theorem enable us to re-formulate the definition of a nilpotent group of class 2 in two ways:

A group G is nilpotent of class 2 if and only if its derived group is contained in its center.

A group G is nilpotent of class 2 if and only if its center has an abelian factor group.

The derived group of a group G coincides with E if and only if the group is abelian, that is, if the group coincides with its center. This link between the derived group and the center, however, does not hold the other way round (as would appear natural at first sight): if the center of a group is the unit subgroup, then it does not follow that the derived group coincides with the group itself. For example, the symmetric group S_n with $n \geqq 3$ is a group without center; but *its derived group is the alternating group* A_n. This can be verified immediately for $n = 3$ and 4; and for $n \geqq 5$ we argue as follows: The factor group S_n/A_n is cyclic of order 2 and hence is abelian. Therefore, by the theorem above, the derived group of S_n is contained in A_n. Now since S_n is non-commutative and A_n is simple it follows that the derived group coincides with A_n. Similarly, if the derived group is the whole group, it does not follow that the center is the unit subgroup. As an illustrative example we mention, without going into details, the multiplicative group of matrices of order $n \geqq 1$ with complex elements and with determinant $+1$.

The following remark is an immediate consequence of the definition of the derived group: *The derived group of a subgroup is always contained in the derived group of the group.*

Let G' be the derived group of a group G. The derived group G'' of G' is called the *second derived group* of G. Continuing further, we obtain a descending sequence of subgroups, the so-called *derived chain* of G. This chain can be continued transfinitely if we define the α-th *derived group* $G^{(\alpha)}$ of a group G as the derived group of $G^{(\alpha-1)}$ when α is not a limit ordinal number and as the intersection of all $G^{(\beta)}$ with $\beta < \alpha$ when α is a limit ordinal number. There exists, then, an ordinal number τ whose cardinal number is not greater than that of the group G itself, for which

$$G^{(\tau)} = G^{(\tau+1)},$$

so that from this term onward the derived chain becomes stationary. Mal'cev [7] has proved that for any given τ there exist groups whose derived chain becomes stationary exactly at τ.

All the successive derived groups of a group G are fully invariant.

For a proof we need only use the fact that the property of being fully invariant is transitive and is preserved in intersections.

Let A and B be any two subsets of a group G. We define the *commutator-*

group $[A, B]$ *of these subsets* as the subgroup generated by all commutators of the form $[a, b]$, where $a \in A$, $b \in B$. Thus,

$$G' = [G, G].$$

With the help of this concept we now construct another descending sequence of fully invariant subgroups of a group G, namely its *lower central chain.* This is the sequence

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_\alpha \supseteq \ldots,$$

where

$$G_{\alpha+1} = [G_\alpha, G],$$

and when α is a limit ordinal number, G_α is the intersection of all G_β with $\beta < \alpha$. Thus, $G_1 = [G, G]$ coincides with the derived group G' of G; $G_2 = [G_1, G]$; that is, G_2 is the commutator-group of G' and G; and so on. This chain, too, becomes stationary at an ordinal number σ, and for every σ there exist groups whose lower central chain becomes stationary exactly at σ. (Mal'cev [7].)

All the terms of the lower central chain of a group G are fully invariant. Suppose this has already been proved for all G_β with $\beta < \alpha$. If α is a limit ordinal number, then we need only use the fact that the intersection of fully invariant subgroups is fully invariant. But if $\alpha - 1$ exists, then G_α is generated by the commutators of the form $[a, g]$ where $a \in G_{\alpha-1}$, $g \in G$. However, if φ is an arbitrary endomorphism of G, then

$$[a, g]\varphi = [a\varphi, g\varphi];$$

but $a\varphi \in G_{\alpha-1}$, $g\varphi \in G$, and so

$$[a\varphi, g\varphi] \in G_\alpha,$$

that is, $G_\alpha \varphi \subseteq G_\alpha$.

The concept of the lower central chain gives us yet another variant of the definition of a nilpotent group of class 2:

A group G is nilpotent of class 2 *if and only if the second term* G_2 *of its lower central chain is the unit subgroup.*

For, the equation $[G', G] = E$ is equivalent to the derived group being contained in the center. Various properties of the commutator-group of a pair of subgroups and some generalizations of this concept can be found in papers by P. Hall [2], Baer [29], and Golovin [3].

§ 15. Groups with operators

Normal, characteristic, and fully invariant subgroups of a group G play similar rôles with respect to the group of inner automorphisms, of all automorphisms and, finally, the set of all endomorphisms of G. A natural generalization of this would be the selection of an arbitrary set V of endomorphisms of G and the study of *V-invariant subgroups*, that is, subgroups that are mapped into themselves under all endomorphisms in V. We shall use this method occasionally; but for various applications—in the theory of rings, in linear algebra, etc.—of even greater value is a further generalization: the study of groups with operators.

Let G be a group and Σ a set of symbols $\sigma, \tau, \ldots$. G is called a *group with operator domain* Σ, and the symbols of Σ are called *operators* of G if with every symbol σ of Σ there is associated a certain endomorphism of G so that to each element a of G there corresponds an element $a\sigma$ of G, where

$$(ab)\sigma = a\sigma \cdot b\sigma.$$

Distinct operators of Σ may be associated with one and the same endomorphism, that is, for $\sigma \neq \tau$ we may have $a\sigma = a\tau$ for all a of G. It is this fact that makes the study of groups with operators more general than that of ordinary groups in which certain sets of endomorphisms have been selected for a special rôle.

Two groups G and $\bar{G}$ with one and the same operator domain Σ are called *operator isomorphic* if they are isomorphic and if the isomorphism between them can be established in such a way that for any two corresponding elements a of G and $\bar{a}$ of $\bar{G}$ and all σ of Σ the elements $a\sigma$ and $\bar{a}\sigma$ also correspond.

For the study of groups with operators, only operator-isomorphic groups shall be considered identical. Every group in the ordinary sense of the word can therefore give rise to several distinct operator groups. At first sight this splitting up of the group concept is inconsistent with the uniformity we achieved when we singled out the concept of group operation as the proper object of our study. We shall see, however, that many important group-theoretical theorems assert an isomorphism between certain groups (or subgroups) and that in the case of operator groups this turns out to be an operator isomorphism. It is clear that by formulating and proving these theorems for operator groups we achieve a greater generality; in order to obtain the corresponding theorems for groups without operators it then suffices to assume that the operator domain is empty.

Let G be a group with operator domain Σ and let V_Σ be the set of endomorphisms of G that correspond to the operators of Σ. A V_Σ-invariant subgroup of G is called an *admissible subgroup* of G with respect to the operator domain Σ. In other words, a subgroup H of G is admissible if for each of its elements a it also contains the corresponding elements $a\sigma$ for all σ of Σ, or if

$$H\sigma \subseteq H.$$

Thus, each operator of Σ induces an endomorphism in every admissible subgroup. Admissible subgroups can therefore be regarded as operator groups with the same operator domain. Subgroups that are admissible subgroups for *every* operator domain are precisely the fully invariant subgroups, while the center, for example, is not always admissible, as we have shown in the preceding section.

Example 1. If we take as operators of a group all the inner automorphisms, then the normal subgroups, and no others, are admissible. If all the automorphisms of the group are chosen as its operators, then the admissible subgroups are characteristic, and if the operator domain consists of the set of all endomorphisms of the group, then only the fully invariant subgroups are admissible.

Example 2. Let R be a ring, not necessarily commutative. A subset R' of R is called a *subring* if it is itself a ring with respect to the operations that are given in R. The additive group of the subring R' is obviously a subgroup of the additive group of R. A subring A of R is called a *left ideal* in R if it permits multiplication on the left by elements of R, that is, if for any a in A and r in R the product ra lies in A. *Right ideals* and *two-sided ideals* are defined similarly. In commutative rings of course one simply speaks of ideals. Every ring has two two-sided ideals: the ring itself and the zero ideal consisting of the zero only.

It is easily verified that the additive group of a ring R undergoes an endomorphism if all the elements of the ring are multiplied on the *right* by a fixed element a of R. The ring R is therefore an operator domain for its additive group and the admissible subgroups are the right ideals. Multiplication of all the ring elements on the *left* by an element a of R also induces an endomorphism of the additive group of the ring. The elements of R therefore constitute yet another operator domain for its additive group; this time the left ideals are admissible. The union of these two operator domains—every ring element must, of course, be taken in two copies—gives an operator domain for which the two-sided ideals of the ring are admissible.

EXAMPLE 3. Every vector space V over a field F is an abelian operator group with the field F as operator domain. For, the condition

$$(a+b)\alpha = a\alpha + b\alpha,$$

where $a, b \in V$, $\alpha \in F$, is part of the definition of a vector space. Admissible subgroups are the linear subspaces.

EXAMPLE 4. Every abelian group can be regarded as an operator group with the ring of integers as operator domain. The endomorphism corresponding to the integer n is the mapping of the element a into a^n (or, in additive notation, na). For in abelian groups the equation

$$(ab)^n = a^n b^n.$$

always holds. For this set of operators every subgroup is admissible.

The introduction of operators leads to a selection of the admissible subgroups from all subgroups and of the operator isomorphisms from all isomorphic mappings of the group in question. If we consider a group G with an operator domain Σ, and if V_Σ is the set of endomorphisms of G that correspond to the operators of Σ, then we can consider the group G in a natural manner as a group with operator domain V_Σ, and from the definition of admissible subgroups it follows that the same subgroups of G are admissible for Σ and for V_Σ. This remark allows us to assume, if necessary, that *the set of operators is a subset of the set of all endomorphisms of the group*. However, only the general definition of an operator domain that we have given above enables us to consider every ring as operator domain of its additive group (Example 2). For the ring may contain elements, different from the zero element, whose product with any ring element is the zero element.

Many of the concepts that we have introduced and some of the theorems that we have proved previously for groups without operators can be carried over to the case of operator groups. We shall indicate here the concepts and results that will be used later; the details of the proofs are left to the reader.

Let G be a group with operator domain Σ. About the admissible subgroups of G we can state the following:

The intersection of any set of admissible subgroups is itself an admissible subgroup. The intersection of all admissible subgroups that contain a given subset M of G is called the *admissible subgroup generated by* M. If M con-

sists of a single element a, then we obtain the *admissible cyclic subgroup* or *monogenic subgroup* of a which differs, in general, from the cyclic subgroup $\{a\}$. *The subgroup generated by any set of admissible subgroups and the union of an ascending sequence of admissible subgroups are themselves admissible subgroups.*

If the admissible subgroup generated by a subset M coincides with the whole group G, then M is a *system of generators for G for the operator domain* Σ. Note that a group may have a finite system of generators for a given operator domain, although as a group in the ordinary sense of the word it may not be finitely generated. For example, the n-dimensional vector space V over a field F has, *quâ* operator group, a system of n generators—any basis of the space will do—while the group V, for a non-denumerable field F, is also non-denumerable, so that as a group without operators it cannot be finitely generated.

If,

$$G_1, G_2, \ldots, G_n, \ldots$$

are groups with the same operator domain Σ and if for each n there exists an operator-isomorphic mapping φ_n of G_n into G_{n+1}, then the (direct) limit group $\overline{G}$ of these groups (see § 7) is also an operator group with the operator domain Σ, and the groups G_n $(n = 1, 2, \ldots)$ are operator-isomorphic to certain admissible subgroups of $\overline{G}$.

A normal subgroup of an operator group which is an admissible subgroup of that group is called an *admissible normal subgroup*. The intersection of any set of admissible normal subgroups and the subgroup generated by such a set are themselves admissible normal subgroups. A group that has no admissible normal subgroups except the group itself and the unit subgroup is called *simple* (with respect to the given operator domain). Such a group when considered without operators need not, of course, be simple.

If G and G' are groups with the same operator domain, then in analogy to the operator isomorphism we call a homomorphic mapping of G onto G' an *operator homomorphism* if for any a of G and its image a' in G' and for every operator σ of Σ the image of $a\sigma$ under this homomorphism is $a'\sigma$. The normal subgroup of G that is mapped onto the unit element $1'$ of G' under such a homomorphism is admissible, for as $1'\sigma = 1'$ for all σ of Σ, it follows that this normal subgroup when it contains an element a also contains all the elements $a\sigma$.

Conversely, let an operator group G with operator domain Σ be mapped homomorphically onto a group G' and let the kernel H of this homomorphism

be admissible. Then the operators of Σ can be *transferred* to G' in the following way: If a' is an element of G' and σ an operator of Σ, then we take one of the originals a of a' in G and denote the image of $a\sigma$ by $a'\sigma$. It is easy to see that the element $a'\sigma$ is independent of the choice of a, because the normal subgroup is admissible. We obtain, in particular, that *the factor group of an operator group with respect to an admissible normal subgroup is also an operator group with the same operator domain, and the natural homomorphic mapping of the group onto its factor group is an operator homomorphism.*

The reader can now prove without any difficulty that every group G' onto which a group G can be mapped operator homomorphically is operator isomorphic to the factor group of G with respect to some admissible normal subgroup; that is, he can prove the *homomorphism theorem* for operator groups.

If H is an admissible normal subgroup of G, then in the relation that exists between subgroups of G containing H and subgroups of the factor group G/H *admissible subgroups correspond to admissible subgroups.* The proof of this statement follows immediately from an application of the above method of transferring operators to a factor group.

The *isomorphism theorem* also remains valid for operator groups:

If A and B are admissible subgroups of an operator group G and if A is a normal subgroup of $\{A, B\}$, then the intersection $A \cap B$ is an admissible normal subgroup of B and the factor groups $\{A, B\}/A$ and $B/(A \cap B)$ are operator isomorphic.

The proof of this theorem is the same as without operators. The operator isomorphism is obtained as a consequence of applying the homomorphism theorem for operator groups.

Zassenhaus' lemma can also be extended to groups with operators. In its formulation we must again speak of admissible subgroups and of operator isomorphisms.

An *operator endomorphism* of a group G with operator domain Σ is an operator-homomorphic mapping of G onto or into itself. In other words, χ is an operator endomorphism if for every element a of G and every operator σ of Σ we have

$$(a\sigma)\chi = (a\chi)\sigma. \tag{1}$$

A special case of the concept of an operator endomorphism is the concept of an *operator automorphism*, that is, an operator-isomorphic mapping of G onto itself.

An immediate consequence of the definition of an operator endomorphism is the following theorem (in which the term permutability must be understood in the sense that the multiplication of endomorphisms is commutative):

An endomorphism χ of a group G is an operator endomorphism with respect to an operator domain Σ if and only if it is permutable with all endomorphisms that correspond to the operators of Σ, that is, with all endomorphisms of the set V_Σ.

For the proof, we replace the operator σ in (1) by the endomorphism corresponding to it. As an example, we note that the operator endomorphisms of a vector space V over a field F are precisely the linear transformations, since the conditions

$$(a+b)\varphi = a\varphi + b\varphi, \qquad (a\alpha)\varphi = (a\varphi)\alpha,$$

where $a, b \in V$, $\alpha \in F$, constitute the definition both of a linear transformation and of an operator endomorphism.

All the properties of operator endomorphisms and automorphisms follow easily from this theorem. For example, *the product of two operator endomorphisms is itself an operator endomorphism.* So is the null endomorphism. We note, further, that the identity automorphism, being permutable with all endomorphisms, is always an operator automorphism; the same applies to the inverse automorphism of an operator automorphism. In conjunction with the above remarks on the product of operator endomorphisms and automorphisms this permits us to speak of the *group of operator automorphisms* of an operator group. This is a subgroup of the group of all automorphisms.

Finally, we remark that *the image of an admissible subgroup of an operator group G under an operator endomorphism is an admissible subgroup*: If H is an admissible subgroup, that is, if for every operator σ

$$H\sigma \subseteq H,$$

then for an operator endomorphism χ we have

$$(H\chi)\sigma = (H\sigma)\chi \subseteq H\chi,$$

so that the subgroup $H\chi$ is admissible. This also follows from the homomorphism theorem.

In particular, the image of the group G itself under an operator endomorphism is an admissible subgroup.

CHAPTER V

SERIES OF SUBGROUPS. DIRECT PRODUCTS. DEFINING RELATIONS

§ 16. Normal series and composition series

In the theory of groups and its applications certain ordered systems of subgroups of a given group play an important rôle: the subgroups are embedded in one another and the systems are subject to various additional conditions. In the present section we shall study properties of such ordered systems or "series" of subgroups; the results to be obtained here will find many applications later.

A finite system of subgroups of a group G

$$G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_k = E \tag{1}$$

beginning with G itself and ending with the unit subgroup, is called a *normal series* of G if every subgroup G_i is a proper normal subgroup of G_{i-1}, $i = 1, 2, \ldots, k$. In particular, G_1 is a normal subgroup of G, G_2 is a normal subgroup of G_1, but not necessarily of G, and so on.

Every group, of course, has normal series: we need only take, for example, the series $G \supset E$. If H is a normal subgroup of G, distinct from G and E, then

$$G \supset H \supset E$$

is a normal series. In other words, *in every group G there exist normal series that pass through a given normal subgroup of G.*

The factor groups

$$G/G_1,\ G_1/G_2,\ \ldots,\ G_{k-1}/E$$

are called the *factors* of the normal series (1). The number of factors is called the *length* of the series; the length of the series (1), for example, is k.

A normal series

$$G \supset H_1 \supset H_2 \supset \ldots \supset H_l = E \tag{2}$$

is called a *refinement* of the normal series (1) if every subgroup G_i of (1) coincides with one of the subgroups H_j, that is, if all the subgroups that occur in (1) also occur in (2). In particular, every normal series is a

refinement of itself. The lengths of the normal series (1) and its refinement (2) of course satisfy the inequality $k \leqq l$.

Two normal series of a group are called *isomorphic* if their lengths are equal and their factors can be put into one-to-one correspondence in such a way that corresponding factors are isomorphic groups. In this definition it is not assumed that the correspondence should preserve the order of the factors. For example, if we take a cyclic group of order six, $G = \{a\}$, $a^6 = 1$, then the normal series $G \supset \{a^2\} \supset E$ and $G \supset \{a^3\} \supset E$ are isomorphic—since their factors are one cyclic group of order two and one of order three—although the factors are differently arranged in the two series.

All the definitions given above carry over to the case of groups with operators. In the definition of a normal series we must, of course, speak of admissible subgroups and admissible normal subgroups and, in the definition of isomorphic series, of operator-isomorphic factors. All further developments of the present section are presented on the understanding that *all the groups to be studied have a (possibly empty) set of operators.*

The following theorem is fundamental in the theory of normal series:[1]

Schreier's Theorem. *Any two normal series of an arbitrary group have isomorphic refinements.*

Proof: Let

$$G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_k = E \tag{3}$$

$$G = H_0 \supset H_1 \supset H_2 \supset \ldots \supset H_l = E \tag{4}$$

be two normal series of a group G. Put

$$G_{ij} = G_i \cdot (G_{i-1} \cap H_j);$$
$$H_{ij} = H_j \cdot (H_{j-1} \cap G_i);$$

here G_{ij} and H_{ij} are groups since, for example, G_i is a normal subgroup, and $G_{i-1} \cap H_j$ a subgroup, of G_{i-1}. For $i = 1, 2, \ldots, k$, and $j = 1, 2, \ldots, l$, we now have

$$G_{i-1} = G_{i0} \supseteq G_{i,\,j-1} \supseteq G_{ij} \supseteq G_{i1} = G_i,$$
$$H_{j-1} = H_{0j} \supseteq H_{i-1,\,j} \supseteq H_{ij} \supseteq H_{kj} = H_j.$$

By Zassenhaus' lemma (§ 10 and § 15) G_{ij} is a normal subgroup of $G_{i,\,j-1}$, and H_{ij} a normal subgroup of $H_{i-1,\,j}$, and the corresponding factor groups are isomorphic,

$$G_{i,\,j-1}/G_{ij} \simeq H_{i-1,\,j}/H_{ij}. \tag{5}$$

[1] O. Schreier [5]. The proof in the text is due to Zassenhaus [1].

If we insert in (3) all the subgroups G_{ij}, $j = 1, 2, \ldots, i-1$, between G_{i-1} and G_i, $i = 1, 2, \ldots k$, then we obtain a refinement of (3) which is, in general, a *normal series with repetitions*, because some subgroups $G_{i,j-1}$ and G_{ij} may be equal. Similarly, we construct a refinement of (4) by means of the subgroups H_{ij}. These refinements are isomorphic, by (5). To conclude the proof it now remains to eliminate the repetitions. However, if $G_{i,j-1} = G_{ij}$, that is, if $G_{i,j-1}/G_{ij} = E$, then we have by (5) $H_{i-1,j} = H_{ij}$, and therefore we can eliminate simultaneously all the repetitions in these refinements of the series (3) and (4) without destroying the isomorphism. This completes the proof of Schreier's theorem.

A normal series that has no refinement (without repetitions) other than itself is called a *composition series*. In other words,

$$G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_k = E$$

is a composition series of G if every G_i, $i = 1, 2, \ldots, k$, is a proper maximal normal subgroup of G_{i-1}. All the factors of a composition series are obviously simple groups. Conversely, every normal series whose factors are all simple groups cannot be further refined; that is, such a series is a composition series. Therefore every normal series that is isomorphic to a composition series is itself a composition series.

The following theorem is an immediate consequence of Schreier's theorem:

JORDAN-HÖLDER THEOREM. *If a group G has a composition series, then any two composition series of G are isomorphic.*

For, any isomorphic refinement of the given pair of composition series must coincide with both these series.

If a group G has a composition series, then every normal series of G can be refined to some composition series; its length, therefore, does not exceed the length of the composition series of G.

For the proof it is sufficient to apply Schreier's theorem to the given normal series and to one of the composition series of the group.

For brevity, we shall in the sequel call the common length of the composition series of a group the *composition length* and the factors of any composition series the *composition factors* of the group.

It is by no means true that every group has a composition series. For example, every normal series of the infinite cyclic group has proper refinements. For, the last subgroup but one of such a series is itself an infinite cyclic group, and therefore additional terms can be inserted between it and

the unit subgroup. More generally, an abelian group without operators must be finite if it has composition series, since the composition factors of such a group can only be cyclic groups of prime order. Every finite group has a composition series, of course. So does every simple group G—the existence of infinite simple groups has been proved in § 9—the only composition series being $G \supset E$. We shall prove below a simple necessary and sufficient condition for the existence of a composition series in a group. First we require some new definitions.

We shall say that a subgroup H of a group G is an *accessible subgroup* if it occurs in a normal series of G. In other words, the accessible subgroups of a group G are all the normal subgroups of G, all the normal subgroups of these, and so on. It is clear that an accessible subgroup of an accessible subgroup is itself an accessible subgroup.

A descending sequence of subgroups of a group G,

$$G = H_0 \supset H_1 \supset H_2 \supset \ldots \supset H_n \supset \ldots, \tag{6}$$

is called a *descending normal chain* of G if every subgroup H_n, $n = 1, 2, \ldots$ is a proper normal subgroup of H_{n-1}. A descending normal chain can be either countable, with the order type of the natural numbers, or finite. In the latter case we say that the chain *breaks off*. Every normal series is an example of a normal chain that breaks off. The following sequence of subgroups of the infinite cyclic group $G = \{a\}$ serves as an example of an infinite descending normal chain:

$$G \supset \{a^2\} \supset \{a^4\} \supset \ldots \supset \{a^{2^n}\} \supset \ldots.$$

An ascending sequence of subgroups of a group G,

$$E \subset F_1 \subset F_2 \subset \ldots \subset F_n \subset \ldots, \tag{7}$$

is called an *ascending normal chain* of G if every subgroup F_n, $n = 1, 2, \ldots$, is a proper normal subgroup of F_{n+1} and if all the subgroups F_n are accessible in G.[1] An ascending normal chain can be either infinite or finite; examples of the former can be found in the additive group of rational numbers or in a group of type p^∞ (§ 7).

A group G has a composition series if and only if all ascending and all descending normal chains break off.

---

[1] The last condition is automatically fulfilled in the case of descending normal chains.

For let G be a group with a composition series and let k be its composition length. If G had an infinite descending normal chain (6), then for $n \geqq k$ the normal series

$$G \supset H_1 \supset H_2 \supset \ldots \supset H_n \supset E,$$

consisting of the first n terms of (6) and the unit subgroup, would have a length exceeding k. But this contradicts Schreier's theorem. Assume now that G has an infinite ascending normal chain (7). Then we take $n \geqq k$ and construct any normal series of G containing F_n:

$$G \supset G_1 \supset \ldots \supset G_{s-1} \supset F_n \supset \ldots \supset E, \quad s \geqq 1.$$

Such a series exists since F_n is, by assumption, an accessible subgroup. But then the series

$$G \supset G_1 \supset \ldots \supset G_{s-1} \supset F_n \supset F_{n-1} \supset \ldots \supset F_2 \supset F_1 \supset E$$

is normal and its length is greater than k, which again contradicts Schreier's theorem.

Conversely, let us assume that all ascending and descending normal chains of a group G break off. From the fact that the ascending chains break off it follows that *every accessible subgroup H of G* (other than E) *must have at least one proper maximal normal subgroup*. For if every proper normal subgroup of H were contained in a larger proper normal subgroup, then we would obtain an infinite ascending chain of normal subgroups of H, and this would be an ascending normal chain of G.

We now construct the required composition series of G as follows: We take a proper maximal normal subgroup H_1 of G. If

$$H_0 = G, \quad H_1, \quad H_2, \quad \ldots, \quad H_n,$$

have been chosen in such a way that each is a proper maximal normal subgroup of the preceding one, then H_n is obviously accessible in G. If $H_n \neq E$ we take as H_{n+1} one of the maximal normal subgroups of H_n. Since a descending normal chain breaks off, we must arrive at the unit subgroup E after a finite number of steps, that is, we obtain a composition series of G. This completes the proof.

If a group has a composition series, what can we say about its subgroups? The example of the countable alternating group (see § 4) shows that *a group with a composition series may contain a subgroup that has no com-*

position series. For, the group is known to be simple (see § 9) and so has a composition series, but its subgroup generated by the permutations

$$b_n = (4n-3,\ 4n-2)(4n-1,\ 4n),\ n = 1,\ 2,\ \ldots,$$

is infinite and abelian—the latter because all the elements b_n are clearly permutable—and therefore cannot have a composition series.

However, *every accessible subgroup H of a group G with a composition series has itself a composition series.* For H occurs in a normal series of G, which by assumption can be refined to a composition series. The segment of this series between H and the unit subgroup is a composition series for H. It also follows that *if H is a proper accessible subgroup of G, then the composition length of H is less than that of G and the composition factors of H form part of the system of composition factors of G.* Furthermore, if H is a normal subgroup of G, then the segment between G and H of a composition series containing H leads to a composition series of the factor group G/H. Hence it follows that every factor group G/H of a group G with a composition series has itself a composition series; its composition length is equal to the difference between the composition lengths of G and H, and its composition factors together with the composition factors of H form the system of composition factors of G.

Certain conclusions about arbitrary subgroups of a group with a composition series can be reached from the following theorem, which refers to arbitrary groups:

If a normal series

$$G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_k = E, \tag{8}$$

is given in a group G, then every subgroup F of G has a normal series whose factors are isomorphic to subgroups of distinct factors of (8).

For if $F_i = F \cap G_i$, $i = 0,\ 1,\ 2,\ \ldots,\ k$, then by applying Zassenhaus' lemma to the case $A = F$, $A' = E$, $B = G_{i-1}$, $B' = G_i$ we find that F_i is a normal subgroup of F_{i-1} and that

$$F_{i-1}/F_i \simeq G_i F_{i-1}/G_i.$$

But $G_{i-1} \supseteq G_i F_{i-1} \supseteq G_i$, that is, the factor group F_{i-1}/F_i is isomorphic to a subgroup of the factor group G_{i-1}/G_i. The series

$$F = F_0 \supseteq F_1 \supseteq F_2 \supseteq \ldots \supseteq F_k = E$$

after deletion of all repetitions, is therefore the required normal series of F.

The theorems of Schreier and Jordan-Hölder and the deductions from them have been obtained for groups with an arbitrary operator domain. If all the inner automorphisms are adjoined to the operator domain, then only the normal subgroups remain admissible. In this case the concept of a composition series turns into that of a principal series: a series of subgroups

$$G = H_0 \supset H_1 \supset H_2 \supset \ldots \supset H_k = E$$

is called a *principal series* of G if every H_i, $i = 1, 2, \ldots, k$, is a maximal normal subgroup of G contained in H_{i-1} as a proper subgroup. The condition for the existence of a composition series that we have proved above turns in the present case into the following theorem:

A group G has a principal series if and only if all its ascending and descending chains of normal subgroups break off.

Such chains will in the sequel be called ascending and descending *principal chains* of G.

The Jordan-Hölder theorem leads in this case to the following theorem:

If a group has a principal series, then any two of its principal series are isomorphic.

The connection between the composition series of a group and of its accessible subgroups does not carry over to the case of principal series. For if a group G has a principal series and if we take one that passes through a given normal subgroup H, then the segment between H and E need not be a principal series of H, since there may exist, in general, normal subgroups of H that are not normal in G.

If the operator domain contains all the automorphisms (or all the endomorphisms) of a group G then the concept of a composition series turns into that of a *characteristic* (or a *fully invariant*) *series*, that is, a series of subgroups of G each of which is a maximal characteristic (fully invariant) subgroup of G contained in the preceding group as proper subgroup.

In this case we obtain from the Jordan-Hölder theorem the following theorem:

If a group has a characteristic (fully invariant) series, then any two characteristic (fully invariant) series of the group are isomorphic.

Further developments of the results of this section will be found in § 56.

§ 17. Direct Products

One of the most important concepts in the whole of group theory is that of the direct product or (when the group operation is written as addition) the direct sum. It is fundamental, in particular, for one branch: the theory of abelian groups. In the present section we shall define the concept and derive some of its simplest properties, while the deeper theory will be treated separately in Chapter XI.

A group G is called the *direct product* of its subgroups $H_1, H_2, \ldots, H_n$ if the following three conditions are satisfied:

1) The subgroups $H_1, H_2, \ldots, H_n$ are normal in G.

2) G is generated by the subgroups $H_1, H_2, \ldots, H_n$.

3) The intersection of every $H_i, i = 1, 2, \ldots, n$, with the subgroup generated by all $H_j, j \neq i$, is E.

This definition is equivalent to the following: G is the direct product of its subgroups $H_1, H_2, \ldots, H_n$ if

1') the elements of any two subgroups H_i and $H_j, i \neq j$ are permutable,

2') every element g of G has a unique representation as a product

$$g = h_1 h_2 \ldots h_n,$$

where $h_i \in H_i, i = 1, 2, \ldots, n$.

Let us show that *the second definition follows from the first.* In order to prove 1') we take elements $a \in H_i, b \in H_j, i \neq j$. Then by 1) we have $a^{-1}b^{-1}a \in H_j$, $b^{-1}ab \in H_i$ so that the commutator $a^{-1}b^{-1}ab$ is contained in $H_i \cap H_j$, which by 3) is E. For the proof of 2') we note that we can write any element g of G in at least one way as a product $g = h_1 h_2 \ldots h_n$; this follows from 2) and the condition 1') which we have already established. This representation is unique; for if we had

$$g = h_1 h_2 \ldots h_n = h_1' h_2' \ldots h_n',$$

where $h_1 \neq h_1'$ say, then again from 1') we would obtain

$$h_1'^{-1} h_1 = (h_2' \ldots h_n')(h_2 \ldots h_n)^{-1} = (h_2' h_2^{-1}) \ldots (h_n' h_n^{-1}),$$

and this contradicts 3).

Conversely, *the first definition follows from the second.* For 2) is part of 2'). For the proof of 3) we assume that the intersection of H_1, say, with the subgroup generated by $H_2, \ldots, H_n$ contains an element c other than

the unit element. This element is contained in H_1 and can also be written as a product $h_2 \dots h_n$ by 1'); but this contradicts 2'). For the proof of 1) we take an element $\bar{h}_i$ of H_i and an arbitrary element g of G. By 2') we have $g = h_1 h_2 \dots h_i \dots h_n$, and then by 1')

$$g^{-1}\bar{h}_i g = h_i^{-1}\bar{h}_i h_i \in H_i.$$

The task of verifying that a given group G is the direct product of its subgroups $H_1, H_2, \dots, H_n$ is simplified considerably by the remark that in the first definition condition 3) can be replaced by the much weaker condition

3_0) The intersection of $H_i, i = 1, 2, \dots, n$, with the subgroup generated by $H_1, \dots, H_{i-1}$ is E.

For the proof it is sufficient to show that 1') and 2') can be deduced from 1), 2), and 3_0). From 3_0) we obtain easily that $H_i \cap H_j = E$, $i \neq j$ so that 1') follows as before. It remains to prove the uniqueness which is part of 2'). If we could find an element g with two distinct representations

$$g = h_1 h_2 \dots h_n = h_1' h_2' \dots h_n',$$

where $h_k \neq h_k'$, while $h_{k+1} = h_{k+1}', \dots, h_n = h_n'$, $k \leqq n$, then we would get

$$h_k'^{-1} h_k = (h_1' h_1^{-1})(h_2' h_2^{-1}) \dots (h_{k-1}' h_{k-1}^{-1}),$$

but this contradicts 3_0).

If a group G is decomposed into the direct product of its subgroups $H_1, H_2, \dots, H_n$, then we call these subgroups the *direct factors* of the given decomposition and we write

$$G = H_1 \times H_2 \times \dots \times H_n.$$

So far we have defined the direct product for a finite number of direct factors only; but this concept can also be used for an *infinite set of direct factors*. The basic definition is then the following: A group G is called the direct product of a certain set of subgroups H_α (α ranges over a given index set) and is written in the form

$$G = \prod_\alpha H_\alpha,$$

if G is generated by these subgroups and if the subgroup of G that is gen-

erated by any finite number of subgroups H_α is their direct product. From this definition we deduce easily that elements of distinct subgroups H_α are permutable and that every element of G has a unique representation as a product of a *finite number* of elements of some of the subgroups H_α (unique, that is, apart from the order of the factors). Moreover, it is easy to see that every subgroup H_α is normal in G: if g is an arbitrary element of G, then $g = h_{\alpha_1} h_{\alpha_2} \dots h_{\alpha_k}$, and since by assumption the subgroups $H_{\alpha_1}, H_{\alpha_2}, \dots, H_{\alpha_k}$ form a direct product in G, we have $g^{-1} H_\alpha g = H_\alpha$. In the same way we can show that the intersection of any subgroup H_α with the group generated by all subgroups $H_{\alpha'}$, $\alpha' \neq \alpha$, is E.

Making use of these remarks we could formulate other definitions of the direct product of an infinite set of subgroups, definitions that are equivalent to the one given above but that do not require a preliminary consideration of the case of a finite number of factors. For example, the reader will have no difficulty in proving the following parallel to one of the definitions given above for the case of a finite number of factors.

A group G is the direct product of its subgroups H_α if and only if

1. the elements of any two distinct subgroups H_α are permutable, and
2. every element of G has a unique representation (apart from the order of the factors) as a product of a finite number of elements chosen from the subgroups H_α.[1]

We now indicate some very simple properties of direct products which follow immediately from the definition.

I. *If*

$$G = \prod_\alpha H_\alpha, \tag{1}$$

and if the factors H_α are again decomposed[1] *into direct products,*

$$H_\alpha = \prod_\beta H_{\alpha\beta}$$

then G is the direct product of all subgroups $H_{\alpha\beta}$, taken over all α and β. This new direct decomposition of G is called a *refinement* of the decomposition (1).

II. *If* (1) *is a direct decomposition of a group G, and if we split the set of subgroups H_α in an arbitrary way into disjoint subsets and replace the*

[1] Some of the H_α may, of course, remain undecomposed.

subgroups H_α that enter into each of these subsets by their product, then we obtain a new direct decomposition of G.

III. *If we choose in each direct factor H_α of the decomposition* (1) *a subgroup H'_α, $E \subseteq H'_\alpha \subseteq H_\alpha$, then the subgroup generated in G by all subgroups H'_α is their direct product.*

If $G = H_1 \times H_2 \times \ldots \times H_n$, then each element g of G can be written in the form $g = h_1 h_2 \ldots h_n$, where $h_i \in H_i, i = 1, 2, \ldots n$. The uniquely defined element h_i is called the *component* of g in the direct factor H_i. We must point out that the component of g in H_i depends on the given direct decomposition:[1] if there is another direct decomposition of G that also contains H_i as one of its direct factors, then the component of g in H_i may now differ from h_i. The concept of a component of an element carries over to direct products with an infinite number of factors; in this case each element has for a given direct decomposition *only a finite number of components distinct from* 1.

If $G = \prod_\alpha H_\alpha$ and if F is an arbitrary subgroup of G, then the set F_α of components of all the elements of F in the direct factor H_α is itself a subgroup. It is called the *component* of F in H_α. If F is a normal subgroup of G, then F_α is a normal subgroup of H_α and therefore also of G. The latter follows from the following general property of direct products:

IV. *If A is a direct factor of a group G, then every normal subgroup A' of A is also normal in G.*

For there exists a normal subgroup B of G for which $G = A \times B$. If g is an arbitrary element of G and $g = ab, a \in A, b \in B$, then

$$g^{-1}A'g = a^{-1}A'a = A'.$$

From the permutability of elements belonging to distinct direct factors of a given direct product it follows that *the components of the product of two elements are the products of the corresponding components.* Therefore, in particular, *a component of the commutator of two elements of a direct product is the commutator of the corresponding components of the elements.* Hence we have

V. *The derived group of a direct product is the direct product of the derived groups of the factors.*

From what we have just shown about the components of the commutator of two elements it follows that *the components of permutable elements of a direct product are permutable,* and therefore

VI. *The center of a direct product is the direct product of the centers of the factors.*

For if an element z belongs to the center of the group $G = \prod_{\alpha} A_\alpha$, then the component z_α of z in H_α is permutable with the corresponding component of every element of G, that is, with all the elements of H_α.

If F is a subgroup of a direct product, then F is contained in the direct product of its components, but it does not, in general, coincide with this product.

F is the direct product of its components when they are all contained in F, that is, when they coincide with the intersections of F and the corresponding direct factors. We can even prove the following property:

VII. *If $G = A \times B$ and if the component of F in A coincides with $F \cap A$, then the component of F in B is $F \cap B$ and F is the direct product of these two intersections.*

For if $f \in F$ and $f = ab$, then $b = a^{-1}f \in F$, since by assumption $a \in F$.

Hence we have

VII′. *If $G = A \times B$ and if the subgroup F contains the direct factor A, then $F = A \times (F \cap B)$.*

Finally, we mention the property

VIII. *If $G = A \times B$, then the direct factor B is isomorphic to the factor group G/A.*

For if Ag is a coset of A in G and if $g = ab$, then $b \in Ag$; that is, each coset of A contains one, and obviously only one, element of B.

So far we have dealt with the decomposition of a given group into the direct product of subgroups. In the sequel we shall often talk of the *direct product of certain given groups*. Suppose, for example, that two groups A and B are given. The set of all pairs (a, b), where a is an element of A and b an element of B, becomes a group if the operation is defined as follows:

$$(a, b) \cdot (a', b') = (aa', bb').$$

It is easily verified that this group is the direct product of its subgroup A' consisting of the pairs of the form $(a, 1)$ and B' consisting of the pairs of the form $(1, b)$.[1] These subgroups are isomorphic to the given groups A

[1] The element 1 in the pair $(a, 1)$ is, of course, the unit element of B, while in $(1, b)$ it is the unit element of A.

and B, respectively, and therefore the group we have constructed can, and from now on will, be called the direct product of A and B. This construction carries over without difficulty to the case of an arbitrary finite number of given groups. If an infinite set of groups A_α is given, then we can proceed in the following way: the elements of the direct product of the groups A_α are those systems of elements a_α, one from each group A_α, in which *all but a finite number of these elements are the unit elements of the corresponding groups.* The definition of multiplication of such systems is the same as in the case of a finite number of direct factors.

This method of forming a new group from given groups by the construction of their direct product will have many applications in the sequel.

In our construction of the direct product of an infinite set of groups we could, of course, have omitted the condition that only a finite number of components should differ from the unit element; we would then consider arbitrary systems of elements, one from each of the given groups A_α. The group so obtained is called the *unrestricted direct product* (or *complete direct product* or *Cartesian product*) of the given groups; interesting properties of this group are described in the paper by Graev [1]. We must mention, however, that for the unrestricted direct product one cannot give an "internal" definition similar to the one we have used above for the ordinary or *restricted* direct product.

These two types of direct products are unified in the following construction of the *direct product with prescribed subgroups*: it is assumed that in each of the given groups A_α a subgroup B_α is prescribed, and only such systems of elements, one from each group A_α, are considered which have not more than a finite number of elements outside the corresponding subgroup B_α; multiplication is component-wise as above. This construction, which is due to Vilenkin [1], is used with advantage in the theory of topological abelian groups.

A group that cannot be decomposed into the direct product of proper subgroups is called *indecomposable*, or, more accurately, indecomposable into a direct product (since we shall later meet other forms of products). *Among the indecomposable groups are, obviously, all the simple groups. The additive group of rational numbers and the additive group of integers, that is, the infinite cyclic groups, are also indecomposable.* This follows from the fact that any two rational numbers have a common non-zero multiple, so that the intersection of any two non-zero subgroups is in both cases itself a non-zero subgroup.

If a cyclic group $\{a\}$ of order p^m is given, where p is a prime number,

then all subgroups other than E are the cyclic subgroups of the elements a, a^p, a^{p^2}, ..., $a^{p^{m-1}}$. In other words, if any two subgroups of the group are given, then one of them is completely contained in the other. Therefore *the cyclic groups of order p^m and the groups of type p^∞ are indecomposable.*

On the other hand *every cyclic group of composite order is decomposable into the direct product of cyclic groups whose orders are powers of distinct prime numbers.*

Let $\{a\}$ be a cyclic group of order

$$n = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k},$$

where $k \geqq 2$ and $p_1, p_2, \dots, p_k$ are distinct prime numbers. We put

$$q_i = p_1^{m_1} \dots p_{i-1}^{m_{i-1}} p_{i+1}^{m_{i+1}} \dots p_k^{m_k} \quad (i = 1, 2, \dots, k).$$

The element a^{q_i} has the order $p_i^{m_i}$. The intersection of the cyclic subgroup $\{a^{q_i}\}$ with the product of all cyclic subgroups $\{a^{q_j}\}$ with $i \neq j$ is E, since the orders of all elements of the latter product are co-prime to p_i. The product of the subgroups $\{a^{q_i}\}, i = 1, 2, \dots, k$ in the group $\{a\}$ is therefore direct and coincides with the group $\{a\}$ itself, since the order of a direct product is equal to the product of the orders of the factors.

Other examples of decomposable groups are the additive group of complex numbers, which splits into the direct sum of the additive group of real and of pure imaginary numbers; also the multiplicative group of non-zero real numbers, which splits into the direct product of the multiplicative group of positive real numbers and the cyclic group of order 2 generated by -1. The multiplicative group of positive rational numbers splits into the direct product of a countable set of infinite cyclic groups generated by the distinct prime numbers. We have already mentioned that the non-cyclic abelian group V of order 4 is the direct product of two cyclic groups of order 2.

The concept of a direct product can also be applied to groups with operators. In this case we must, of course, restrict ourselves to decompositions of the group into the direct product of factors which are all admissible for the given operator domain. Conversely, if groups A_α with one and the same operator domain Σ are given, then we can consider the direct product G of these groups as an operator group with Σ as operator domain by postulating that for

$$g = a_{\alpha_1} a_{\alpha_2} \dots a_{\alpha_k}, \quad g \in G, \quad a_{\alpha_i} \in A_{\alpha_i},$$

we have

$$g\omega = a_{\alpha_1}\omega \cdot a_{\alpha_2}\omega \ldots a_{\alpha_k}\omega,$$

where $\omega \in \Sigma$. From this equation it follows, in particular, that *a component of an admissible subgroup is itself an admissible subgroup.*

We shall see later (in § 26) that there exist decomposable groups that cannot be split into the direct product of indecomposable groups. The question, therefore, arises under what conditions a group has such a decomposition. Moreover, a group may have many distinct decompositions. This leads to the problem, Under what conditions is the decomposition of a group into the direct product of indecomposable groups unique? Further, two direct decompositions of a group are called *isomorphic* if a one-to-one correspondence between the factors of these decompositions can be established for which corresponding factors are isomorphic. The problem of finding conditions under which any two direct decompositions of a given group into decomposable factors are isomorphic or, more generally, any two direct decompositions of a given group have isomorphic refinements is the object of numerous investigations. All these problems will be considered in Chapter XI and, for various classes of abelian groups, in Chapters VI-VIII.

§ 18. Free groups. Defining relations

It is the aim of this section to establish a method of giving a group without making use of individual properties of the elements of the set in which the group operation is defined. In order to achieve this we must first construct a special class of groups, the so-called *free groups*, which are in a certain sense universal for all existing groups whatsoever.

Let $\mathfrak{M}$ be a non-empty (finite or infinite) set of symbols $x_\alpha, x_\beta, x_\gamma, \ldots$.[1] We shall denote these symbols also by $x_\alpha^{+1}, x_\beta^{+1}, x_\gamma^{+1}, \ldots$ and we construct another set $x_\alpha^{-1}, x_\beta^{-1}, x_\gamma^{-1}, \ldots$ in one-to-one correspondence with the first set: An expression

$$w = x_{\alpha_1}^{\varepsilon_1} x_{\alpha_2}^{\varepsilon_2} \ldots x_{\alpha_n}^{\varepsilon_n} \qquad (\varepsilon_i = \pm 1, \quad i = 1, 2, \ldots, n), \tag{1}$$

that is, an ordered system of a finite number of symbols of the form x_α^{+1} and x_α^{-1} (where each symbol that enters into the expression (1) may occur

[1] To simplify the understanding of the following construction the reader may assume at first that the set $\mathfrak{M}$ consists of two symbols x_1 and x_2 only.

several times) is called a *word*. If in (1) no symbol x_α^{+1} stands next to its associated symbol x_α^{-1}, then w is called a *reduced word*.[k] Examples of reduced words are $x_\alpha x_\beta^{-1} x_\alpha x_\alpha x_\gamma$, and $x_\alpha x_\alpha x_\alpha x_\beta x_\alpha^{-1} x_\beta$, but not $x_\alpha x_\beta^{-1} x_\beta x_\alpha x_\gamma$.[1]

The number n is called the *length* of the reduced word w and is denoted by $l(w)$. For any set $\mathfrak{M}$ we can obviously construct words of arbitrary length. Reduced words of length 1 are precisely the symbols x_α and x_α^{-1}. We also count as a word the *empty word* w_0, which contains no symbols, and we put $l(w_0) = 0$.

The set of all reduced words that can be written by means of our collection of symbols is now made into a group by the following definition of the group operation: Suppose two reduced words are given,

$$w_1 = x_{\alpha_1}^{\varepsilon_1} x_{\alpha_2}^{\varepsilon_2} \dots x_{\alpha_n}^{\varepsilon_n} \qquad (\varepsilon_i = \pm 1, \quad i = 1, 2, \dots, n), \tag{2}$$

$$w_2 = x_{\beta_1}^{\delta_1} x_{\beta_2}^{\delta_2} \dots x_{\beta_m}^{\delta_m} \qquad (\delta_j = \pm 1, \quad j = 1, 2, \dots, m) \tag{3}$$

and suppose that

$$\alpha_{n-i+1} = \beta_i \quad \text{and} \quad \varepsilon_{n-i+1} + \delta_i = 0$$

for all i, $1 \leqq i \leqq k$ (where k is subject to the condition $0 \leqq k \leqq \min(n, m)$), but that either $\alpha_{n-k} \neq \beta_{k+1}$, or $\alpha_{n-k} = \beta_{k+1}$, $\varepsilon_{n-k} = \delta_{k+1}$. Then we set

$$w_1 w_2 = x_{\alpha_1}^{\varepsilon_1} x_{\alpha_2}^{\varepsilon_2} \dots x_{\alpha_{n-k}}^{\varepsilon_{n-k}} x_{\beta_{k+1}}^{\delta_{k+1}} x_{\beta_{k+2}}^{\delta_{k+2}} \dots x_{\beta_m}^{\delta_m}. \tag{4}$$

Put differently: in order to form the product $w_1 w_2$ we write w_2 immediately following w_1; if the resulting expression

$$x_{\alpha_1}^{\varepsilon_1} x_{\alpha_2}^{\varepsilon_2} \dots x_{\alpha_n}^{\varepsilon_n} x_{\beta_1}^{\delta_1} x_{\beta_2}^{\delta_2} \dots x_{\beta_m}^{\delta_m} \tag{5}$$

is a reduced word, that is, if the symbols x_{α_n} and x_{β_1} are distinct, or if they are equal and have the same exponents, then we have obtained the product $w_1 w_2$. Otherwise it is necessary first to carry out certain *cancellations*, that is, to delete successively pairs of symbols with opposite exponents standing

[1] The notation for words that we are using should not suggest that we have here any kind of "multiplication" of symbols. A word is merely an ordered system of symbols and we could equally well separate the symbols constituting the word by placing commas between them.

next to one another. Clearly it can happen that in performing these cancellations we delete all the symbols of one of the factors w_1, w_2, or of both.

The unit element for the multiplication of reduced words so defined is obviously the empty word w_0. The inverse of (2) is the word

$$w_1^{-1} = x_{\alpha_n}^{-\varepsilon_n} \dots x_{\alpha_2}^{-\varepsilon_2} x_{\alpha_1}^{-\varepsilon_1}.$$

In particular, the inverse of the symbol x_α is x_α^{-1}.

The proof of the *associative law* for the multiplication of words is a little laborious. Let w_1, w_2, and w_3 be non-empty reduced words.[1] We shall prove the equation

$$w_1 (w_2 w_3) = (w_1 w_2) w_3 \tag{6}$$

by induction on the length of the middle factor w_2.

Consider first the case $l(w_2) = 1$, that is, $w_2 = x_\alpha^\varepsilon$. If the last symbol of w_1 and the first symbol of w_3 are both different from $x_\alpha^{-\varepsilon}$, then no cancellations have to be performed and (6) holds. It also holds when only one of the two symbols in question is equal to $x_\alpha^{-\varepsilon}$, since there are then no cancellations in one of the products $w_1 w_2$, $w_2 w_3$. Finally, when both symbols are equal to $x_\alpha^{-\varepsilon}$, let

$$w_1 = x_{\beta_1}^{\delta_1} \dots x_{\beta_s}^{\delta_s} x_\alpha^{-\varepsilon}, \quad w_3 = x_\alpha^{-\varepsilon} x_{\gamma_1}^{\eta_1} \dots x_{\gamma_t}^{\eta_t}.$$

Then the expression

$$x_{\beta_1}^{\delta_1} \dots x_{\beta_s}^{\delta_s} x_\alpha^{-\varepsilon} x_{\gamma_1}^{\eta_1} \dots x_{\gamma_t}^{\eta_t}$$

is a reduced word, since there cannot be any cancellations in it, and this word is equal both to the left-hand and to the right-hand side of (6).

Now let $l(w_2) \geqq 2$. If

$$w_2 = x_{\alpha_1}^{\varepsilon_1} x_{\alpha_2}^{\varepsilon_2} \dots x_{\alpha_{n-1}}^{\varepsilon_{n-1}} x_{\alpha_n}^{\varepsilon_n},$$

we put

$$w_2' = x_{\alpha_1}^{\varepsilon_1} x_{\alpha_2}^{\varepsilon_2} \dots x_{\alpha_{n-1}}^{\varepsilon_{n-1}}.$$

Then w_2' is a reduced word, $l(w_2') < l(w_2)$, and $w_2 = w_2' \cdot x_{\alpha_n}^{\varepsilon_n}$. Equation

[1] The associative law is obvious for three factors one of which is w_0.

(6) in the case in question will now be verified by a repeated application of the same equation in cases when the length of the middle factor is less than n:

$$w_1(w_2w_3) = w_1[(w_2'x_{\alpha_n}^{\varepsilon_n})w_3] = w_1[w_2'(x_{\alpha_n}^{\varepsilon_n}w_3)] = (w_1w_2')(x_{\alpha_n}^{\varepsilon_n}w_3) =$$

$$= [(w_1w_2')x_{\alpha_n}^{\varepsilon_n}]w_3 = [w_1(w_2'x_{\alpha_n}^{\varepsilon_n})]w_3 = (w_1w_2)w_3.$$

Some of the parentheses that occur in the preceding equations may, of course, contain products that become reduced words only after certain cancellations. That, however, does not affect the argument.

We can now speak of the group of reduced words consisting of the symbols of the set $\mathfrak{M}$ and their inverses. This group is called a *free group*. Clearly, it is completely determined when the set $\mathfrak{M}$ is given and does not depend on any individual properties of the elements of this set. We define the *rank* of the free group constructed from $\mathfrak{M}$ as the cardinal number of $\mathfrak{M}$. Then one can prove by elementary set-theoretical considerations that a free group of finite rank is countable and that the cardinal number of a free group of infinite rank is equal to its rank.

A free group of rank 1 is obviously an infinite cyclic group. *Every free group whose rank exceeds* 1 *is non-commutative*: if $\alpha \neq \beta$, then $x_\alpha x_\beta$ and $x_\beta x_\alpha$ are distinct elements of the group. *All elements of a free group, except the unit element, have infinite order*: if in

$$w = x_{\alpha_1}^{\varepsilon_1}x_{\alpha_2}^{\varepsilon_2}\dots x_{\alpha_n}^{\varepsilon_n}$$

the symbols $x_{\alpha_1}^{\varepsilon_1}$ and $x_{\alpha_n}^{\varepsilon_n}$, $x_{\alpha_2}^{\varepsilon_2}$ and $x_{\alpha_{n-1}}^{\varepsilon_{n-1}}$, $\dots$, $x_{\alpha_k}^{\varepsilon_k}$ and $x_{\alpha_{n-k+1}}^{\varepsilon_{n-k+1}}$, are inverse in pairs, and if this is not the case for $x_{\alpha_{k+1}}^{\varepsilon_{k+1}}$ and $x_{\alpha_{n-k}}^{\varepsilon_{n-k}}$, then we put

$$\overline{w} = x_{\alpha_{k+1}}^{\varepsilon_{k+1}}x_{\alpha_{k+2}}^{\varepsilon_{k+2}}\dots x_{\alpha_{n-k}}^{\varepsilon_{n-k}}.$$

Such a k satisfying the inequality $0 \leqq k \leqq n/2$ must exist, since w is not the empty word. Now for $s > 0$ we have

$$w^s = x_{\alpha_1}^{\varepsilon_1}\dots x_{\alpha_k}^{\varepsilon_k}\overline{w}^s x_{\alpha_{n-k+1}}^{\varepsilon_{n-k+1}}\dots x_{\alpha_n}^{\varepsilon_n}.$$

The expression on the right-hand side of this equation does not admit any

cancellations, that is, is a non-empty reduced word. Hence it follows that $w^s \neq 1$.

Every word is equal to the product of the symbols that constitute it. The set $\mathfrak{M}$ is therefore a system of generators of the free group constructed by means of $\mathfrak{M}$. Such a system of generators of a free group will be called a *system of free generators*. In the sequel we shall retain the name "word" for the elements[1] of a free group and we shall write them as products of powers of free generators, for example, $x_\alpha^3 x_\beta^{-1} x_\alpha x_\beta^2$ instead of $x_\alpha x_\alpha x_\alpha x_\beta^{-1} x_\alpha x_\beta x_\beta$.

In Chapter IX the reader will become acquainted with many deep and important results in the theory of free groups. Here we shall prove just one theorem which makes completely manifest the significance of the free groups for the whole theory of groups.

Every group is isomorphic to a factor group of a free group. Let G be an arbitrary group and M a system of generators of G; we denote the elements of M by $a_\alpha, a_\beta, \ldots$. We now take a free group W with a free system of generators of the same cardinal number as M. Between the elements of M and the chosen system of free generators of W we set up a one-to-one correspondence and denote by x_α that element of W which corresponds to the element a_α of M. The mapping that carries the element x_α of W into its corresponding element a_α in G and, in general,

$$x_{\alpha_1}^{\varepsilon_1} x_{\alpha_2}^{\varepsilon_2} \ldots x_{\alpha_k}^{\varepsilon_k}, \quad \varepsilon_i = \pm 1, \quad i = 1, 2, \ldots, k, \tag{7}$$

into the element

$$a_{\alpha_1}^{\varepsilon_1} a_{\alpha_2}^{\varepsilon_2} \ldots a_{\alpha_k}^{\varepsilon_k} \tag{8}$$

of G, is obviously a homomorphic mapping of W onto G. By the homomorphism theorem (§ 10) we have

$$G \simeq W/H,$$

and the theorem is proved. Note that the normal subgroup H of W consists of precisely those words of the form (7) for which the product (8) is equal to the unit element of G.

From this proof of the theorem it follows that *every finitely generated group is a factor group of a free group of finite rank.* More explicitly, *every group with n generators is a factor group of a free group of rank n.*

It is clear that this representation of a group G as a factor group of a

free group is by no means unique, since it depends on the choice of the generating set M.

Let G be an arbitrary group and let it be represented as a factor group of a normal subgroup H of a free group W. If, as above, x_α, x_β, ... are free generators of W, we denote their images under the natural homomorphism by a_α, a_β, ..., and the set of all these elements of G (which need not, of course, be all distinct) by $\mathfrak{M}$. Let the word

$$x_{\alpha_1}^{\varepsilon_1} x_{\alpha_2}^{\varepsilon_2} \dots x_{\alpha_k}^{\varepsilon_k} \quad (\text{the } \varepsilon_i \text{ are integers})$$

be an arbitrary element of H. In G there corresponds to this the equation

$$a_{\alpha_1}^{\varepsilon_1} a_{\alpha_2}^{\varepsilon_2} \dots a_{\alpha_k}^{\varepsilon_k} = 1,$$

which will be called a *relation* between the elements of M in G.

We choose in H a subset $\mathfrak{N}$ such that H is the normal subgroup generated by $\mathfrak{N}$ in W. The system of relations that correspond to the words in $\mathfrak{N}$ is called a *system of defining relations of* G. All the relations that link the elements of M in G can be considered as *consequences* of the defining relations, since every element of H can be written as a product of powers of the elements of $\mathfrak{N}$ and their conjugates.

A group G is completely determined by its defining relations, since the set $\mathfrak{N}$ completely determines the normal subgroup H of the free group W and therefore the factor group W/H. Since we have shown above that every group is a factor group of a free group, we now see that *every group can be given by a system of defining relations connecting a certain set of symbols; two groups given by defining relations between certain systems of generators are isomorphic if a one-to-one correspondence between these systems can be set up for which the defining relations of one group go over into the defining relations of the other, and conversely.*

On the other hand, *if an arbitrary set of symbols M and an arbitrary set of relations* equating certain words in the symbols of M to the unit element are given, *then there is always a group for which these relations form a system of defining relations.* For the proof, it is sufficient to take the free group over the set M and take the normal subgroup generated by the left-hand sides of the given relations and then go over to its factor group.

VON DYCK'S THEOREM: *If a group G is given by a system of defining relations and if a group G' is given by these relations and some further relations in the same symbols, then G' is isomorphic to a factor group of G.*

For if we represent G and G' as factor groups of one and the same free group W,

$$G \simeq W/H, \qquad G' \simeq W/H',$$

then H is contained in H'.

This theorem is often useful if one wants to find defining relations of a group given in some other way.

Examples 1. A finite cyclic group of order n is given by a generating element a and the defining relation

$$a^n = 1.$$

2. The additive group of rational numbers R was represented in § 7 as the union of an ascending sequence of infinite cyclic groups. On the basis of that result we can now give R by the generators

$$a_1, a_2, a_3, \ldots, a_n, \ldots$$

and the defining relations

$$a_1 = a_2^2, \quad a_2 = a_3^3, \ldots, \quad a_n = a_{n+1}^{n+1}, \ldots.$$

3. The group of type p^∞ can be given by the generators

$$a_1, a_2, \ldots, a_n, \ldots$$

and the defining relations

$$a_1^p = 1, \quad a_{n+1}^p = a_n, \quad n = 1, 2, \ldots$$

4. The symmetric group S_3 of degree 3 is given by two generators a and b and the defining relations

$$a^3 = 1, \quad b^2 = 1, \quad abab = 1. \tag{9}$$

For, the elements

$$a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \qquad b = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \tag{9'}$$

generate the group S_3 and satisfy the relations (9), so that S_3 is (by von Dyck's Theorem) a factor group of the group given by the defining relations (9)—the group S_3 is defined in terms of the generators (9′) by the relations (9) and, possibly, others. But from the relations (9) it follows that $ba = a^2b$. Every product of powers of a and b in the group defined by the relations (9) can therefore be reduced by means of these relations to the form $a^\alpha b^\beta$, $\alpha = 0, 1, 2$, $\beta = 0, 1$; that is, the group with the defining relations (9) consists of not more than six elements and therefore coincides with S_3.

5. In § 9 we proved that the quaternion group Q has order 8 and is generated by two elements a and b, subject to the relations

$$a^4 = 1, \quad b^4 = 1, \quad a^2 = b^2, \quad aba = b. \tag{10}$$

In the course of the proof we also established that the group defined by the relations (10) has not more than eight elements. Hence it follows (again by von Dyck's Theorem) that (10) is a system of defining relations for the quaternion group Q. Note that two of the four relations (10) are not written in the form required above. The transition from this notation to the standard one, in the present case

$$a^2b^{-2} = 1, \quad abab^3 = 1,$$

is obvious.

We shall now make a few additional remarks about groups given by defining relations, but we refer the reader to the much deeper problems in Chapter X. We know that a free group is given by a system of free generators without any defining relations. Conversely, if in a group G a system of generators M can be chosen which are not linked by any relations[1] then every element of G is uniquely represented as a word in the elements of M, that is, the group G is isomorphic to the free group over M as system of free generators. In other words, *G is in this case a free group, and M is a system of free generators for G.*

In order that a group with generators $a_\alpha, a_\beta, \ldots$ be abelian it is sufficient to have among the defining relations the equations of the form

[1] The trivial "relations" of the form $aa^{-1} = 1$ do not satisfy the above definition of a relation and therefore do not count as relations.

$$[a_\alpha, a_\beta] = 1 \tag{11}$$

for all pairs of generators; the left-hand side is the commutator of a_α and a_β. For if any two generating elements are permutable, then it follows easily that any two products of powers of these elements are permutable. Examples 2 and 3 above show, however, that a group may turn out to be abelian although no equations of the form (11) occur among the defining relations.

Every group can be given by generators and defining relations in many distinct ways. Although defining relations represent a convenient method of giving a group "abstractly," that is, giving all the groups isomorphic to a group as well as the group itself, nevertheless in the overwhelming majority of cases we can say very little about a group given by relations. For example, if a group is given by a system of generators and a system of defining relations then we cannot, as a rule, say whether the group is finite or infinite, whether it is commutative or not, and so on. Moreover, the group may turn out to consist of the unit element only—this will happen, of course, if the normal subgroup that is generated by the left-hand sides of the defining relations of the group coincides with the whole free group—but even this cannot, in general, be established by considering the defining relations. Also the following extreme case is possible: our group may actually be a free group, but it may be given by a system of generators with non-trivial relations.

A *finite* group is sometimes given not by defining relations but by means of *Cayley's group table*. If a finite group G is of order n, then we number its elements beginning with the unit element:

$$1, \ a_2, \ a_3, \ \ldots, \ a_n. \tag{12}$$

We now construct a square table of n rows and n columns and label its rows downward and its columns from left to right with the symbols (12), and at the intersection of the row labelled a_i and the column labelled a_j we put the element that is equal to the product $a_i a_j$. Thus, if we take the symmetric group S_3 of degree 3, i.e. the group with the generators a and b and the relations $a^3 = 1, b^2 = 1, abab = 1$ (see above, Example 4), and introduce the notation:

$$a_2 = a, \quad a_3 = a^2, \quad a_4 = b, \quad a_5 = ab, \quad a_6 = a^2 b,$$

then the Cayley table is

	1	a_2	a_3	a_4	a_5	a_6
1	1	a_2	a_3	a_4	a_5	a_6
a_2	a_2	a_3	1	a_5	a_6	a_4
a_3	a_3	1	a_2	a_6	a_4	a_5
a_4	a_4	a_6	a_5	1	a_3	a_2
a_5	a_5	a_4	a_6	a_2	1	a_3
a_6	a_6	a_5	a_4	a_3	a_2	1

The non-cyclic group V of order 4, which is the direct product of two cyclic groups of order 2 (this group is given by the generators a and b and the defining relations

$$a^2 = 1,\ b^2 = 1,\ ab = ba),$$

can be given by the following Cayley table:

	1	a_2	a_3	a_4
1	1	a_2	a_3	a_4
a_2	a_2	1	a_4	a_3
a_3	a_3	a_4	1	a_2
a_4	a_4	a_3	a_2	1

A group has a Cayley table that is symmetrical with respect to the main diagonal if and only if it is abelian.

PART TWO

ABELIAN GROUPS

CHAPTER VI

FOUNDATIONS OF THE THEORY OF ABELIAN GROUPS

§ 19. The rank of an abelian group. Free abelian groups

The theory of abelian groups, one of the most important classes of groups, is well developed. In the present chapter we shall give an account of the fundamental concepts and facts of the theory of abelian groups, particularly of finitely generated abelian groups. These concepts and facts will be constantly used in the following two chapters which go more deeply into the theory.

We shall adopt the additive instead of the multiplicative notation in this chapter and in the sequel whenever we deal with problems specially related to abelian groups. The basic changes in terminology and notation that are consequences of this convention have been indicated at the end of § 3. In addition, we mention that instead of the unit subgroup we must now speak of the *null subgroup*, which will be denoted by the symbol 0. Instead of the product of subsets of a group we shall now speak of the *sum* of subsets; since all subgroups of an abelian group are normal and therefore permutable among each other, *the sum of two or any finite number of arbitrary subgroups of an abelian group is itself a subgroup* (see § 8). Finally, instead of the direct product (see § 17) we have the *direct sum* of abelian groups. This concept is quite fundamental for all abelian groups.

In accordance with the general terminology introduced in § 3, an abelian group is called *periodic* if the orders of all its elements are finite, *torsion-free* if all the elements, except the null element, have infinite order, and *mixed* if it contains elements both of finite and of infinite order.

If G is a mixed abelian group and F the set of all its elements of finite order, then F is obviously a subgroup of G. This uniquely defined subgroup is called the *maximal periodic* subgroup, or briefly, the *periodic part of* G. The factor group G/F is torsion-free. Thus *every mixed abelian group is an extension* (in the sense of § 10) *of a periodic group, namely its periodic part, by means of a torsion-free group.*

Among the periodic groups there are, in particular, the abelian groups in which the orders of all elements are powers of a fixed prime number p. These groups are called *primary with respect to* p or *p-primary.*

Every periodic abelian group can be decomposed in a unique way into the direct sum of primary groups with respect to distinct prime numbers.

For, the totality of all elements of a periodic abelian group G whose orders are powers of the prime number p is a subgroup of G, which we denote by G_p; it is characteristic, and even fully invariant, in G. All the subgroups G_p, for distinct p, form a direct sum in G, since the sum of all these subgroups with the exception of a particular G_q consists of elements whose orders are co-prime to q, so that the intersection of this sum with G_q is the null subgroup. On the other hand, every element of G is contained in the sum of all subgroups G_p; this follows from the fact, proved in § 17, that every finite cyclic group is decomposable into the direct sum of primary cyclic groups.

We now introduce the concept of the *rank of an abelian group* G. A finite system of elements $v_1, v_2, \ldots, v_k$ of a group G is called *linearly dependent* if there exist integers $\alpha_1, \alpha_2, \ldots, \alpha_k$, not all zero, for which

$$\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_k v_k = 0,$$

where on the right-hand side we have, of course, the null element of G. A system of elements that does not have this property is called *linearly independent*. We shall call an element u of G *linearly dependent* on the system of elements $\{u', u'', \ldots, u^{(l)}\}$, of G if an integral multiple αu of the element, with $\alpha \neq 0$, is contained in $\{u', u'', \ldots, u^{(l)}\}$, that is to say, if integers $\beta_1, \beta_2, \ldots, \beta_l$, exist for which

$$\alpha u = \beta_1 u' + \beta_2 u'' + \ldots + \beta_l u^{(l)}.$$

Obviously *a system of elements $v_1, v_2, \ldots, v_k$ is linearly dependent if and only if at least one of its elements v_i is linearly dependent on the remaining elements of the system.* The following properties of linear dependence are also obvious. Every system that contains elements of finite order is linearly dependent; in particular, the null element is linearly dependent. Every subsystem of a linearly independent system is itself linearly independent. Every element that occurs in a finite system of elements is linearly dependent on that system.

Two systems of elements of G, $u', u'', \ldots, u^{(k)}$ and $v', v'', \ldots, v^{(l)}$ are called *equivalent* if every element of the first system is linearly dependent on the second system, and vice versa. Every element u of G that is linearly dependent on one of these systems is also linearly dependent on the other. For if with $\alpha \neq 0$,

$$\alpha u \in \{u', u'', \ldots, u^{(k)}\},$$

and with $\beta_i \neq 0$, $i = 1, 2, \ldots, k$,

$$\beta_i u^{(i)} \in \{v', v'', \ldots, v^{(l)}\},$$

then $(\alpha\beta_1\beta_2 \ldots \beta_k)\, u \in \{v', v'', \ldots, v^{(l)}\}$. Hence the concept of equivalence of systems of elements is transitive.

STEINITZ' EXCHANGE THEOREM. *Suppose that in a group G two finite systems of elements are given*

$$u', u'', \ldots, u^{(k)} \tag{I}$$
$$v', v'', \ldots, v^{(l)} \tag{II}$$

the first of which is a linearly independent system each of whose elements is linearly dependent on the second system. Then $k \leqq l$, *and from* (II) k *elements can be omitted such that the remaining elements, together with the elements of* (I), *form a system equivalent to* (II).

Proof. The theorem is vacuously true for $k = 0$. We assume that it is proved for $k - 1$.

The subsystem $u', u'', \ldots, u^{(k-1)}$ of (I) is itself linearly independent and its elements are linearly dependent on (II). We therefore obtain a system

$$u', u'', \ldots, u^{(k-1)}, v^{(k)}, \ldots, v^{(l)}, \tag{III}$$

equivalent to (II) possibly after a change of the numbering of the elements in (II). Now $u^{(k)}$, being linearly dependent on (II), must also be linearly dependent on (III), that is, there exist coefficients $\alpha, \beta_1, \ldots, \beta_l$ for which $\alpha \neq 0$ and

$$\alpha u^{(k)} = \beta_1 u' + \beta_2 u'' + \ldots + \beta_{k-1} u^{(k-1)} + \beta_k v^{(k)} + \ldots + \beta_l v^{(l)}.$$

It follows that $l \geqq k$ and that at least one of the coefficients $\beta_k, \ldots, \beta_l$ is different from zero, since otherwise $u^{(k)}$ would turn out to be linearly dependent on the system $u', u'', \ldots, u^{(k-1)}$. Let $\beta_k \neq 0$. Then

$$\beta_k v^{(k)} = (-\beta_1) u' + \ldots + (-\beta_{k-1}) u^{(k-1)} + \alpha u^{(k)} + (-\beta_{k+1}) v^{(k+1)} + \ldots + (-\beta_l) v^{(l)},$$

that is, $v^{(k)}$ is linearly dependent on the system

$$u', u'', \ldots, u^{(k-1)}, u^{(k)}, v^{(k+1)}, \ldots, v^{(l)}. \tag{IV}$$

Since (III) and (IV) are equivalent systems, (II) and (IV) are also equivalent. This completes the proof.

From the exchange theorem it follows that *two linearly independent equivalent systems of elements of a group G consist of an equal number of elements.*

The concept of linear dependence can be extended to the case of infinite systems of elements in the following way: an infinite system of elements of an abelian group G is called *linearly dependent* if it contains at least one finite linearly dependent subsystem, and *linearly independent* if all its finite subsystems are linearly independent. Correspondingly, an element is *linearly dependent* on an infinite system of elements if it is linearly dependent in the previous sense on a finite subsystem. Since the union of an ascending sequence of linearly independent systems of a group G is itself linearly independent, *every non-periodic group has maximal linearly independent systems* and *every linearly independent system can be embedded in one that is maximal.* If a group G is periodic, then it contains no linearly independent systems.

If a group G has finite maximal linearly independent systems, then all these systems are equivalent and consist, as we have shown above, of the same number of elements. This number is called the *rank* of the abelian group G; and G itself is called a *group of finite rank.* It is convenient to include among the groups of finite rank all periodic abelian groups, assigning them the rank zero. A group that does not have finite rank is called a *group of infinite rank.* In this case the rank of the group is the cardinal number of a maximal linearly independent system of its elements; it is equal to the cardinal number of the factor group of the given group with respect to its periodic part and is therefore an invariant of the group.

Every subgroup A and every factor group G/A of an abelian group G of finite rank is itself of finite rank, and the sum of the two ranks is equal to the rank of G.

The first part follows from the fact that every linearly independent system of elements of A is also linearly independent in G, the second from the fact that by choosing in G/A any linearly independent system of elements (i.e. cosets of A) and one representative from each of these cosets we obtain a linearly independent system of elements of G.

For the proof of the third part, we select a maximal linearly independent system of elements of A

$$a_1, a_2, \ldots, a_k, \quad k \geqq 0, \tag{1}$$

and a maximal linearly independent system of cosets of G/A

$$b_1+A, \quad b_2+A, \ldots, \quad b_l+A, \qquad l \geqq 0, \tag{2}$$

where

$$b_1, \ b_2, \ \ldots, \ b_l$$

is an arbitrary system of representatives of these cosets. Then

$$a_1, \ a_2, \ \ldots, \ a_k, \ b_1, \ b_2, \ \ldots, \ b_l \tag{3}$$

is a linearly independent system of elements of G. For from an equation

$$\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_k a_k + \beta_1 b_1 + \beta_2 b_2 + \ldots + \beta_l b_l = 0 \tag{4}$$

we obtain, by going over to the factor group of A, the equation

$$\beta_1 (b_1 + A) + \beta_2 (b_2 + A) + \ldots + \beta_l (b_l + A) = 0,$$

but since (2) is a linearly independent system, we have

$$\beta_1 = \beta_2 = \ldots = \beta_l = 0.$$

The equation (4) now reduces to

$$\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_k a_k = 0,$$

and from the linear independence of (1) it follows that

$$\alpha_1 = \alpha_2 = \ldots = \alpha_k = 0.$$

It remains to prove that (3) is a maximal linearly independent system of G. If g is an arbitrary element of G, then the coset $g + A$ is linearly dependent on (2)

$$\alpha (g + A) = \gamma_1 (b_1 + A) + \gamma_2 (b_2 + A) + \ldots + \gamma_l (b_l + A);$$

hence

$$\alpha g = a + \gamma_1 b_1 + \gamma_2 b_2 + \ldots + \gamma_l b_l,$$

where a is an element of A and $\alpha \neq 0$. However, a is linearly dependent on (1)

$$\beta a = \delta_1 a_1 + \delta_2 a_2 + \ldots + \delta_k a_k,$$

where $\beta \neq 0$, and therefore

$$(\alpha\beta) g = \delta_1 a_1 + \delta_2 a_2 + \ldots + \delta_k a_k + (\beta\gamma_1) b_1 + (\beta\gamma_2) b_2 + \ldots + (\beta\gamma_l) b_l,$$

which is what we had to prove.

From this theorem it follows that *the rank of a mixed group is equal to the rank of the factor group of its periodic part* and also that *the direct sum of a finite number of groups of finite rank is itself of finite rank and the rank is equal to the sum of the ranks of the direct summands.*

We shall now study abelian groups of a special type which play a very significant rôle in the general theory.

A *free abelian group* is a direct sum of a finite or infinite number of infinite cyclic groups.[1] If

$$U = \sum_{\nu} \{u_\nu\}$$

is a decomposition of a free abelian group U into the direct sum of infinite cyclic groups, then the totality of generators u_ν of all these cyclic direct summands (one from each summand) is called a *basis* of U. Every element of U can be written in one and only one way as a sum, with integer coefficients, of a finite number of elements of the basis.

A free abelian group U has, in general, many distinct decompositions into a direct sum of infinite cyclic groups and therefore has many distinct bases. Thus, if the elements $u_1, u_2, \ldots$ occur in a basis of U, we can change the basis by replacing the element u_1 by $u_1 + \alpha u_2$, where α is an arbitrary integer. We shall in the following section frequently carry out without further explanation such a transformation of a basis of U.

A free abelian group is torsion-free, and every basis of such a group is one of its maximal linearly independent systems. It follows from results previously obtained that *if a free group U has finite rank n, then all its bases consist of n elements,* that is to say, every decomposition of U into the direct sum of infinite cyclic groups consists of n summands. If the rank of a group U is infinite, then the cardinal number of any of its bases obviously coincides with the cardinal number of the group itself.

Note that by no means every maximal linearly independent system of a free abelian group is a basis. For example, a free group of rank 1, that is, an infinite cyclic group $\{u\}$, has two bases, u and $-u$, but every element of the group except the null element is a maximal linearly independent system in the group.

---

[1] It is often convenient to include among the free abelian groups the null group, generated by an empty set of infinite cyclic groups. Without this convention many theorems require a cumbersome special consideration of the exceptional null subgroup. [*Trans.*]

Free abelian groups play the same rôle in the theory of abelian groups as free groups do in the general theory of groups:

Every abelian group G is isomorphic to a factor group of a free abelian group, and an abelian group with n generators is isomorphic to a factor group of a free abelian group of rank n.

For the proof, we choose in G a system of generators $M = (a_\alpha)$, where α ranges over an index set, and we take a free abelian group U with a basis consisting of elements u_α that stand in one-to-one correspondence with the elements a_α of M. The mapping

$$k_1 u_{\alpha_1} + k_2 u_{\alpha_2} + \ldots + k_n u_{\alpha_n} \to k_1 a_{\alpha_1} + k_2 a_{\alpha_2} + \ldots + k_n a_{\alpha_n}$$

is obviously a homomorphic mapping of U onto G. By the homomorphism theorem (§ 10) G is therefore isomorphic to the factor group of U with respect to the subgroup V consisting of those elements of U that this homomorphism maps onto the null element of G,

$$G \simeq U/V.$$

Every subgroup of a free abelian group is itself free.[1]

Let V be a subgroup of the free abelian group U. We assume that we have well-ordered a basis of U,

$$a_1, a_2, \ldots, a_\alpha, \ldots, \quad \alpha < \tau.$$

Every element x of U, $x \neq 0$, can be written uniquely in the form

$$x = k_1 a_{\alpha_1} + k_2 a_{\alpha_2} + \ldots + k_n a_{\alpha_n},$$

where $\alpha_1 < \alpha_2 < \ldots < \alpha_n$ and all the k_i are different from zero. We shall call α_n the *last index* and k_n the *last coefficient* of x. We now consider the elements of V whose last index is smallest among the last indices of all the elements of V, and from these elements we choose an element b_1 with the smallest positive last coefficient. It is easy to see that every element v of V that has the same last index as b_1 is contained in the cyclic subgroup $\{b_1\}$. For if we denote the last coefficient of b_1 by k, and that of v by l, and if $l = kq + r$, $0 \leqq r < k$, then the element $v - qb_1$, which is contained in V, has for $r > 0$ the same last index as b_1 but a smaller last coefficient and

[1] The special case of this theorem that refers to free abelian groups of finite rank will be proved independently in the following section.

has for $r = 0$ a smaller last index. In both cases, if $v - qb_1 \neq 0$ we obtain a contradiction to the choice of b_1; therefore $v = qb_1$.

We now assume that we have already chosen elements b_β in V for all β less than γ such that these elements are linearly independent, in other words, that the subgroup V' they generate is the direct sum of the cyclic groups $\{b_\beta\}$ and that every element of V whose last index does not exceed the last index of one of the elements b_β is contained in V'. Among the elements of V that lie outside V' we now choose those with the smallest last index and select from them an element b_γ with the smallest positive last coefficient. Every multiple of b_γ has the same last index as b_γ so that $V' \cap \{b_\gamma\} = 0$ and hence

$$\{V', b_\gamma\} = V' + \{b_\gamma\}.$$

Moreover, if an element w of V has the same last index as b_γ and if the last coefficients of b_γ and w are k_γ and k, respectively, then (by definition of b_γ) k must be divisible by k_γ, $k = k_\gamma k'$. Therefore the last index of $w - k'b_\gamma$ is smaller than that of b_γ, and therefore $w - k'b_\gamma \in V'$ and $w \in V' + \{b_\gamma\}$. This process of choosing elements b_β may be continued as long as not all the elements of V are exhausted. V is therefore a free abelian group with the basis $b_1, b_2, \ldots, b_\beta, \ldots$, where β is less than a certain ordinal number σ.

Finally, we prove the following theorem:

If the factor group of an abelian group G with respect to a subgroup B is a free group, then B is a direct summand of G.

For let

$$G/B = \sum_\alpha \{\bar{a}_\alpha\}$$

be a decomposition of G/B into the direct sum of infinite cyclic groups. From each coset $\bar{a}_\alpha$ we choose a representative a_α. The subgroup A of G generated by all the elements a_α is a direct sum of cyclic subgroups $\{a_\alpha\}$, and $A \cap B = 0$. Moreover, every coset of B in G contains some element of A, so that

$$G = \{B, A\} = B + A.$$

Note that among the subgroups of an abelian group G whose factor groups are free there need not be a minimal one and therefore G need not be decomposable into the direct sum of a free group and a group without free factor groups; as an example we mention the unrestricted direct sum of a countable number of infinite cyclic groups (see § 17).

§ 20. Finitely generated abelian groups

Finitely generated abelian groups can be treated exhaustively. This class of groups is of particular interest in view of its exceptionally important rôle in various applications; finitely generated abelian groups are, for example, a fundamental tool in combinatorial topology.

We know from the preceding section that every abelian group with n generators is a factor group of a free abelian group of rank n, which we shall denote by U_n throughout the present section. We know, further, that every subgroup of U_n is itself free and that its rank does not exceed n. Without making reference to this latter result we shall now prove the following more general *theorem on the subgroups of* U_n; the whole theory of finitely generated abelian groups will be based essentially on this theorem.

Every subgroup V *of* U_n *is itself a free group and its rank* k *does not exceed* n. *Moreover, we can choose bases* $\bar{u}_1, \bar{u}_2, \ldots, \bar{u}_n$ *in* U_n, *and* $v_1, v_2, \ldots, v_k$ *in* V *for which*

$$v_i = e_i \bar{u}_i, \quad i = 1, 2, \ldots, k,$$

where $e_1, e_2, \ldots, e_k$ *are positive integers and* e_{i+1} *is divisible by*

$$e_i, \; i = 1, 2, \ldots, k-1.$$

Proof. For $n = 1$ the truth of the theorem follows immediately from the theorem on the subgroups of cyclic groups (§ 6). Let us suppose the theorem proved for U_{n-1}. If a subgroup V, other than the null group, is given in U_n, then to every choice of a basis for U_n there corresponds uniquely a certain positive integer, namely the smallest positive integer that occurs as a coefficient in those linear forms with respect to this basis that constitute the subgroup V. This minimal positive coefficient may change, in general, with a change of basis of U_n. We now select a basis

$$u_1, u_2, \ldots, u_n \tag{1}$$

of U_n for which this minimal coefficient assumes its smallest possible value. Let e_1 ($e_1 \geqq 1$) be the minimal positive coefficient with respect to this basis and let

$$v_1 = e_1 u_1 + \alpha_2 u_2 + \ldots + \alpha_n u_n$$

be one of the elements of V for which the expression in terms of (1) contains e_1 as one of the coefficients.[1]

[1] The assumption that e_1 is the coefficient of u_1 is legitimate since we do not regard the basis of U_n as ordered.

We divide each coefficient $\alpha_2, \ldots, \alpha_n$ by ε_1:

$$\alpha_i = \varepsilon_1 q_i + r_i, \quad 0 \leqq r_i < \varepsilon_1, \quad i = 2, 3, \ldots, n,$$

and transform the basis (1) of U_n by replacing u_1 by

$$\bar{u}_1 = u_1 + q_2 u_2 + \ldots + q_n u_n.$$

In the new basis

$$\bar{u}_1, u_2, \ldots, u_n$$

v_1 is expressed in the following way:

$$v_1 = \varepsilon_1 \bar{u}_1 + r_2 u_2 + \ldots + r_n u_n.$$

Since all the $r_i, i = 2, \ldots, n$, are non-negative and less than ε_1, it follows from the choice of ε_1 that

$$r_2 = r_3 = \ldots = r_n = 0,$$

so that $v_1 = \varepsilon_1 \bar{u}_1$.

We now collect all those elements of V for which the coefficient of u_1 in their representation in the new basis is equal to zero. These elements form a subgroup V' of V whose intersection with the cyclic subgroup generated by v_1 is 0. We shall show that the sum of $\{v_1\}$ and V' is V.

Let

$$v = \beta_1 \bar{u}_1 + \beta_2 u_2 + \ldots + \beta_n u_n$$

be an arbitrary element of V. If $\beta_1 = \varepsilon_1 q + r$, $0 \leqq r < \varepsilon_1$, then V contains the element

$$v' = v - q v_1 = r \bar{u}_1 + \beta_2 u_2 + \ldots + \beta_n u_n$$

which has as coefficient of $\bar{u}_1$ a number less than ε_1; hence by the definition of ε_1 we have $r = 0$. Therefore v' is contained in V' and

$$v = q v_1 + v'$$

is in the sum of the subgroups $\{v_1\}$ and V'.

If $V' = 0$, then it follows that $V = \{v_1\}$ and the theorem is proved. But if $V' \neq 0$, then we obtain a decomposition of V into the direct sum

$$V = \{v_1\} + V'.$$

V' is contained in the subgroup $U' = \{u_2, \ldots, u_n\}$, which is a free

group of rank $n-1$ and is therefore, by the induction hypothesis, free. Furthermore, there exist bases $\bar{u}_2, \ldots, \bar{u}_n$ of U' and $v_2, \ldots, v_k$ of V' for which $k-1 \leqq n-1$ and $v_i = \varepsilon_i u_i$, where $\varepsilon_i > 0$ and ε_{i+1} is divisible by ε_i, $i = 1, 2, \ldots, k-1$.

We now know that V is a free group of rank k, $k \leqq n$.[1] In order to prove that the bases

$$\bar{u}_1, \bar{u}_2, \ldots, \bar{u}_n \tag{2}$$

of U_n and

$$v_1, v_2, \ldots, v_k \tag{3}$$

of V satisfy all requirements of the theorem it only remains to show that ε_2 is divisible by ε_1. Let $\varepsilon_2 = \varepsilon_1 q_0 + r_0$, $0 \leqq r_0 < \varepsilon_1$. We transform the basis (2) of U_n, replacing the element $\bar{u}_1$ by

$$\bar{u}_1' = \bar{u}_1 - q_0 \bar{u}_2.$$

With respect to this basis the element $v_2 - v_1$ of V is expressed in the form

$$v_2 - v_1 = (-\varepsilon_1)\bar{u}_1' + r_0 \bar{u}_2,$$

from which it follows, again by the choice of ε_1, that $r_0 = 0$.

The theorem on the subgroups of U_n is now completely proved. We shall use it to obtain the following *fundamental theorem.*

Every finitely generated abelian group is the direct sum of cyclic groups.[2]

Proof. Let G be a finitely generated abelian group. We know that G is isomorphic to a factor group of a free group U_n with respect to a subgroup V. In accordance with the above theorem we choose bases $u_1, u_2, \ldots, u_n$ in U_n and $v_1, v_2, \ldots, v_k$ in V such that we have $v_i = \varepsilon_i u_i$, for $i = 1, 2, \ldots, k$, where $\varepsilon_i > 0$ and ε_{i+1} is divisible by ε_i. Owing to this choice of a basis, the element

$$u = \alpha_1 u_1 + \alpha_2 u_2 + \ldots + \alpha_n u_n \tag{4}$$

of U_n is contained in V if and only if the coefficients α_i are divisible by ε_i, $i = 1, 2, \ldots, k$, and the coefficients α_j are zero, $j = k+1, \ldots, n$. For if the α's satisfy these conditions, then u can be expressed in terms of the basis $v_1, v_2, \ldots, v_k$. Conversely, if

---

[1] Note that the rank of a proper subgroup of a free group may be equal to the rank of the group.

[2] This direct sum may, of course, consist of a single summand, if the group is itself cyclic.

$$u = \beta_1 v_1 + \beta_2 v_2 + \ldots + \beta_k v_k,$$

then we need only replace each v_i by $\varepsilon_i u_i$ and equate with (4), since the expression of an element of U_n in terms of a basis is unique. The element $u_i + V$ of the factor group U_n/V is of order ε_i for $i \leqq k$, and of infinite order for $i > k$. The cyclic subgroups generated by these elements have the whole factor group as their sum, in fact as their *direct* sum, because every element of U_n/V is *uniquely* expressible as a sum of elements of the cyclic subgroups $\{u_i + V\}$. Of course, if the first few numbers $\varepsilon_1, \varepsilon_2, \ldots$ are equal to 1, then the corresponding direct summands $\{u_1 + V\}, \{u_2 + V\}, \ldots$ may be excluded. Since G is isomorphic to U_n/V, the theorem is proved not only for U_n/V but also for G.

From this theorem it follows, in particular, that *every non-cyclic finitely generated abelian group is decomposable.* From § 17 we know that an infinite cyclic group and also a primary cyclic group (that is, a cyclic group of order p^m, where p is a prime number), is indecomposable; on the other hand, a non-primary finite cyclic group is decomposable into the direct sum of primary cyclic groups. This last result enables us to assert the following stronger form of the fundamental theorem:

Every finitely generated abelian group G is the direct sum of a finite number of indecomposable cyclic subgroups, some finite and primary, some infinite.

The generating elements (one from each summand) of the cyclic direct summands in the decomposition of G into the direct sum of indecomposable subgroups form a so-called *basis* of G. In the case of a free group this concept of a basis coincides with that defined in the preceding section.

From the fundamental theorem it follows, in particular, that *every finite abelian group is decomposable into the direct sum of finite cyclic groups, which can even be taken as primary.* This theorem marks the very beginning of the theory of abelian groups. It was partially known to Gauss, the first complete proof being due to Frobenius and Stickelberger [1]. A large number of other proofs have been given since then; there are also several distinct proofs of the fundamental theorem for infinite abelian groups with a finite number of generators.

We therefore obtain all finitely generated abelian groups if we form all the possible direct sums of finite systems of infinite, or finite and primary, cyclic groups. But are all the abelian groups constructed in this way actually distinct? The answer to this question is given in the affirmative by the following theorem.

If a finitely generated abelian group is decomposed into the direct sum of indecomposable summands, then the number of infinite cyclic summands and the totality of the orders of the primary cyclic summands is independent of the decomposition, that is, of the choice of a basis.

In other words, *any two decompositions of a finitely generated abelian group G into the direct sum of indecomposable cyclic groups are isomorphic.*

We shall combine the proof of this theorem with the proof of a theorem on the subgroups of G that will be formulated below. First we prove the following statement:

Every subgroup H of a finitely generated abelian group G is itself finitely generated.

For G is isomorphic to the factor group of a free abelian group U with respect to a subgroup V. The subgroup H corresponds in U to a subgroup U' containing V,

$$H \simeq U'/V.$$

But U' is finitely generated, as we have proved above. Hence the same is true for H.

The subgroup theorem for a finitely generated abelian group G is the following:

Suppose a decomposition of G into the direct sum of indecomposable cyclic groups contains r infinite cyclic summands $r \geqq 0$; *suppose, further, that the number of p-primary cyclic summands for a given prime number p is* k_p, *where* $k_p \geqq 0$, *and that the orders of these summands are*

$$p^{\alpha_{p1}},\ p^{\alpha_{p2}},\ \ldots,\ p^{\alpha_{pk_p}},$$

where

$$\alpha_{p1} \geqq \alpha_{p2} \geqq \cdots \geqq \alpha_{pk_p}.$$

Suppose now that an arbitrary decomposition of a subgroup H of G into the direct sum of indecomposable cyclic groups contains s infinite cyclic summands and, for each prime number p, l_p *cyclic p-primary summands and that the orders of the summands are*

$$p^{\beta_{p1}},\ p^{\beta_{p2}},\ \ldots,\ p^{\beta_{pl_p}},$$

where

$$\beta_{p1} \geqq \beta_{p2} \geqq \cdots \geqq \beta_{pl_p}. \tag{5}$$

Then

$$s \leqq r, \tag{6}$$

and for each prime number p

$$l_p \leqq k_p, \tag{7}$$

$$\beta_{pi} \leqq \alpha_{pi}, \qquad i = 1, 2, \ldots, l_p. \tag{8}$$

Proof. This theorem will now be proved together with the isomorphism theorem for the decompositions of G. First of all, the elements of infinite order that occur in an arbitrary basis of G form a maximal linearly independent system of G, as one can easily see. The number of such elements is therefore equal to the rank of the group; that is, it does not depend on the choice of a basis. This also proves relation (6), since the rank of the subgroup H cannot exceed the rank of G.

We know, moreover, that the periodic part A of G is the direct sum of p-primary subgroups for distinct prime numbers,

$$A = \sum_p A_p,$$

while the periodic part of H is the direct sum of its intersections B_p with the subgroups A_p, $B_p = H \cap A_p$. But it is easy to verify that A_p is generated by those elements of an arbitrary basis of G whose orders are powers of p. Thus the proof of both theorems is reduced to the case of a finite primary group A_p and a subgroup B_p.

We first conclude the proof of the subgroup theorem. The subgroup consisting of the elements of order p in A_p is a direct sum of k_p cyclic summands of order p, so that its order is p^{k_p}. The corresponding subgroup of B_p is of order p^{l_p}. This proves that $l_p \leqq k_p$. Suppose now that

$$\beta_{p1} \leqq \alpha_{p1}, \ldots, \beta_{p,\,j-1} \leqq \alpha_{p,\,j-1}, \text{ but } \beta_{pj} > \alpha_{pj}. \tag{9}$$

The set C of all elements of A_p that are divisible by $p^{\alpha_{pj}}$, that is, of those elements c for which the equation

$$p^{\alpha_{pj}} x = c$$

has a solution in A_p, is a subgroup of A_p. If $a_1, a_2, \ldots, a_{k_p}$ is the given basis of A_p and if the order of a_i is $p^{\alpha_{pi}}$, $i = 1, 2, \ldots, k_p$, then it is easy to verify that C is the direct sum of the cyclic subgroups generated by

$$p^{\alpha_{pj}} a_1, \; p^{\alpha_{pj}} a_2, \; \ldots, \; p^{\alpha_{pj}} a_{j-1},$$

so that C has a basis consisting of $j - 1$ elements. On the other hand, by (9) and (5), the subgroup C' of B_p consisting of the elements that are

divisible by $p^{\alpha_{pj}}$ in B_p has a basis containing not fewer than j elements. However, C' is a subgroup of C and we have already proved (7); that is, we have proved that the number of elements in the basis of a subgroup of a finite primary abelian group is not greater than the number of elements in the basis of the group itself. The contradiction we have thus obtained concludes the proof of the subgroup theorem.

The isomorphism theorem for the direct decompositions of A_p follows immediately from the subgroup theorem; we put $B_p = A_p$ and take into account the fact that for two given bases of A_p we have not only the inequalities (7) and (8) but, by symmetry, also the opposite inequalities, so that in fact we have

$$l_p = k_p,$$
$$\beta_{pi} = \alpha_{pi}, \qquad i = 1, 2, \ldots, l_p.$$

The number of infinite cyclic summands—the rank of the group—and the orders of the primary cyclic summands in any decomposition of a finitely generated abelian group are called the *invariants* of the group. This is a *complete system of invariants*, since any two groups for which these invariants coincide are isomorphic. The sequence of integers $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_k$, each divisible by the preceding one, which were the orders of the cyclic summands in the decomposition we obtained for the proof of the fundamental theorem is also invariant, that is, independent of the choice of the direct decomposition of the group; the reader will have no difficulty in proving this with the help of the complete system of invariants. These numbers are sometimes called the *torsion coefficients* of G; the orders of the primary cyclic summands will be called for brevity the *finite invariants* of the group.

Through the subgroup theorem we have obtained a complete picture of the invariants of the subgroups of a finitely generated abelian group. But that does not exhaust all the possible questions that can be asked about these subgroups. For example, many mathematicians have investigated the total number of subgroups of a finite abelian group or the number of subgroups of one special form or another. In this direction there is the following problem: If a finite primary abelian group is given by its invariants and if a basis is chosen in the group, is it then possible to enumerate all the subgroups of the group by assigning to each a certain "canonical" basis? Such a basis ought to be uniquely determined by the choice of the basis of the group and it ought to be "best possible" in a certain sense. A solution of this problem was given by Birkhoff [3].[n]

§ 21. The ring of endomorphisms of an abelian group

For the endomorphisms of an abelian group G we can introduce, apart from the multiplication studied in § 12, an operation of addition. The *sum* of two endomorphisms χ and η is defined as the mapping that carries every element a of G into

$$a\chi + a\eta,$$

$$a(\chi + \eta) = a\chi + a\eta.$$

This mapping is also an endomorphism of G, since[1]

$$(a+b)(\chi+\eta) = (a+b)\chi + (a+b)\eta = (a\chi + b\chi) + \\ + (a\eta + b\eta) = a(\chi+\eta) + b(\chi+\eta).$$

The addition of endomorphisms is commutative and associative. The null endomorphism plays the rôle of the zero. If χ is an endomorphism of G, then the mapping $-\chi$ that carries every element a of G into $-a\chi$,

$$a(-\chi) = -a\chi,$$

is also an endomorphism, for

$$(a+b)(-\chi) = -(a+b)\chi = -(a\chi + b\chi) = a(-\chi) + b(-\chi),$$

The sum of the endomorphisms χ and $-\chi$ is the null endomorphism. We can, therefore, introduce the *subtraction* of endomorphisms:

$$\chi - \eta = \chi + (-\eta).$$

Sums and products of endomorphisms of an abelian group are linked by the distributive laws:

$$(\chi_1 + \chi_2)\eta = \chi_1\eta + \chi_2\eta, \tag{1}$$

$$\eta(\chi_1 + \chi_2) = \eta\chi_1 + \eta\chi_2. \tag{2}$$

For we have for an arbitrary $a \in G$

$$a[(\chi_1 + \chi_2)\eta] = [a(\chi_1 + \chi_2)]\eta = (a\chi_1 + a\chi_2)\eta = \\ = (a\chi_1)\eta + (a\chi_2)\eta = a(\chi_1\eta) + a(\chi_2\eta) = a(\chi_1\eta + \chi_2\eta),$$

[1] Here we use, in an essential way, the commutative law of the group operation in G. In the case of a non-abelian group G the sum of two endomorphisms χ and η is an endomorphism if and only if $G\chi$ and $G\eta$—the images of G under these endomorphisms—are element-wise permutable. Such endomorphisms χ and η are then called *summable*.

which proves (1). The proof of (2) is just as simple.

All these results, together with those of § 12 on the multiplication of endomorphisms, are combined in the following theorem.

The set of all endomorphisms of an abelian group is a ring with respect to the operations of addition and multiplication of endomorphisms.

The endomorphisms of a non-commutative group do not form a ring, since it is not possible to perform additions and subtractions without restriction. Properties of the systems of endomorphisms of a non-commutative group are studied in papers by Fitting [1, 4].

We shall now consider some examples. First of all, let us find the *ring of endomorphisms of an infinite cyclic group*. Let a be a generator of the group. An endomorphism carries a into an element na (where n is an integer) and is completely determined when n is given. Thus there exists a one-to-one correspondence between the endomorphisms of an infinite cyclic group and the integers. If

$$a\chi = na, \quad a\eta = ma$$

then

$$a(\chi\eta) = (na)\eta = (nm)a$$
$$a(\chi + \eta) = na + ma = (n + m)a.$$

So we see that *the ring of endomorphisms of an infinite cyclic group is isomorphic to I, the ring of integers.* By the same method one shows that *the ring of endomorphisms of a finite cyclic group of order n is isomorphic to I_n, the ring of residue classes of I* (mod n).

Now let us find the ring of endomorphisms of R, the additive group of rational numbers. Every endomorphism of R is completely determined by the image of the number 1: if $1 \cdot \chi = r$ and if $\left(\frac{1}{n}\right)\chi = r'$, then $nr' = \left(n \cdot \frac{1}{n}\right)\chi = r$; hence $r' = \frac{r}{n}$, and therefore

$$\left(\frac{m}{n}\right)\chi = \frac{m}{n}r. \tag{3}$$

Conversely, by choosing an arbitrary rational number r and defining the mapping χ of R by the formula (3) we obtain an endomorphism of R. In this way we establish a one-to-one correspondence between the endomorphisms of R and the rational numbers; but from

$$1 \cdot \chi = r, \quad 1 \cdot \eta = s$$

it follows that

$$1 \cdot (\chi\eta) = r\eta = rs,$$
$$1 \cdot (\chi + \eta) = r + s.$$

Hence *the ring of endomorphisms of R is isomorphic to the field of rational numbers.* Thus every endomorphism of R, except the null endomorphism, has an inverse and is therefore an automorphism.

Finally, let us find the *ring of endomorphisms of a group of type p^∞.* This group is given by generators

$$a_1, a_2, \ldots, a_n, \ldots \tag{4}$$

and the relations

$$pa_1 = 0, \quad pa_{n+1} = a_n, \quad n = 1, 2, \ldots . \tag{5}$$

An endomorphism χ of this group is completely determined by giving the images of all the elements (4); and since all the elements of our group whose order does not exceed p^n lie in the subgroup $\{a_n\}$, we have

$$a_n\chi = k_n a_n, \quad n = 1, 2, \ldots, \tag{6}$$

where

$$0 \leqq k_n < p^n; \tag{7}$$

furthermore, since the relations (5) must hold for the images of the elements (4), we have

$$p(a_{n+1}\chi) = a_n\chi,$$

so that

$$p(k_{n+1}a_{n+1}) = k_{n+1}a_n = k_n a_n$$

Therefore

$$k_{n+1} \equiv k_n \pmod{p^n}, \quad n = 1, 2, \ldots . \tag{8}$$

Thus, to every endomorphism χ of a group of type p^∞ there corresponds a sequence of natural numbers

$$(k_1, k_2, \ldots, k_n, \ldots) \tag{9}$$

subject to the conditions (7) and (8). To distinct endomorphisms there correspond distinct sequences, since at least one a_n has different images under the endomorphisms. On the other hand, every sequence (9), subject to the conditions (7) and (8), defines an endomorphism, namely that given by the equations (6).

Suppose now that besides the endomorphism χ defined by the sequence (9) we have another endomorphism η of the group of type p^∞ corresponding to the sequence

$$(l_1, l_2, \ldots, l_n, \ldots). \tag{10}$$

Then

$$a_n(\chi+\eta) = (k_n + l_n)\,a_n, \qquad a_n(\chi\eta) = (k_n l_n)\,a_n.$$

However, from the conditions (8) for the sequence (9) and similar conditions for the sequence (10) we have:

$$k_{n+1} + l_{n+1} \equiv k_n + l_n \pmod{p^n},$$

$$k_{n+1} l_{n+1} \equiv k_n l_n \pmod{p^n},$$

and these congruences remain valid if the left-hand sides are replaced by their positive remainders modulo p^{n+1}, the right-hand sides modulo p^n. In this way there correspond to the sum and product of the endomorphisms χ and η the sum and product of the sequences (9) and (10), obtained by component-wise addition and multiplication and subsequent reduction modulo p^n at the n-th place.

The set of sequences of the form (9) subject to the conditions (7) and (8), with addition and multiplication defined by the rules just described is therefore isomorphic to the ring of endomorphisms of a group of type p^∞; that is to say, it is itself a commutative ring. This ring is called the *ring of p-adic integers* and plays a very significant rôle in various branches of algebra, mainly in the theory of fields and in topological algebra. Thus, the *ring of endomorphisms of a group of type p^∞ is isomorphic to the ring of p-adic integers.*

The sequence $(0, 0, \ldots, 0, \ldots)$, which corresponds to the null endomorphism, is the zero of the ring of p-adic integers, and the sequence $(1, 1, \ldots, 1, \ldots)$, which corresponds to the identity automorphism, is the unit element. Further, since an endomorphism of a group of type p^∞ is an automorphism if and only if it does not carry the element a_1 into zero, we find that the p-adic integer (9) has an inverse if and only if $k_1 \neq 0$.

In the same way we could prove a number of other properties of the ring of p-adic integers. We shall only show that *this ring has no divisors of zero.* For, the image of a group of type p^∞ under any non-null endomorphism is the whole group and not a proper subgroup, and therefore the result of performing two non-null endomorphisms in succession cannot be the null endomorphism.

We now pass on to the problem of the *ring of endomorphisms of a direct sum.* For this purpose it is convenient to introduce the concept of the *group of homomorphisms* of one abelian group into another. We consider the set of all homomorphic mappings of an abelian group A into an abelian

group B and define the *sum* of any two homomorphisms χ, η of this set by the formula

$$a(\chi + \eta) = a\chi + a\eta, \qquad a \in A.$$

The proof that the mapping $\chi + \eta$ is a homomorphism and that the set of homomorphisms of A into B is in this way turned into an abelian group is a literal repetition of the one we gave at the beginning of this section for the special case of the addition of endomorphisms.

We note that if three abelian groups A, B, and C are given, then we can also speak of the *product* of a homomorphism of A into B by a homomorphism of B into C, defining it as the result of performing the homomorphic mappings in succession; it is, of course, a homomorphism of A into C.

Now let G be an abelian group represented as a direct sum of a finite number of groups H_i,

$$G = \sum_{i=1}^{n} H_i.$$

We denote by R_{ii} the ring of endomorphisms of H_i, and by R_{ij} for $i \neq j$, the group of homomorphisms of H_i into H_j. Then the following theorem holds (see Kiškina [1]).

The ring of endomorphisms of the group $G = \sum_{i=1}^{n} H_i$ *is isomorphic to the ring of square matrices* (χ_{ij}) *of order* n, *where* $\chi_{ij} \in R_{ij}$ *and where the opertions of addition and multiplication of matrices are defined in the usual way.*[1]

For let us associate with every matrix (χ_{ij}) of this form a mapping χ of G into itself which is defined as follows: If $g \in G$ and

$$g = \sum_{i=1}^{n} h_i, \qquad h_i \in H_i,$$

then we put

$$g\chi = \sum_{i=1}^{n} \sum_{j=1}^{n} h_i \chi_{ij}.$$

It is easy to see that this mapping is an endomorphism of G. Conversely, every endomorphism χ of G corresponds in this sense to a matrix; for if h_i is an arbitrary element of H_i and if

$$h_i\chi = \sum_{j=1}^{n} h_{ij}, \qquad h_{ij} \in H_j,$$

[1] Note that with matrices of the given form not only addition but also multiplication can always be performed and that the resulting matrices are obviously themselves of the same form.

then we put

$$h_i\chi_{ij} = h_{ij};$$

the mapping χ_{ij} is obviously a homomorphism of H_i into H_j. The proof that this one-to-one correspondence between the endomorphisms of G and the matrices of the form (χ_{ij}) preserves sums and products is not difficult and is left to the reader. It follows, in particular, that the matrices of the form (χ_{ij}) actually form a ring.

From this theorem and results of § 12 it follows that the group of automorphisms of $G = \sum_{i=1}^{n} H_i$ is isomorphic to the multiplicative group of those matrices of the form (χ_{ij}) that have an inverse in the ring of all these matrices. The identity automorphism of G corresponds to the matrix that has the unit elements of the rings R_u down the main diagonal and zeros elsewhere.

Let us apply these results to the case of *finitely generated abelian groups* which, as we know, are direct sums of infinite and finite primary cyclic groups. We have already studied the rings of endomorphisms of cyclic groups. It is now easy to prove the following statement: If A and B are two infinite or finite primary cyclic groups, then the group of homomorphisms of A into B is 1) isomorphic to B if A is infinite, 2) cyclic of order $p^{\min(k,\,l)}$ if A and B are primary with respect to the same prime number p and are of order p^k and p^l, respectively, 3) null in all other cases. We observe, further, that if $\{a\}$, $\{b\}$, and $\{c\}$ are three cyclic groups and if φ is a homomorphism of the first into the second and ψ a homomorphism of the second into the third, where

$$a\varphi = kb,\ b\psi = lc,$$

then

$$a(\varphi\psi) = (kl)c.$$

Therefore, if we regard these groups of homomorphisms of cyclic groups as the additive groups of the ring of integers I and its residue-class ring I_n, then we find that the product of homomorphisms corresponds to the product of the associated integers reduced, of course, modulo the order of $\{c\}$.

We leave it to the reader to supply the details of the proofs of the statements in the preceding paragraph and to obtain the actual description of the ring of endomorphisms of a finitely generated abelian group given by its invariants. We note only the following results, which refer to the case of free abelian groups.

The ring of endomorphisms of a free abelian group of rank n is isomorphic to the ring of all square matrices of order n with integer coefficients.

The group of automorphisms of a free abelian group of rank n is isomorphic to the group of those square matrices of order n with integer elements whose determinants are ± 1.

The groups of automorphisms and rings of endomorphisms of various classes of abelian groups are studied in a number of papers, particularly those by Shoda [1], [3], Baer [14], [27], Derry [1], Shiffman [1], Kiškina [1].

§ 22. Abelian groups with operators

In various applications of abelian groups with operators the domain of operators turns out to be an associative ring R with elements $\alpha, \beta, \gamma, \ldots$ where in addition to the conditions for operators

$$(a+b)\alpha = a\alpha + b\alpha$$

the following two conditions hold:

$$a(\alpha+\beta) = a\alpha + a\beta, \tag{1}$$

$$a(\alpha\beta) = (a\alpha)\beta \text{ [1]} \tag{2}$$

They form a link between the group operation in G and the operations defined in the ring R.

Only when conditions (1) and (2) are satisfied shall we say that *the group G has an operator ring R*. We shall then also say that G is a *module over the ring R* or, briefly, an *R-module.*

(1) and (2) are plausible conditions, because if we consider the ring of endomorphisms of an abelian group G or any subring of it as operator domain for the group, then (1) and (2) follow immediately from the definitions of sum and product of endomorphisms. Further, if a ring is considered as a right operator domain for its additive group, then (1) and (2) become the distributive law for the ring operations and the associative law for the multiplication. Finally, the vector spaces over a field F which are studied

[1] We must keep in mind that the sign + on the left-hand side of (1) is the sign of addition in R, on the right-hand side it is the sign of the group operation in G. Similarly in (2) we should distinguish between multiplication of elements of R and the effect of an operator of R on an element of G.

in higher algebra are obviously F-modules. Note that every abelian group without operators can be regarded as a module over the ring of integers.

From (1) it follows that

$$a\alpha = a(\alpha + 0) = a\alpha + a\cdot 0,$$

so that $a\cdot 0 = 0$; that is, the zero element of the ring R as an operator corresponds to the null endomorphism of G.[1]

Further,

$$a\alpha = a(\alpha - \beta + \beta) = a(\alpha - \beta) + a\beta,$$

so that

$$a(\alpha - \beta) = a\alpha - a\beta. \tag{1}$$

If the ring R has a unit element ε, then the operator ε need not correspond to the identity automorphisms of G. For example, conditions (1) and (2) are satisfied if we put $a\alpha = 0$ for every a of G and every α of R; but in this case the presence of an operator ring does not contribute anything to the study of the group G. The general case can easily be reduced to this extreme case and the case in which the operator ε corresponds to the identity automorphism.

For let G be an abelian group with an operator ring R that has a unit element ε. We denote by H the set of all the elements a of G for which $a\varepsilon = a$, and by K the set of all the elements of G for which $a\varepsilon = 0$. H and K are admissible subgroups of G and their intersection consists of the null element only. *Their direct sum is* G, because we have for every a of G

$$a = a\varepsilon + (a - a\varepsilon),$$

where obviously $a\varepsilon \in H$, $a - a\varepsilon \in K$. Clearly we have the right to restrict our investigations to the direct summand H as a group with operators for which ε corresponds to the identity automorphism. In what follows, if we speak of an *operator ring with unit element* we shall always take this restriction for granted, in other words, we shall assume that

$$a\varepsilon = a \tag{3}$$

for all a of G.

If G is a group with an operator ring R, then the set α of all elements

[1] The symbol 0 on the left-hand side is the zero element of R; that on the right-hand side, the null element of G.

$\mathfrak{a}$ of R that *annihilate* a given element a of G, that is, for which $a\alpha = 0$, is a right ideal of R, as equations (1′) and (2) indicate. This ideal $\mathfrak{a}$ is called the *order* of a. For ordinary abelian groups, that is, groups with the ring of integers I as operator ring, this definition agrees essentially with the usual one: if an element a has order n in the usual sense, then it is annihilated by the multiples of n only, in other words, by the numbers of the ideal $\mathfrak{n}$ in I.

If the order of an element is the null ideal of R, then a is called an *element of infinite order*. In the additive group of a ring R without divisors of zero and with R itself as right operator domain, all the elements, except zero, have infinite order. The order of the null element of G is, of course, always the whole ring R, and it is the only element whose order is R, if we consider an operator ring with unit element (see condition (3)).

If an operator ring R with unit element is studied, then the admissible monogenic subgroup of an element a of G (see § 15) consists of all elements of the form $a\alpha$, $\alpha \varepsilon R$. For these elements form a subgroup of G by (1), this subgroup is admissible by (2), a is contained in this subgroup by (3), and finally the subgroup is monogenic since every admissible subgroup containing a must also contain all the elements $a\alpha$.

The admissible monogenic subgroup of an element a is operator-isomorphic to the factor groups $R/\mathfrak{a}$, where $\mathfrak{a}$ is the order of a. In particular, if $\mathfrak{a}$ is a two-sided ideal of R, then the monogenic subgroup of a is operator-isomorphic to the additive group of the residue-class ring $R/\mathfrak{a}$. For by associating the element α of R with the element $a\alpha$ of G we obtain by (1) and (2) an operator-homomorphic mapping of the additive group of R onto the monogenic subgroup of a, and it is precisely the elements of $\mathfrak{a}$ that are mapped onto the null element.

Every result of the general theory of abelian groups gives rise to the question: for which operator rings does this result remain valid? A revision of the contents of the theory of abelian groups from this point of view is far from complete, although it would be of considerable interest for the theory of rings as well. We restrict ourselves here to a few remarks concerning results that have been proved in the preceding sections of this chapter. In order to avoid needless complication we shall assume that *the operator ring R is a ring with a unit element and without divisors of zero.*

The periodic part F of a group G, that is, the set of all elements whose orders are not the null ideal, is a subgroup, provided that *the intersection of any two non-zero right ideals of R is itself not the zero ideal.* This subgroup is admissible if we assume in addition that the ring R is *commutative.*

In that case, the factor group G/F is also an R-module and all its elements other than the null element have infinite order.

The theorem on the decomposition of a periodic abelian group into the direct sum of primary groups requires much stronger restrictions on the operator ring R. In any case, it is sufficient to assume that R is a *commutative principal ideal ring.*

The definition of linear dependence of elements preserves its meaning in groups with any operator ring R. If we assume this ring to be commutative, then the exchange theorem remains valid and the concept of the *rank* of a group can therefore be introduced. Under the same assumption it remains true that the rank of a group is equal to the sum of the rank of an arbitrary (admissible) subgroup and the rank of its factor group.

In a group with operator ring R, the rôle of the infinite cyclic group is taken over by the additive group of R, considered as a right R-module; we can choose as generator the unit element of R or any divisor of the unit element. The direct sum of an arbitrary set of such groups will be called a *free R-module.* If R is a commutative ring, then the rank of a free R-module is equal to the number of monogenic direct summands.

Every R-module is isomorphic to a factor group of a free R-module, and if R is commutative, then an R-module with n generators is isomorphic to a factor group of a free R-module of rank n.

This theorem is proved by means of an operator-homomorphic mapping of a free R-module with a suitable system of generators onto the given R-module, and an application of the homomorphism theorem for operator groups.

If the right ideals of R are principal, then every admissible subgroup of a free R-module, except the null subgroup is itself free.

In order to prove this theorem we have to repeat the proof of the corresponding theorem of § 19, but with the following modifications: if we consider in the given subgroup the elements with a given last index ν, then we cannot say that among them there is an element with smallest positive last coefficient. However, it is easy to see that the last coefficients of all these elements form a right ideal in R, which by assumption is principal, that is, of the form αR. The element with last index ν and last coefficient α will now play the rôle of the element with smallest positive last coefficient.

In the paper by Everett [1] it is proved that the conditions we have imposed on R—existence of a unit element, absence of divisors of zero, all right ideals are principal—are also necessary for the theorem on subgroups of a free R-module to be valid.

If we wish to extend to abelian operator groups the theorem on the connection between the bases of a free abelian group of finite rank and the bases of its subgroups or the fundamental theorem on finitely generated abelian groups that follows from it, then we must impose much stronger restrictions on the operator ring R. In the paper by Teichmüller [1] it is proved that these results remain valid provided that *all left and all right ideals of R are principal.*[1] The special case of a Euclidean ring R is treated in Chapter XV of the second edition of van der Waerden's *Modern Algebra*.

[1] See § 24 of the first edition of this book.

CHAPTER VII

PRIMARY AND MIXED ABELIAN GROUPS

§ 23. Complete abelian groups

The theory of primary abelian groups is one of the richest and deepest branches of the whole theory of groups; the theory of countable primary groups, in particular, has attained its final form. A number of separate theories—the theory of complete groups, the problem of serving subgroups, and others—have gradually emerged from the framework of the general theory of primary groups. It is expedient to treat the theory of primary groups in close connection with the theory of mixed abelian groups, all the more because this method leads to a natural approach to the main problem in the theory of mixed abelian groups; namely, the problem of their decomposition into the direct sum of a periodic group and a torsion-free group.

We begin with the study of an important class of abelian groups which is, in a way, dual to the class of free abelian groups.

An abelian group G is called *complete*[1] if for every element a of G and every natural number n the equation

$$nx = a$$

has at least one solution in G, or if each element a is *divisible* in G by every natural number. Obviously, for a group G to be complete it is sufficient that each element of the group be divisible by every prime number.

It follows immediately from the definition that *every factor group of a complete group is complete* and that *the direct sum of an arbitrary set of complete groups is itself a complete group.*

If an abelian group G contains a complete subgroup A, then A is a direct summand of G.

For let B be one of the maximal subgroups of G whose intersection with A is the null subgroup; the existence of such a subgroup follows from a theorem proved in § 7. A and B form a direct sum in G. Now if G contains an element g not in $A + B$, then the intersection of the subgroups $A + B$ and $\{g\}$ cannot be the null element, since otherwise the intersection of A and $B + \{g\}$ would also be the null element, in contradiction to the choice of B. A mul-

[1] Note that the term complete group is also used (§ 13, p. 92) for a group without center and without outer automorphisms. There is no danger of confusion between the two concepts. Complete abelian groups are also called *divisible* groups. [*Trans.*]

tiple of g therefore belongs to $A + B$; that is,

$$pg = a + b, a \epsilon A, b \epsilon B;$$

we can assume here that p is a prime number, for it is sufficient to replace g by a multiple that is not contained in $A + B$, while a prime multiple of the latter is contained in $A + B$.

Now there exists an element a' in A such that $pa' = a$. Hence

$$p(g - a') = b \epsilon B, g - a' \notin A + B.$$

We put $g' = g - a'$. Every element of $\{g', B\}$ has the form $kg' + b'$, where $0 \leqq k \leqq p - 1, b' \epsilon B$. If the intersection of A and $\{g', B\}$ is not the null element, then there exists an element $\bar{a}$ in $A, \bar{a} \neq 0$, such that

$$\bar{a} = kg' + b'.$$

Here $k \neq 0$, since $A \cap B = 0$; but $pg' \epsilon B$ and p and k are co-prime. Hence $g' \epsilon A + B$, which is impossible. On the other hand, the intersection of A and $\{g', B\}$ cannot be the null element, because this contradicts the choice of B. Thus $G = A + B$.

The sum of an arbitrary set of complete subgroups of an abelian group is itself a complete subgroup.

For if complete subgroups A_α of an abelian group G are given, then every element of their sum has the form $a_{\alpha_1} + a_{\alpha_2} + \ldots + a_{\alpha_k}$, where $a_{\alpha_i} \epsilon A_{\alpha_i}$. If $a_{\alpha_i} \epsilon A_{\alpha_i}$, $pa_{\alpha_i} = \bar{a}_{\alpha_i}$, $i = 1, 2, \ldots, k$, then the element $\bar{a}_{\alpha_1} + \bar{a}_{\alpha_2} + \ldots + \bar{a}_{\alpha_k}$ lies in the sum of the subgroups A_α and

$$p(\bar{a}_{\alpha_1} + \bar{a}_{\alpha_2} + \ldots + \bar{a}_{\alpha_k}) = a_{\alpha_1} + a_{\alpha_2} + \ldots + a_{\alpha_k}.$$

In particular, the sum $\bar{A}$ of all complete subgroups of an abelian group G is the unique maximal complete subgroup of G. In the direct decomposition

$$G = \bar{A} + G',$$

which exists by the above theorem, the summand G' contains no complete subgroup. We shall call an abelian group *reduced* if none of its subgroups is complete. We therefore have: *Every abelian group can be decomposed into the direct sum of two groups, one complete and the other reduced.* An abelian group G may have many direct decompositions of this kind, but the

complete summand is always the same, and the reduced summands are therefore isomorphic.

It is easy to give a survey of all complete abelian groups. *Groups of type R*, that is, groups isomorphic to the additive group of all rational numbers, are obviously complete, and so are groups of type p^∞ for all prime numbers p (see § 7). That every element of a group of type p^∞ is divisible by p follows from the definition of the group, and that it is divisible by every prime number q, other than p, is true even within the cyclic subgroup of order p^n generated by that element. It now turns out that these groups and their direct sums exhaust all complete groups.

Every complete abelian group is decomposable into the direct sum of a set of groups of type R and of groups of type p^∞ for various prime numbers p.

For, the periodic part F of a complete abelian group G is itself complete, since every solution x of the equation $nx = a$ has finite order if a has finite order. We therefore have the direct decomposition

$$G = F + H,$$

where H is torsion-free and complete (because it is isomorphic to a factor group of a complete group). In § 19 we proved that F is the direct sum of primary groups F_p for distinct prime numbers p. Furthermore, every F_p is complete: if $a \in F_p$, then a solution of the equation $px = a$ has as its order a power of p and is therefore contained in F_p, whereas every equation $qx = a$ with $(p, q) = 1$ is known to be solvable even in $\{a\}$.

It therefore remains to consider two special cases: a complete group that is torsion-free and a complete group that is primary with respect to p.

If G is a complete torsion-free group and a an element of G, $a \neq 0$, then there exist elements $a_1, a_2, \ldots, a_n, \ldots$ in G such that

$$a_1 = a, \quad na_n = a_{n-1}, \quad n = 2, 3, \ldots.$$

These elements generate in G a subgroup of type R (see Example 2, § 18). Let M be a maximal linearly independent system of G. We embed each element of M in a subgroup of type R in the way just described. It follows from the linear independence of M that the sum G' of all these subgroups is direct. Now G' must be equal to G. For, every element b of G is linearly dependent on M, so that we have an equation

$$nb = k_1 a_1 + k_2 a_2 + \ldots + k_r a_r,$$

where $n \neq 0, a_1, a_2, \ldots, a_r \in M$. Since G' is complete, we can find an element c in G' that satisfies the same linear relation. Hence

$$n(b - c) = 0, \text{ that is, } b = c \text{ and } G' = G.$$

We now turn to the case of a group that is p-primary and remark, first of all, that every element of a complete primary group is contained in a subgroup of type p^∞. For if a is an element of order p^k in a complete group, then we put

$$a_1 = p^{k-1}a, \quad a_2 = p^{k-2}a, \ \ldots, \ a_{k-1} = pa, \quad a_k = a.$$

Now we choose as a_{k+1} one of the elements x for which $px = a$; if the element a_n, $n \geqq k$, has been chosen, then we choose as a_{n+1} a solution of the equation $px = a_n$. The elements $a_1, a_2, \ldots, a_n, \ldots$ obviously generate a subgroup of type p^∞ containing a.

Hence, by the usual transfinite process, we can construct a set of subgroups of type p^∞ in the complete primary group G such that their sum G' is direct and that no subgroup of G of type p^∞ has the null element as its intersection with G'. We now show that G' is equal to G. If G contains an element a outside G', and if $G' \cap \{a\} = 0$, then we embed a in a subgroup of type p^∞ and obtain a contradiction to the definition of G'. If $p^k a \in G'$, but $p^{k-1}a \notin G'$, then we can find an element a' in G' such that $p^k a' = p^k a$, because G' is complete. Now $a - a'$ is not null, but the intersection of its cyclic subgroup with G' is the null element, and we again have the previous case. We have thus shown that G is a direct sum of groups of type p^∞.

This completes the proof of the theorem.

As a particular case of this theorem we see that the additive group of all real numbers, which is a complete torsion-free group whose cardinal number is that of the continuum, is decomposable into the direct sum, whose cardinal number is that of the continuum, of a set of groups of type R.

Every direct decomposition of a complete abelian group can be refined to a decomposition into the direct sum of groups of type R and of type p^∞. Any two decompositions of a complete group into the direct sum of groups of type R and of type p^∞ are isomorphic.

The first part of this theorem follows from the fact that *every direct summand of a complete group is itself complete*—if $G = A + B$ and $n(a' + b') = a$, where $a, a' \in A$, $b' \in B$ then $na' = a$—and therefore, as we have shown above, is a direct sum of groups of type R and of type p^∞.

For the proof of the second part, we take an arbitrary decomposition of the group G into the direct sum of groups of type R and of type p^∞. If we select from every direct summand of type R of this decomposition one element, other than the null element, then we obtain a maximal linearly independent system of G. If now follows from results of § 19 that the number of direct summands of type R (that is, the cardinal number of this set) does not depend on the choice of the decomposition. On the other hand, if we take for a fixed p the sum of the direct summands of type p^∞ that occur in the given decomposition, then we obtain a subgroup A of G consisting of all those elements whose order is finite and a power of p; clearly, this subgroup does not depend on the choice of the decomposition. The number of elements of A whose order is not greater than p is p^n if there are n summands of type p^∞; but if there are infinitely many such elements in A then the cardinal number of this set is the same as the cardinal number of the set of direct summands of type p^∞ in the given direct decomposition of G. This shows that the number of direct summands of type p^∞ (that is, the cardinal number of this set) again does not depend on the choice of the decomposition.

Every abelian group can be embedded in a complete abelian group.

The following simple proof of this theorem is due to Kulikov [2]. We know that an abelian group G can be represented as a factor group of a free abelian group U

$$G = U/N.$$

We take any decomposition of U into the direct sum of infinite cyclic groups. We now embed each cyclic direct summand in a group of type R—just as, for example, the additive group of integers is embedded in the additive group of rational numbers—and take the direct sum of all these groups of type R. We obtain a complete group V containing U. The factor group V/N, which is also complete, contains U/N as a subgroup, that is, contains G.

From this theorem we deduce the converse of the theorem that a complete group is a direct summand of every abelian group containing it (see Baer [26]).

If an abelian group G is a direct summand of every abelian group that contains it as a subgroup, then it is complete.

For G must be a direct summand of every complete group in which it is contained. But we know that every direct summand of a complete group is itself complete.

The following result, partly contained in the paper by Baer [26] and completely proved by Kulikov, supplements the theorem on the embedding of every abelian group in a complete group.

In every complete abelian group containing a given group G there is at least one complete subgroup that is minimal among those containing G. Between any two minimal complete groups containing G there exists an isomorphism extending the identity automorphism of G. [An isomorphism φ_1 between two groups H_1 and K_1 is said to be an *extension* of an isomorphism φ between their subgroups H and K if $h\varphi = k$ implies $h\varphi_1 = k$, $h \in H$, $k \in K$.]

If G is complete there is nothing to prove. Assume that G is not complete and let G be contained in a complete group $\overline{G}$. Since the union of an ascending sequence of complete groups is complete, there exist maximal complete subgroups of $\overline{G}$ whose intersection with G is the null element. Let H be one of them. We have a direct decomposition

$$\overline{G} = H + K,$$

where K can be chosen to contain G. K, as a direct summand of a complete group, is complete and is the required minimal complete subgroup containing G. For if there exists a complete group K' between G and K

$$G \subset K' \subset K,$$

then

$$K = K' + K'',$$

that is,

$$\overline{G} = K' + (K'' + H).$$

The subgroups K'' and, therefore, $K'' + H$ are complete, and since $(K'' + H) \cap G = 0$ we have a contradiction to the choice of H.

Now let K_1 and K_2 be any two minimal complete groups containing G. Since G is not complete, it contains an element a such that for some prime number p the equation

$$px = a$$

has no solution in G. Let b_1 and b_2 be solutions of this equation in K_1 and K_2, respectively. We obtain an isomorphism φ' between $K_1' = \{G, b_1\}$ and $K_2' = \{G, b_2\}$ if we map the subgroup G identically onto itself and put

$$b_1\varphi' = b_2.$$

Suppose that for all ordinal numbers β less than α we have already found subgroups $K_1^{(\beta)}$, of K_1 forming an ascending sequence, and subgroups $K_2^{(\beta)}$, of K_2 and isomorphisms $\varphi^{(\beta)}$, mapping $K_1^{(\beta)}$ onto $K_2^{(\beta)}$, such that these isomorphisms extend one another. If α is a limit number, then we denote the union of the subgroups $K_i^{(\beta)}$, by $K_i^{(\alpha)}$, $i=1,2$, and define $\varphi^{(\alpha)}$ as the union of all isomorphisms $\varphi^{(\beta)}$, $\beta<\alpha$. But if the number $\alpha-1$ exists, then let a_1 be an element of $K_1^{(\alpha-1)}$ such that for a certain prime number p the equation

$$px=a_1$$

has no solution in $K_1^{(\alpha-1)}$; we denote a solution in K_1 by b_1. If $a_1\varphi^{(\alpha-1)}=a_2$ and if b_2 is a root of the equation

$$px=a_2$$

in K_2, then we put

$$K_i^{(\alpha)}=\{K_i^{(\alpha-1)},\ b_i\},\ i=1,\ 2.$$

The mapping $\varphi^{(\alpha)}$ that coincides with $\varphi^{(\alpha-1)}$ on $K_i^{(\alpha-1)}$ and carries b_1 into b_2 is an isomorphism between $K_1^{(\alpha)}$ and $K_2^{(\alpha)}$.

This construction terminates when the subgroups $K_1^{(\alpha)}$ and $K_2^{(\alpha)}$ are complete, that is, when they coincide with K_1 and K_2 respectively. This concludes the proof of the theorem.

We note that a complete group may have several minimal complete subgroups containing a given subgroup G. For example, take the direct sum of two groups of type p^∞, a group A with generators

$$a_1, a_2, \ldots, a_n, \ldots$$

and with relations

$$pa_1=0,\quad pa_{n+1}=a_n,\quad n=1,\ 2,\ \ldots,\ .$$

and a group B with generators

$$b_1, b_2, \ldots, b_n, \ldots$$

and with relations

$$pb_1=0,\quad pb_{n+1}=b_n,\quad n=1,\ 2,\ \ldots,$$

then $\{a_1\}$ is contained in the subgroup A as well as in the subgroup of type p^∞ generated by the elements

$$a_1,\ a_2+b_1,\ \ldots,\ a_n+b_{n-1},\ \ldots\ .$$

§ 24. Direct sums of cyclic groups

We have already studied two classes of abelian groups that are direct sums of cyclic groups, namely free abelian groups—that is, direct sums of an arbitrary set of infinite cyclic groups—and finitely generated abelian groups—that is, direct sums of a finite number of arbitrary cyclic groups. These groups turned out to have a number of properties in common; and we now wish to show that these are, in fact, properties of the direct sums of any set of arbitrary cyclic groups. Clearly we may assume that all the finite cyclic summands of these direct sums are primary with respect to various prime numbers.

There exist several criteria for an abelian group to be the direct sum of cyclic groups. We shall only establish one such condition, which refers to the case of primary groups. But we first have to introduce a few concepts that are essential for the whole theory of primary abelian groups.

If G is a p-primary group, then the set G_1 of all elements of G of order at most p is a fully invariant subgroup of G. We shall call this subgroup the *lowest layer* of G. [In a group G the set of all elements of a given order is said to form a *layer* of G. Infinite groups in which all layers are finite—such groups are necessarily periodic—have been studied by Černikov [12].]

An element a of a p-primary group G is said to be of *infinite height* if for every k the equation

$$p^k x = a$$

has at least one solution in G. But if this equation can be solved only for $k \leqq h$, then we say that a is an element of *finite height*, or more precisely, of *height* h.

[It follows from this definition that in every primary abelian group G the null element is an element of infinite height. If the null element is the only element of infinite height in G, then G is called a *group without elements of infinite height* (compare "group without center"). This slightly inaccurate but convenient terminology saves a lot of circumlocution later.] P

Note that it would be more accurate to speak of the *height of* a *in* G, since the height of a in a subgroup H of G may turn out to be less than in G itself.

The following properties of the height of an element are immediate consequences of the definition. If a_1 and a_2 are two elements of a group G, of height h_1 and h_2 respectively, then $a_1 + a_2$ is of height h_1 if $h_1 < h_2$, and of height at least h if $h_1 = h_2 = h$. If a is an element of height h, then pa is an element of height at least $h + 1$. If a and b generate the same

cyclic subgroup of G, then they have the same height in G. If G is a direct sum, then an element that is contained in a direct summand has the same height in that summand as in G. The height of an arbitrary element of a direct sum is equal to the least height of its components.

In complete primary groups, and in them only, every element has infinite height. Furthermore, if *every element of the lowest layer of a primary group G has infinite height in G, then G is complete.* For suppose that it has already been proved that all elements of G of order p^n have infinite height. If a is any such element and b_1, b_2 are two solutions of the equation $px = a$, then $b_1 - b_2$ is of order p and therefore of infinite height. It follows from the first statement of the preceding paragraph that b_1 and b_2 have the same height. However, since a is an element of infinite height, the equation $px = a$ must have solutions whose heights exceed any given natural number. So we see that all the solutions of $px = a$ for any element a of order p^n—in other words, all elements of order p^{n+1}—must have infinite height in G.

We now prove the following *criterion of Kulikov* [2].

Kulikov's Criterion. *A primary abelian group G is a direct sum of cyclic groups if and only if it is the union of an ascending sequence of subgroups*

$$A^{(1)} \subseteq A^{(2)} \subseteq \ldots \subseteq A^{(n)} \subseteq \ldots \tag{1}$$

such that the elements of each subgroup are of finite and bounded height in G.

Proof. If G is representable as a direct sum of cyclic groups, then we can take as $A^{(n)}$, $n = 1, 2, \ldots$, the sum of those direct cyclic summands whose order does not exceed p^n.

Conversely, let G be represented as the union of the ascending sequence (1) subject to the condition of the theorem. As x_1 we select one of the elements of order p in $A^{(1)}$ with the greatest possible height in G; such elements exist, since the elements of $A^{(1)}$ are of bounded height in G.

Suppose now that for all ordinal numbers α less than a certain β we have already chosen elements x_α satisfying the following conditions:

1) all the elements x_α have order p;

2) if x_α is contained in $A^{(n)}$, then it is not in $A^{(n-1)}$, and if H_α is the subgroup generated by all $x_{\alpha'}$ with $\alpha' < \alpha$, then:

a) H_α contains the lowest layer $A_1^{(n-1)}$ of $A^{(n-1)}$;

b) x_α is not contained in H_α and has maximal height in G among all elements of $A^{(n)}$ outside H_α.

If the subgroup H_β generated by all x_α, $\alpha < \beta$, does not coincide with the lowest layer G_1 of G, then we choose x_β in the following way: It follows from 2a) that there exists an n such that all x_α are contained in $A^{(n)}$, but not all are contained in $A^{(n-1)}$. If H_β does not coincide with $A_1^{(n)}$, then we take as x_β one of the elements of order p of $A^{(n)}$ lying outside H_β and of maximal height in G. But if H_β and $A_1^{(n)}$ are equal, then we take an analogous element from the smallest subgroup of the sequence (1) whose lowest layer is greater than $A_1^{(n)}$. In both cases we obviously appeal to the conditions on the subgroups $A^{(n)}$ imposed by the theorem.

The selection of the elements x_α can thus be continued as long as they do not generate the lowest layer of G. Suppose this occurs when the x_α have been chosen for all α less than γ. It follows from 1) and 2b) that the lowest layer of G has the direct decomposition

$$G_1 = \sum_{\alpha<\gamma} \{x_\alpha\}. \tag{2}$$

Let h_α be the height of x_α in G and y_α an element of G for which

$$p^{h_\alpha} y_\alpha = x_\alpha.$$

By (2), the cyclic subgroups $\{y_\alpha\}$ form a direct sum which we denote by F,

$$F = \sum_{\alpha<\gamma} \{y_\alpha\}. \tag{3}$$

Let us show that *every element z of G of order p has the same height in F as in G* (z is an element of F, since $G_1 \subseteq F$). By (2), z can be written in the form

$$z = x'_{\alpha_1} + x'_{\alpha_2} + \ldots + x'_{\alpha_n},$$

where the element $x'_{\alpha_i}, i = 1, 2, \ldots, n$, is a multiple of x_{α_i} and therefore has the same height in F as in G. In view of the direct decomposition (3), the height h of z in F is the smallest of the numbers h_{α_i}, $i = 1, 2, \ldots, n$. The height of this element in G cannot be less than h; we show that it cannot be greater. Let k be the index for which $h_{\alpha_k} = h$ but $h_{\alpha_i} > h$ for $i > k$. Then in the sum

$$z = (x'_{\alpha_1} + \ldots + x'_{\alpha_k}) + (x'_{\alpha_{k+1}} + \ldots + x'_{\alpha_n})$$

the second term either does not occur (if $k = n$) or its height in G is greater than h. As for the first term, it is not contained in H_{α_k} and its

height in G cannot be greater than the height of x_{α_k} in G, so that $h_{\alpha_k} = h$, otherwise we would have a contradiction to condition 2b) imposed on the choice of x_{α_k}. Thus z is a sum of two elements with distinct height. Hence its height is equal to the smaller of the two heights, that is, does not exceed h. This proves that z has the same height in F as in G.

Suppose now that F is different from G. Let g be an element of G of smallest order outside F, and let its order be p^s; clearly $s \geqq 2$. The element $p^{s-1}g$ is of order p and therefore belongs to F; we have proved that it has the same height in F as in G. There exists, then, an element f of F such that

$$p^{s-1}f = p^{s-1}g.$$

The order of the element $g - f$ does not exceed p^{s-1}, that is, $g - f$ is contained in F. But then g must also be contained in F, contrary to our assumption. This shows that $F = G$ and completes the proof of the criterion.

From this criterion we deduce the following two theorems (Prüfer [2]), which are fundamental in the theory of primary abelian groups.

Prüfer's First Theorem. *Every primary group in which the orders of the group elements are bounded is a direct sum of cyclic groups.*

For in this case the heights of all elements of the group are finite and also bounded, so that we can apply Kulikov's criterion, putting all the $A^{(n)}$ equal to the group itself.

Prüfer's Second Theorem. *Every countable primary group without elements of infinite height is a direct sum of cyclic groups.*

For since the group is countable it can be represented as the union of an ascending sequence of finitely generated subgroups, and these subgroups, as periodic commutative groups, are all finite. The heights of the elements of each of these subgroups are finite, and since there is only a finite number of them, they are bounded.

Kulikov's criterion also leads to a simple proof of the following result:

If a primary group G is a direct sum of cyclic groups, then every subgroup H of G is also a direct sum of cyclic groups.

For by Kulikov's criterion G is the union of an ascending sequence of subgroups $A^{(n)}$, $n = 1, 2, \ldots$, where all the elements of each subgroup $A^{(n)}$ have finite and bounded heights in G. If

$$B^{(n)} = H \cap A^{(n)}, \quad n = 1, 2, \ldots,$$

then all the elements of each subgroup $B^{(n)}$ have finite order in G and a

fortiori in H, and also bounded heights. H is, however, the union of the subgroups $B^{(n)}$, and we can therefore again apply Kulikov's criterion.

We shall now leave the study of primary groups and return to the general case. The preceding result and the theorem on subgroups of free abelian groups at the end of § 19 lead to the following general result.

If an abelian group G is a direct sum of cyclic groups, then every subgroup H of G is also a direct sum of cyclic groups.

For if G^* is the periodic part of G, then G, as the direct sum of cyclic groups, is the direct sum of G^* and of a free subgroup K. The factor group of our subgroup H with respect to its periodic part H^* is, by the isomorphism theorem, isomorphic to a subgroup of G/G^*, that is, is isomorphic to a subgroup of K. Therefore H/H^* is itself free, as a subgroup of a free group, and by the theorem at the end of § 19, H is the direct sum of H^* and a free subgroup. Furthermore G^* is the direct sum of primary subgroups for distinct prime numbers p, and each of these primary subgroups is a direct sum of cyclic groups. H^* is the direct sum of its intersections with these primary subgroups, and it now remains to apply the preceding theorem on the subgroups of a direct sum of primary cyclic groups.

If an abelian group G is a direct sum of cyclic groups, then every direct decomposition of G can be refined to a decomposition with cyclic direct summands.

For by the preceding theorem every direct summand of G is a direct sum of cyclic groups.

If an abelian group G is a direct sum of cyclic groups, then any two direct decompositions of G with infinite and finite primary cyclic summands are isomorphic.

For the number of infinite cyclic summands in any direct decomposition is equal to the rank of G, that is to say, is independent of the choice of decomposition. Moreover, the direct summands of one of the given decompositions whose orders are powers of a prime number p generate a primary subgroup which does not depend on the choice of the decomposition. This permits us to confine ourselves to the case in which G is itself primary.

We take one of the decompositions of G into the direct sum of cyclic groups and denote by $A^{(n)}$ the sum of the direct summands whose orders are p^n; if there are no such summands, we put $A^{(n)} = 0$. Then

$$G = A^{(1)} + A^{(2)} + \ldots + A^{(n)} + \ldots .$$

Similarly the lowest layer G_1 of G decomposes into the direct sum of the lowest layers of the $A^{(n)}$,

$$G_1 = A_1^{(1)} + A_1^{(2)} + \ldots + A_1^{(n)} + \ldots.$$

Let

$$B^{(n)} = A_1^{(n)} + A_1^{(n+1)} + \ldots;$$

then

$$B^{(n)} = A_1^{(n)} + B^{(n+1)},$$

and

$$A_1^{(n)} \simeq B^{(n)}/B^{(n+1)}, \quad n = 1, 2, \ldots.$$

It is easy to see, however, that the subgroup $B^{(n)}$, $n = 1, 2, \ldots$, can be defined independently of the particular direct decomposition of G: $B^{(n)}$ consists of precisely those elements of order p in G whose height is not less than $n-1$. The subgroup $A_1^{(n)}$ is therefore defined by G itself up to isomorphism, and since $A^{(n)}$, as the direct sum of cyclic groups of one and the same order p^n, is completely determined by its lowest layer and the number n, we have established the isomorphism of any two decompositions of G into the direct sum of cyclic groups.

The theorem on subgroups of direct sums of cyclic groups enables us, finally, to prove the following theorem:

Every abelian group is the union of a countable ascending sequence of direct sums of cyclic groups.

This is obvious for complete groups, since groups both of type R and of type p^∞ are unions of ascending sequences of cyclic groups. But in the preceding section we proved that an arbitrary abelian group G can be embedded in a complete group $\overline{G}$; it is therefore the union of its intersections with those direct sums of cyclic groups for which the union of their ascending sequence is $\overline{G}$. These intersections, however, are themselves direct sums of cyclic groups.

§ 25. Serving subgroups

A subgroup H of an abelian group G is called a *serving* (or *isolated* or *pure*) *subgroup* if for every element h of H and every natural number n the equation

$$nx = h$$

can be solved in H provided that it can be solved in G. Examples of serving subgroups are the null subgroup, the group G itself, and every direct summand of G or of its periodic part.

From the definition it follows that if H is a serving subgroup of G and K a serving subgroup of H, then K is a serving subgroup of G. Moreover, the union of an ascending sequence of serving subgroups is itself a serving subgroup.

If H is a serving subgroup of G, then in the natural one-to-one correspondence between the subgroups of G/H and the subgroups of G that contain H, serving subgroups correspond to serving subgroups.

For let A be a subgroup of G containing H. If A is a serving subgroup of G, and if there exists an element g in G such that

$$n(g + H) = a + H, \quad a \in A,$$

then

$$ng = a + h \in A;$$

as A is a serving subgroup, there exists an element $a' \in A$ such that $na' = a + h$, that is,

$$n(a' + H) = a + H.$$

This proves that A/H is a serving subgroup of G/H, and we have not even used the fact that H is a serving subgroup.

Conversely, suppose that A/H is a serving subgroup of G/H and that there exists an element g in G such that $ng = a$, where $a \in A$. Then

$$n(g + H) = a + H,$$

and therefore there exists an element a'' in A such that

$$n(a'' + H) = a + H,$$

that is,

$$na'' = a + h, \quad h \in H.$$

From the equation $ng = a$ it follows that

$$n(a'' - g) = h,$$

and as H is a serving subgroup, it contains an element h' such that $nh' = h$. Thus,

$$a = n(a'' - h'),$$

and since $a'' - h'$ is an element of A we have proved that A is a serving subgroup.

For primary groups the definition of a serving subgroup is equivalent to the following: *A subgroup H of a p-primary group G is a serving subgroup of G if and only if every element of H has the same height in H as in G.* For the division by any integer co-prime to p can be carried out even within every cyclic group of order p^n.

The following more general result holds:

In order that H be a serving subgroup of a primary group G it is sufficient that every element of the lowest layer of H has the same height in H as in G.

For suppose it has been proved that every element of H of order p^n has the same height in H as in G and let h be an element of H of order p^{n+1}. If there exists an element g in G satisfying the equation $p^k g = h$, then we also have $p^{k+1} g = ph$, and since ph is an element of H of order p^n, we can, by hypothesis, find an element h' such that $p^{k+1} h' = ph$. Hence

$$p(p^k h' - h) = 0,$$

that is, the element $p^k h' - h$ of H is of order p. But

$$p^k h' - h = p^k (h' - g),$$

and therefore we can find an element h'' in H such that $p^k h' - h = p^k h''$. Hence

$$h = p^k (h' - h''),$$

which shows that the height of h in H is the same as in G.

If a serving subgroup H of a primary group G contains the lowest layer of G, then it is equal to G.

For if G is distinct from H, let p^n be the smallest order of the elements of G outside H, $n > 1$, and let g be one of these elements. Then pg is contained in H, and since H is a serving subgroup, it contains an element h such that $pg = ph$. Hence $g - h$ is an element of order p and therefore belongs to H, and so g must also belong to H.

We have mentioned above that every direct summand of an abelian group is a serving subgroup. The converse does not always hold. *Every primary group G that is decomposable into the direct sum of cyclic groups with unbounded orders contains a serving subgroup that is not a direct summand of G.* (See Prüfer [2]).

For the proof we can confine ourselves to the case in which G is the direct sum of a countable set of cyclic groups whose generators $a_1, a_2, \ldots, a_n, \ldots$ have the orders $p^{k_1}, p^{k_2}, \ldots, p^{k_n}, \ldots$, and where

$$k_1 < k_2 < \ldots < k_n < \ldots .$$

We denote by H the subgroup of G that is generated by the elements $b_1, b_2, \ldots, b_n, \ldots$, where

$$b_n = a_n - p^{k_{n+1}-k_n} a_{n+1}, \qquad n = 1, 2, \ldots .$$

An arbitrary element h of H has the form

$$h = \sum_{n=1}^{N} l_n b_n = l_1 a_1 + \sum_{n=2}^{N} (l_n - l_{n-1} p^{k_n - k_{n-1}}) a_n - l_N p^{k_{N+1}-k_N} a_{N+1}. \quad (1)$$

The height of this element in G is equal to the greatest exponent of p that divides all the coefficients of the generators a_n, $n = 1, 2, \ldots, N+1$, on the right-hand side of (1). It is clear that then the same power of p also divides all the coefficients l_n, $n = 1, 2, \ldots, N$, and therefore h has the same height in H as in G. This proves that H is a serving subgroup of G.

The expression (1) of an arbitrary element h of H shows that H does not contain any multiples of a_1 except the null element. Furthermore, the factor group G/H is a group of type p^∞ since it is generated by the elements $\bar{a}_n = a_n + H$, which are linked by the relations

$$p^{k_1}\bar{a}_1 = 0, \quad p^{k_{n+1}-k_n}\bar{a}_{n+1} = \bar{a}_n, \quad n = 1, 2, \ldots,$$

It follows that H cannot be a direct summand of G, for otherwise G would have a subgroup of type p^∞, which contradicts the theorem of the preceding section on the subgroups of direct sums of cyclic groups.

We shall now prove two theorems giving conditions under which a serving subgroup is a direct summand. The first of these theorems can be regarded as a generalization of the theorem of § 19, according to which every subgroup with a free factor group is a direct summand; for every subgroup with a torsion-free factor group is easily seen to be a serving subgroup.

If H is a serving subgroup of the abelian group G and if the factor group $\bar{G} = G/H$ is a direct sum of cyclic groups, then H is a direct summand of G.

For let

$$\bar{G} = \sum_{\alpha} \{\bar{a}_\alpha\}. \quad (2)$$

In each coset $\bar{a}_\alpha$ we can select as representative an element a_α whose order is equal to the order of $\bar{a}_\alpha$ in $\bar{G}$. This is clear if the order of $\bar{a}_\alpha$ is infinite. But if it is finite and equal to n and if a_α' is an arbitrary element of $\bar{a}_\alpha$, then na_α' belongs to H, and since H is a serving subgroup it contains an element h satisfying the equation $nh = na_\alpha'$. As a_α we can now choose $a_\alpha' - h$, which is obviously an element of $\bar{a}_\alpha$.

We denote by A the subgroup of G that is generated by all the elements a_α. H and A together generate the whole group G, and their intersection is the null element. For if h is contained in this intersection,

$$h = k_1 a_{\alpha_1} + \ldots + k_n a_{\alpha_n},$$

then we have in $\bar{G}$ the equation

$$k_1 \bar{a}_{\alpha_1} + \ldots + k_n \bar{a}_{\alpha_n} = 0,$$

from which it follows by (2) that $k_i \bar{a}_{\alpha_i} = 0$, $i = 1, 2, \ldots, n$. This means, however, that $k_i a_{\alpha_i} = 0$, $i = 1, 2, \ldots, n$ and therefore $h = 0$. This establishes the direct decomposition

$$G = A + H.$$

The following theorem (Prüfer [2], Kulikov [1]) will be used frequently in the sequel.

If H is a periodic serving subgroup of an abelian group G and if the orders of the elements of H are bounded, then H is a direct summand of G.

Suppose that the orders of all the elements of H are divisors of n. We denote by nG the set of all the elements of G that are divisible by n; this is easily seen to be a subgroup of G. The intersection of H and nG is the null element; for every element of this intersection is divisible by n in G and therefore also in the serving subgroup H. But the n-fold multiple of every element of H is the null element. Therefore H and nG form a direct sum in G which we denote by L.

$$L = H + nG. \tag{3}$$

We now consider the factor group $\bar{G} = G/nG$ and show that $\bar{L} = L/nG$ is a serving subgroup of it. We note first of all that the order of every element of $\bar{G}$ is a divisor of n and that every element of $\bar{L}$ can be written in the form $h + nG$, $h \in H$. Let $h + nG$ be divisible by m in $\bar{G}$,

$$m(g + nG) = h + nG,$$

so that

$$mg = h + ng'.$$

We can restrict ourselves to the case in which m is a divisor of n, $n = mm'$, and therefore

$$h = m(g - m'g').$$

Since H is a serving subgroup it contains an element h' such that $mh' = h$; therefore

$$m(h' + nG) = h + nG,$$

which proves that $\bar{L}$ is a serving subgroup of $\bar{G}$.

Since the orders of all elements of $\bar{G}/\bar{L}$ are bounded, $\bar{G}/\bar{L}$ is the direct sum of a finite number of primary groups. By Prüfer's first theorem (see the preceding section) each of these is, in turn, a direct sum of cyclic groups. By what we have proved above $\bar{L}$ is therefore a direct summand of $\bar{G}$:

$$\bar{G} = \bar{L} + \bar{K}. \tag{4}$$

We denote by K the complete inverse image of $\bar{K}$ in G, that is, $\bar{K} = K/nG$. From (4) it follows that

$$\{L, K\} = G, \qquad L \cap K = nG$$

and therefore, by (3),

$$\{H, K\} = G, \qquad H \cap K = 0,$$

that is,

$$G = H + K,$$

which is what we had to prove.

From this theorem we can deduce a number of interesting corollaries (see Kulikov [1]); some of them will occur in § 29. Here we prove the following lemma (Prüfer [2]).

LEMMA. *If an element a of a p-primary group G has order p and finite height n, then it is contained in a cyclic direct summand of G of order p^{n+1}.*

For let b be an element such that $p^n b = a$. The lowest layer of $\{b\}$ is $\{a\}$, and every element of $\{a\}$ has the same height in $\{b\}$ as in G. Hence, by what we have proved above, $\{b\}$ is a serving subgroup of G, and since we can apply the preceding theorem, $\{b\}$ is a direct summand of G.

From this we obtain the following result.

Every indecomposable primary group is either cyclic or of type p^∞. For if all the elements of the lowest layer of a primary group G have infinite height in G, then G is complete, as we proved in the preceding section; and since G is indecomposable, it is a group of type p^∞. But if the lowest layer of G contains at least one element of finite height, then G has a cyclic direct summand, as we have just proved, and since G is indecomposable, it is itself cyclic. Hence *if a primary group is not a direct sum of cyclic groups and of groups of type p^∞, then it cannot be the direct sum of indecomposable groups.*

§ 26. Primary groups without elements of infinite height

A primary abelian group which is a direct sum of cyclic groups does not contain elements of infinite height: for we know that the height of an element of a direct sum is equal to the smallest height of its components, and the height of each element of a cyclic group is finite. Prüfer's second theorem (see § 24) shows that, as far as countable groups are concerned, the direct sums of cyclic groups exhaust all primary groups without elements of infinite height. For non-countable groups the corresponding theorem does not hold. This was shown first by Prüfer [1] by means of a very complicated example; much simpler ones were later given by Ulm [2] and Kuroš [9]. Kulikov [1, 2] has shown, further, that for any non-countable cardinal number m there exists a primary group G with the following properties: G is of cardinal number m, has no elements of infinite height, and does not admit direct decompositions in which the cardinal numbers of all the direct summands do not exceed a certain m' less than m. Moreover, Kulikov [2] has made a certain survey of primary groups without elements of infinite height which, while not amounting to a complete classification, is nevertheless sufficient to show that it is impossible to extend Prüfer's second theorem to non-countable groups. The present section is devoted to an exposition of this theory of Kulikov.

A subgroup B of a primary abelian group G is called a *basic subgroup* if it is a serving subgroup of G and a direct sum of cyclic groups and if the factor group G/B is a complete group. Thus in every complete primary group the only basic subgroup is the null subgroup. On the other hand, if G is a direct sum of p-primary cyclic groups, then G is a basic subgroup of itself and, if the orders of the elements are bounded, is the only one.

Every primary abelian group G possesses basic subgroups.

By the above remark on basic subgroups of complete groups we can assume that G is not complete. G has, therefore (see § 24), elements of

order p and of finite height which by the lemma at the end of the preceding section are contained in cyclic direct summands. Thus G has serving subgroups with elements of bounded orders. It follows from this and from the result at the beginning of § 25 that we can find in G an ascending sequence of subgroups

$$B_1 \subseteq B_2 \subseteq \ldots \subseteq B_n \subseteq \ldots \tag{1}$$

with the following properties:

1) Every B_n, $n = 1, 2, \ldots$, is a serving subgroup of G.
2) The orders of the elements of B_n do not exceed p^n.
3) B_n cannot be embedded in a larger subgroup with the properties 1) and 2).

We denote the union of the sequence (1) by B. This is a serving subgroup of G, because it is the union of an ascending sequence of serving subgroups. Moreover, by Kulikov's criterion (§ 24) B is a direct sum of cyclic groups. Since each B_n is a serving subgroup, $n = 1, 2, \ldots$, and the orders of its elements are bounded, the heights of all its elements are also bounded and finite.

We show now that the factor group G/B is complete. We know from § 24 that it is sufficient to show that every coset $x + B$ of order p has infinite height in G/B. By assumption, we have $px \in B$. But since B is a serving subgroup, it contains an element b such that $pb = px$ or $p(x - b) = 0$. We can therefore assume that x itself has order p in G, that is, $px = 0$.

Now B_n, $n = 1, 2, \ldots$, is a serving subgroup of G, and the orders of its elements do not exceed p^n. By what we have proved in the preceding section there exists a direct decomposition

$$G = B_n + C_n, \quad n = 1, 2, \ldots. \tag{2}$$

Accordingly x decomposes into

$$x = y + z,$$

where $y \in B_n$, $z \in C_n$. z is not the null element, since x is not contained in B; the order of z is therefore p. The height of z in G is not less than n. For otherwise, by the lemma of the preceding section, z is contained in a cyclic direct summand of C_n whose order does not exceed p^n; but by (2) this contradicts property 3) of B_n. The element $z = x - y$ is, however, con-

tained in the coset $x + B$. This coset therefore contains elements of arbitrarily large height, so that $x + B$ has infinite height in G/B.

This proves that B is a basic subgroup of G.

Any two basic subgroups of a primary abelian group G are isomorphic.

Let B be an arbitrary basic subgroup of G. We know from § 24 that all decompositions of B into a direct sum of cyclic groups are isomorphic. The cardinal number of the summands of order p^k, $k = 1, 2, \ldots$ in any such decomposition is obviously equal to the number of cyclic direct summands of the same order p^k in a decomposition of the factor group B/p^nB, where $n > k$ and p^nB is the subgroup of B that consists of all the elements of B whose height in B is greater than or equal to n. Therefore the theorem follows if we can show that the factor group B/p^nB does not depend, in fact, on the choice of the basic subgroup B.

We denote by p^nG the subgroup of G that consists of all elements whose height in G is greater than or equal to n. Since B is a serving subgroup,

$$B \cap p^nG = p^nB. \tag{3}$$

On the other hand

$$\{B, p^nG\} = G. \tag{4}$$

For if x is an arbitrary element of G, then since G/B is complete there exists an element y in G such that x and p^ny lie in the same coset of B; that is, $x = p^ny + b$, where $b \in B$.

The isomorphism theorem now leads by (3) and (4) to the isomorphism

$$B/p^nB \simeq G/p^nG.$$

Thus, in all basic subgroups B of G the factor groups B/p^nB for given n are isomorphic. This concludes the proof of the theorem.

Let us apply these results to primary groups without elements of infinite height. We see that these groups can be split into disjoint classes such that in one class we have all the groups with isomorphic basic subgroups. Every primary group that is a direct sum of cyclic groups determines a certain class, since it can be considered, for example, as a basic subgroup of itself. *The task of classifying all primary groups without elements of infinite height is therefore reduced to a survey of the groups with a given basic subgroup B.*

For this purpose we introduce a new concept. We take the decomposition of B into the direct sum of cyclic groups and denote by $B^{(n)}$, $n = 1, 2, \ldots$, the direct sum of the summands of order p^n in this decomposition; if there are no summands of that order, we put $B^{(n)} = 0$. We then take the un-

restricted direct sum (in the sense of § 17, end) of all the groups $B^{(n)}$; we call the periodic part of this sum the *closure* of B and denote it by $\bar{B}$. In other words, the elements of $\bar{B}$ are sequences of elements, one from each $B^{(n)}$ such that the orders of all the elements of every such sequence are bounded; addition of sequences is component-wise.

Since all the decompositions of B into the direct sum of cyclic groups are isomorphic, $\bar{B}$ is uniquely determined by B. It is easy to see that $\bar{B}$ is primary and contains no elements of infinite height. B is the subgroup of $\bar{B}$ consisting of those sequences that contain only a finite number of elements different from the null element. Hence a group B is equal to its closure $\bar{B}$ if and only if the orders of the elements of B are bounded, since it is precisely in this case that there are only finitely many groups $B^{(n)}$ different from the null group.

B is a basic subgroup of its closure.

The fact that B is a direct sum of cyclic groups is part of our assumption. To show that B is a serving subgroup of $\bar{B}$ we note that the sum $C^{(n)} = B' + B'' + \ldots + B^{(n)}$, $n = 1, 2, \ldots$ is a direct summand of $\bar{B}$—the complementary summand is the subgroup consisting of those sequences whose first n components are null elements. Therefore B, as the union of the ascending sequence of serving subgroups $C^{(n)}$ of $\bar{B}$, is itself a serving subgroup of $\bar{B}$. We show, finally, that the factor group $\bar{B}/B$ is complete. If $x = (x_1, x_2, \ldots, x_n, \ldots)$ is an arbitrary element of $\bar{B}$ then, since the orders of its components are bounded, for each k we can find an N such that for all $n \geqq N$ the height of x_n in $B^{(n)}$ is not less than k. Hence it follows that the height of $x' = (0, \ldots, 0, x_N, x_{N+1}, \ldots)$ in $\bar{B}$ is also not less than k. But x' belongs to the coset $x + B$. This coset therefore contains elements of arbitrarily large height, and so its height in the factor group $\bar{B}/B$ is infinite.

We can now prove that *there exist primary groups without elements of infinite height that are not direct sums of cyclic groups.*

Let B be a countable primary group (and therefore the direct sum of cyclic groups) having elements of arbitrarily large order. Its closure $\bar{B}$ therefore has the cardinal number of the continuum. $\bar{B}$ cannot be the direct sum of cyclic groups, since it would then contain two non-isomorphic basic subgroups—$\bar{B}$ itself and B—in contradiction to the above theorem on the isomorphism of all basic subgroups of a given primary group.

All primary abelian groups without elements of infinite height whose basic subgroups are isomorphic to B are certain subgroups of the closure $\bar{B}$ of B, namely those that contain B and whose images in the factor group $\bar{B}/B$ are complete subgroups.

For let C/B be an arbitrary complete subgroup of $\bar{B}/B$. As a subgroup of $\bar{B}$, C is primary and without elements of infinite height and B is contained in C as a basic subgroup: for B is a serving subgroup of $\bar{B}$, and therefore of C, and C/B is by hypothesis complete. So we see that C belongs to the class of groups we have to study.

Now let G be an arbitrary primary group without elements of infinite height whose basic subgroups are isomorphic to B. We select one of these basic subgroups and denote it by B_0. We know that B has a direct decomposition

$$B = \sum_{n=1}^{\infty} B^{(n)},$$

where $B^{(n)}$ is a direct sum of cyclic groups or order p^n. Hence

$$B_0 = \sum_{n=1}^{\infty} B_0^{(n)},$$

with $B_0^{(n)} \simeq B^{(n)}$. We introduce the notation

$$D^{(k)} = \sum_{n>k} B_0^{(n)},$$

so that

$$B_0 = B_0^1 + B_0^2 + \ldots + B_0^{(k)} + D^{(k)},$$

and

$$G^{(k)} = \{D^{(k)},\ p^k G\},$$

where $p^k G$, is, as before, the subgroup consisting of all those elements of G whose height in G is not less than k. We have shown above (see equation (4)) that for all k, $k = 1, 2, \ldots$ we have

$$G = \{B_0,\ p^k G\};$$

therefore

$$G = \{B_0^1 + B_0^2 + \ldots + B_0^{(k)},\ G^{(k)}\}.$$

Let x be an element in the intersection of $B_0^1 + B_0^2 + \ldots + B_0^{(k)}$ and $G^{(k)}$. As an element of the second subgroup it has the form $x = y + z$, where $y \in D^{(k)}$, $z \in p^k G$. Since the elements x and y belong to B_0, $z = x - y$ is also an element of B_0. The height of z in G is not less than k; so is its height in B_0, since B_0 is a serving subgroup of G. However, all the elements of B_0 whose height in B_0 is not less than k belong to $D^{(k)}$. Therefore x, as the sum of two elements of $D^{(k)}$, is also contained in $D^{(k)}$, and since x belongs to $B_0^1 + B_0^2 + \ldots + B_0^{(k)}$, it is the null element.

This shows that we have the direct decomposition

$$G = B_0^1 + B_0^2 + \ldots + B_0^{(k)} + G^{(k)}, \quad k = 1, 2, \ldots; \tag{5}$$

moreover, since $G^{(k)}$ contains both $B_0^{(k+1)}$ and $G^{(k+1)}$ as subgroups, we also have

$$G^{(k)} = B_0^{(k+1)} + G^{(k+1)}, \quad k = 1, 2, \ldots;$$

in other words, the direct decompositions (5) are successive refinements of one another by means of a decomposition of the last summand. It follows that a given element x of G has one and the same component in the direct summand $B_0^{(n)}$ of every decomposition (5) for $k = n, n+1, \ldots$; we denote this component by x_n.

By setting up a correspondence between each element x of G and the sequence $(x_1, x_2, \ldots, x_n, \ldots)$ of its components we obviously obtain a homomorphic mapping of G into the closure $\bar{B}$ of B—the orders of the components x_n do not exceed the order of x; that is, the sequence of components is, in fact, contained in $\bar{B}$. This mapping is even an isomorphism: for an element x that is mapped into the null sequence must lie in $G^{(k)}$ for $k = 1, 2, \ldots$, so that it has infinite height in G. But since G has no such elements other than the null element, we see that $x = 0$. In this isomorphic mapping of G onto a subgroup C of $\bar{B}$, B_0 is mapped onto B: it is precisely the elements of B_0 that correspond to sequences of components with only a finite number of elements other than the null element, and every such sequence corresponds to some element of B_0. Since G/B_0 is complete it follows, finally, that C/B is complete. This concludes the proof of the theorem.

It should be noted that in the course of the proof the construction of the subgroup C of $\bar{B}$ onto which G is mapped isomorphically depends on the choice of the basic subgroup B_0 of G. It is still an open question what the conditions are to which we must subject the complete subgroups C/B and C'/B of $\bar{B}/B$ to ensure that the corresponding subgroups C and C' of $\bar{B}$ be isomorphic.

A number of further properties of primary groups that are closures of direct sums of cyclic groups can be found in the paper by Kulikov [2]. See also a paper by Kaloujnine [8].

§ 27. Ulm factors. The existence theorem

We now proceed to the study of primary abelian groups with elements of nfinite height. One must not think that such a group necessarily contains a complete subgroup: if a is an element of infinite height in a group G, then the elements $b_n, n = 1, 2, \ldots$, satisfying the equations $p^n b_n = a$ by no means have to lie in a single subgroup of type p^∞ The main theorem of the present section will show that the structure of reduced primary groups is, even in the countable case, much more complicated than that of primary groups without elements of infinite height. The restriction to reduced groups to which we shall adhere in the following is justified by the results of § 23.

Since the sum and difference of two elements of infinite height in a primary group G also have infinite height in G, the set of all elements of infinite height in G is a subgroup which will be denoted by G^1. We denote by G^2 the subgroup consisting of all the elements of infinite height in G^1. More generally, if we have already defined subgroups G^α of G for all ordinal numbers α less than β (such that they form a descending sequence), then we take as G^β the subgroup consisting of all elements of infinite height in $G^{\beta-1}$ if β is not a limit number, and the intersection of all subgroups G_α, $\alpha < \beta$, if β is a limit number.

We obtain a descending sequence of subgroups of G

$$G = G^0 \supset G^1 \supset \ldots \supset G^\alpha \supset \ldots,$$

which must become stationary at a certain index γ. More accurately, there exists an ordinal number γ whose cardinal number does not exceed the cardinal number of G itself such that $G^\gamma = G^{\gamma+1}$, and therefore $G^\gamma = G^\delta$, for all $\delta > \gamma$. The equation $G^\gamma = G^{\gamma+1}$ shows, however, that all the elements of G^γ have infinite height in G^γ, so that G^γ is complete. Since we have assumed that G is reduced, G^γ must be the null group.

Let τ be the first ordinal number for which $G^\tau = \mathbf{0}$. τ is called the *type* of the reduced group G. Groups that contain no elements of infinite height have type 1.

If G is a reduced primary group of type τ, then for all α less than τ we form the factor groups

$$\bar{G}^\alpha = G^\alpha / G^{\alpha+1}.$$

The sequence

$$\bar{G}^0, \ \bar{G}^1, \ \ldots, \ \bar{G}^\alpha, \ \ldots, \ \alpha < \tau,$$

is called the *sequence of Ulm factors* of G. From the construction of this sequence it is clear that it is completely determined by G itself and that the sequence of Ulm factors of G^α, $\alpha < \tau$, is

$$\overline{G}^\alpha,\ \overline{G}^{\alpha+1},\ \ldots,\ \overline{G}^\beta,\ \ldots,\ \alpha \leqq \beta < \tau.$$

The significance of the Ulm factors for the theory of primary groups will become apparent later, particularly in the following section.

In establishing the simplest properties of the Ulm factors of a primary group we shall make use of the following remark. Let the primary group G be mapped homomorphically onto a primary group H such that the subgroup A of G that is mapped onto the null element of H consists entirely of elements of infinite height in G. Then *the image of every element of infinite height in G is of infinite height in H*; conversely *every inverse image of an element of infinite height in H is an element of infinite height in G*. The first statement follows immediately from the definition of a homomorphic mapping; we prove the second. Let h be an element of infinite height in H and g one of its inverse images in G. If $p^n h' = h$, $h' \in H$, and if g' is one of the inverse images of h' in G, then

$$p^n g' = g + a, \quad a \in A.$$

By our assumption on A there exists an element b in G such that $p^n b = a$. Hence

$$p^n(g' - b) = g,$$

which shows that g has infinite height in G.

It follows, in particular, that *all Ulm factors of a primary group G are groups without elements of infinite height.* To see this we need only apply this remark to the natural homomorphism of G^α onto the factor group $G^\alpha/G^{\alpha+1} = \overline{G}^\alpha$.

We shall now prove that the group $F^\sigma = G/G^\sigma$, $\sigma \leqq \tau$, is a primary group of type σ and that its sequence of Ulm factors is

$$\overline{G}^0,\ \overline{G}^1,\ \ldots,\ \overline{G}^\alpha,\ \ldots,\ \alpha < \sigma.$$

We consider the natural homomorphic mapping of G onto F. From the above remark it follows that in this homomorphism G^1 is mapped onto F^1, and since $G^1 \supseteq G^\sigma$, the factor group $G/G^1 = \overline{G}^0$ and $F/F^1 = \overline{F}^0$ are isomorphic by the theorem on the correspondence between subgroups in homomorphic mappings. Suppose now that we have already proved for all α

less than β that G^α is mapped onto F^α in this homomorphism. If $\beta - 1$ exists, then, as above, we obtain that G^β is mapped onto F^β and that $\overline{G}^{\beta-1} \simeq \overline{F}^{\beta-1}$. If, however, β is a limit number, G^β is again mapped onto F^β, because the former is the intersection of all subgroups G^α, $\alpha < \beta$, the latter the intersection of their images.

If a primary group G is the direct sum of groups H_ν, $G = \sum_\nu H_\nu$, then for every α less than the type of G we have

$$\overline{G}^\alpha \simeq \sum_\nu \overline{H}_\nu^\alpha.$$

Here we have of course put $\overline{H}_\nu^\alpha = 0$, if α exceeds the type of H_ν.

We shall prove that for every β the subgroup G^β is the sum (and clearly the direct sum) of all subgroups H_ν^β. This will be assumed to hold for all α less than β (it is true for $\beta = 0$). If $\beta - 1$ exists, then $G^{\beta-1} = \sum_\nu H_\nu^{\beta-1}$, and therefore every element of H_ν^β has infinite height in $G^{\beta-1}$, so that $G^\beta \supseteq \sum H_\nu^\beta$; on the other hand, if g is an arbitrary element of infinite height in $G^{\beta-1}$ and $g = \sum_\nu h_\nu$, $h_\nu \in H_\nu^{\beta-1}$ then every h_ν must have infinite height in $H_\nu^{\beta-1}$, and hence $G^\beta \subseteq \sum H_\nu^\beta$. Therefore $G^\beta = \sum_\nu H_\nu^{\beta-1}$, and as an easy consequence of the definition of a direct sum

$$\overline{G}^{\beta-1} = G^{\beta-1}/G^\beta \simeq \sum_\nu H_\nu^{\beta-1}/H_\nu^\beta = \sum_\nu \overline{H}_\nu^{\beta-1}.$$

If, however, β is a limit number, then the assertion follows from the fact that G^β is the intersection of all G^α, $\alpha < \beta$.

So far we have started from the definition of the type of a primary group and of its Ulm factors, and we have not been interested in the question whether every ordinal number can occur as the type of some primary group or whether it happens, for instance, that the sequence of subgroups $G \supset G^1 \supset \ldots \supset G^\alpha \supset \ldots$ always breaks off at a finite place. Also, we do not know what the conditions are to which a sequence of primary groups without elements of infinite height must be subjected if it is to be the sequence of Ulm factors of some primary group. A complete answer to these questions has been given by Kulikov. It is very complicated, however, and we restrict ourselves from now on to the consideration of *countable* primary groups.

If G is a reduced primary group, then we know that its type τ has a finite or countable cardinal number. The Ulm factors of the group are countable primary groups without elements of infinite height and therefore, by Prüfer's

Second Theorem, direct sums of cyclic groups. We can say, further, (and the countability of the group does not play any rôle here) that *the orders of the elements in all Ulm factors* $\bar{G}^\alpha$, *except possibly* $\bar{G}^{\tau-1}$ *if* $\tau - 1$ *exists, are not bounded.* For if $\alpha < \tau - 1$, then $G^{\alpha+1} \neq 0$ and we can therefore find an element that has finite height in $G^{\alpha+1}$ but infinite height in G^α.

Now it turns out that this necessary property of the Ulm factors is also sufficient in the countable case; this is brought out by the following theorem (see[1] Zippin [1]):

EXISTENCE THEOREM. *Suppose that* τ *is an ordinal number of an at most countable cardinal number and that for each* α, $0 \leqq \alpha < \tau$, *a countable primary group* A_α *without elements of infinite height is given such that for all* α *except, possibly,* $\alpha = \tau - 1$ *(if* τ *is not a limit number)* A_α *contains elements of arbitrarily large order. Then there exists a countable reduced primary group of type* τ *for which the sequence*

$$A_0,\ A_1,\ A_2,\ \ldots,\ A_\alpha,\ \ldots, \qquad \alpha < \tau,$$

is the sequence of Ulm factors.

Proof. Every group A_α is, by Prüfer's Second Theorem, a direct sum of cyclic groups. Let the generators of these cyclic groups be

$$a_{\alpha 1},\ a_{\alpha 2},\ \ldots,\ a_{\alpha i},\ \ldots,$$

where $a_{\alpha i}$ has the order $p^{n_{\alpha i}}$. We define a group G in the following way: its generators are elements $c_{\alpha i}$, in one-to-one correspondence with the elements $a_{\alpha i}$ (α assumes all values less that τ). With every $c_{\alpha i}$ we associate either the equation $p^{n_{\alpha i}} c_{\alpha i} = 0$, or an equation $p^{n_{\alpha i}} c_{\alpha i} = c_{\beta j}$, where $\beta > \alpha$, and the system of relations so obtained together with the relations of commutatively shall form a system of defining relations for G. In addition we require that the following conditions be satisfied:

1) Let an element $c_{\alpha i}$ be given; if the relation associated with it is $p^{n_{\alpha i}} c_{\alpha i} = c_{\alpha_1 i_1}$ and that associated with $c_{\alpha_1 i_1}$ is $p^{n_{\alpha_1 i_1}} c_{\alpha_1 i_1} = c_{\alpha_2 i_2}$ and so on, then after a finite number of steps we shall reach an element $c_{\alpha_k i_k}$, whose associated relation is of the form $p^{n_{\alpha_k i_k}} c_{\alpha_k i_k} = 0$.

2) If there are given: an element $c_{\beta j}$, $\beta > 0$, an ordinal number γ, less than β, and a natural number N, then there shall exist an element $c_{\alpha i}$ such that $\gamma \leqq \alpha < \beta$, $n_{\alpha i} > N$ and that the relation associated with it has the form $p^{n_{\alpha i}} c_{\alpha i} = c_{\beta j}$.

[1] The paper by Zippin contains only a sketch of a complete proof of the theorem.

3) If τ is a limit number, then for every γ less than τ and every natural number N there shall exist an element $c_{\alpha i}$ such that $\gamma < \alpha$, $n_{\alpha i} > N$ and that the relation associated with it has the form $p^{n_{\alpha i}} c_{\alpha i} = 0$.

We shall show that a system of equations satisfying these three conditions actually exists and that the group G so defined satisfies the conditions of the theorem. The proof is by induction over the ordinal number τ. For $\tau = 1$, G is given by the generators $c_{01}, c_{02}, \ldots, c_{0i}, \ldots$ and the relations $p^{n_{0i}} c_{0i} = 0$; that is, conditions 1)-3) are satisfied and the group itself is isomorphic to A_0.

Let us suppose at first that $\tau - 1$ exists. Let G' be the group of type $\tau - 1$ having the sequence

$$A_0, A_1, A_2, \ldots, A_\alpha, \ldots, \quad \alpha < \tau - 1,$$

as the sequence of its Ulm factors; this group is given by the generators $c_{\alpha i}$, $\alpha < \tau - 1$, and the relations of the above type associated with these generators, and conditions 1)-3) as well, are satisfied. We now define G as follows: If the relation associated with $c_{\alpha i}$, $\alpha < \tau - 1$ in G' is $p^{n_{\alpha i}} c_{\alpha i} = c_{\beta j}$, $\beta < \tau - 1$, then the same relation shall be associated with $c_{\alpha i}$ in G. But if the relation in G' is $p^{n_{\alpha i}} c_{\alpha i} = 0$, then it is replaced in G by a relation $p^{n_{\alpha i}} c_{\alpha i} = c_{\tau-1, j}$. It is easy to see that we can arrange this such that condition 2) is satisfied for the elements $c_{\tau-1, i}$; for the set of elements $c_{\tau-1, i}$ is at most countable, and if $\tau - 1$ is a limit number, we can appeal to condition 3), but if $\tau - 1$ is not a limit number, then there exist elements $c_{\tau-2, i}$ with arbitrarily large exponent $n_{\tau-2, i}$, and for all elements $c_{\tau-2, i}$ of G' the associated relations have the form $p^{n_{\tau-2, i}} c_{\tau-2, i} = 0$. Finally, we associate with the elements $c_{\tau-1, i}$ relations $p^{n_{\tau-1, i}} c_{\tau-1, i} = 0$. We obtain a system of defining relations satisfying conditions 1) and 2); condition 3) does not come into play in this case.

The abelian group G we have just constructed is, by 1), primary. We show that *all elements* $c_{\alpha i}$, $\alpha < \tau$, *are different from the null element.* We take an element $c_{\alpha i}$ and write down the relations

$$p^{n_{\alpha i}} c_{\alpha i} = c_{\alpha_1 i_1}, \quad p^{n_{\alpha_1 i_1}} c_{\alpha_1 i_1} = c_{\alpha_2 i_2}, \ldots,$$

$$\ldots, \quad p^{n_{\alpha_k i_k}} c_{\alpha_k i_k} = c_{\tau-1, j}, \quad p^{n_{\tau-1, j}} c_{\tau-1, j} = 0;$$

it follows from our construction that we must be led in this way to one of the elements $c_{\tau-1, j}$. We introduce the notation

$$n_{\alpha i} + n_{\alpha_1 i_1} + \ldots + n_{\alpha_k i_k} + n_{\tau-1, j} = l(\alpha, i).$$

We take, further, a group P of type p^∞ with generators $d_1, d_2, \ldots, d_n, \ldots$ and relations

$$pd_1 = 0, \quad pd_n = d_{n-1}, \quad n = 2, 3, \ldots .$$

If we now set up a correspondence between the element $c_{\alpha i}$ of G and the element $d_{l(\alpha,i)}$ of P, then all the defining relations of G are satisfied in P and all the elements $c_{\alpha i}$ correspond in P to elements other than the null element. This shows that from the defining relations of G it cannot be deduced that any $c_{\alpha i}$ is the null element. Moreover, we see that the order of $c_{\alpha i}$ in G is $p^{l(\alpha,i)}$.

We are now in a position to state by induction on α and by applying 2) that every element $c_{\alpha i}$ is contained in G^α, the subgroup of G defined as at the beginning of the present section. In particular, all elements $c_{\tau-1,i}$ belong to $G^{\tau-1}$. If F is the subgroup of G that is generated by all elements $c_{\tau-1,i}$, then the factor group G/F is isomorphic to G'. Since G' is of type $\tau-1$, it follows that there are no elements in G belonging to $G^{\tau-1}$ but outside F, so that $F = G^{\tau-1}$. Therefore it follows that $\overline{G}^\alpha \simeq \overline{G}'^\alpha \simeq A_\alpha$, $\alpha < \tau - 1$. As to $G^{\tau-1}$, this is the direct sum of the cyclic groups $\{c_{\tau-1,i}\}$ and is therefore isomorphic to $A_{\tau-1}$. This follows from the fact that the defining relations exhibit G itself as the direct sum of subgroups each of which is generated by all those $c_{\alpha i}$ whose cyclic subgroups contain a fixed element $c_{\tau-1,j}$. G therefore satisfies all the requirements of the theorem.

Now let τ be a limit number. Every group A_α, $0 \leqq \alpha < \tau$, is the direct sum of cyclic groups with unbounded orders. This enables us to split A_α into the direct sum of a countable set of subgroups each of which contains elements of arbitrarily high orders. Let this decomposition be

$$A_\alpha = A_{\alpha\alpha} + A_{\alpha,\alpha+1} + \ldots + A_{\alpha\sigma} + \ldots, \quad \alpha \leqq \sigma < \tau.^1$$

By induction hypothesis there exists a group H_α of type $\alpha + 1$, with

$$A_{0\alpha}, \ A_{1\alpha}, \ A_{2\alpha}, \ \ldots, \ A_{\alpha\alpha}$$

as its sequence of Ulm factors. We know already that the direct sum of all groups H_α, $0 \leqq \alpha < \tau$ will satisfy all the requirements of the theorem. The system of generators $c_{\alpha i}$ of this direct sum is obtained as the union of the corresponding systems of generators of the groups H_α, while the relations corresponding to them in these groups are preserved. Conditions 1)

[1] This choice of indices is obviously at our disposal.

and 2) are obviously satisfied. Condition 3) is also satisfied, since every subgroup $A_{a\alpha}$, $0 \leqq \alpha < \tau$, contains elements of arbitrarily high orders.

This concludes the proof of the theorem.

§ 28. Ulm's Theorem

The main theorem of the preceding section tells us what an enormous variety of reduced primary groups exist, even in the countable case: an arbitrary ordinal with a countable cardinal number can be chosen as the type of such a group, and an arbitrary sequence of countable primary groups without elements of infinite height (with only one quite natural restriction) as the sequence of its Ulm factors. The type and the Ulm factors of a group can be used, in fact, not only for the construction of the wide variety of groups under consideration but also for their complete classification. This is the content of the following theorem.

Ulm's Theorem. *If two countable reduced primary groups A and B have the same type τ, and if for each α less than τ their Ulm factors $\bar{A}_\alpha$ and $\bar{B}_\alpha$ are isomorphic, then A and B are isomorphic.*

This theorem was first proved by Ulm [1] by means of the theory of infinite matrices and then by Zippin [1] by group-theoretical methods.[9] The theorem states that a countable reduced primary group is completely determined by its type and the sequence of its Ulm factors; since, by Prüfer's Second Theorem, every Ulm factor in the countable case is a direct sum of cyclic groups and therefore completely determined by the number of cyclic direct summands of order p^n (for all n), we can give every countable primary group by a system of numerical invariants. Naturally these systems of invariants turn out to be more complicated than those of finitely generated abelian groups.

Let

$$A = A^0 \supset A^1 \supset A^2 \supset \ldots \supset A^\alpha \supset \ldots \supset A^\tau = 0$$

be the sequence of subgroups of A defined as in the preceding section: if $\alpha - 1$ exists, then A^α is the subgroup of all elements of infinite height in $A^{\alpha-1}$, and if α is a limit number, then A^α is the intersection of all A^β, $\beta < \alpha$. Similarly we construct the sequence

$$B = B^0 \supset B^1 \supset B^2 \supset \ldots \supset B^\alpha \supset \ldots \supset B^\tau = 0.$$

An element a of A is said to be *of type* α if it is contained in A^α but not in

$A^{\alpha+1}$. Every element of A has a certain type: if a given element is contained in all A^β, where β is less than a limit number α, then it is also contained in their intersection, that is, in A^α.

Let X be a subgroup of A and $\alpha < \tau$. The intersection $X \cap A^\alpha$ is a subgroup of A^α. Suppose that in the natural homomorphism of A^α onto the Ulm factor $\bar{A}^\alpha = A^\alpha/A^{\alpha+1}$ this intersection is mapped onto the subgroup $\bar{A}^\alpha_X$ of $\bar{A}^\alpha$. X is called a *perfect* subgroup of A if $\bar{A}^\alpha_X$ is for each α a serving subgroup of $\bar{A}^\alpha$. (For the definition of a serving subgroup see § 25.)

The definition of the type of an element and of a perfect subgroup carry over to B, of course.

Finally we introduce the following definition: Let $X \subset A$ and $Y \subset B$ be isomorphic subgroups. An isomorphism φ between X and Y is called *type preserving* if the elements of X and Y that correspond under φ have the same type in A and B, respectively.

The main tool in the proof of Ulm's theorem is the following lemma.

LEMMA. *Let φ be a type-preserving isomorphism between two finite perfect subgroups X of A and Y of B, and let a be an element of A, not contained in X. Then we can find a finite perfect subgroup $\overline{X}$ of A, containing X and a, and a finite perfect subgroup $\overline{Y}$ of B, containing Y, such that $\overline{X}$ and $\overline{Y}$ are isomorphic and that the isomorphism $\bar{\varphi}$ between them can be chosen as type preserving and as an extension of φ.*[1]

We remark, first of all, that it is sufficient to consider the case when $pa \in X$; if $p^n a \in X$, but $p^{n-1}a \notin X$, $n > 1$, then we can adjoin the elements $p^{n-1}a, p^{n-2}a, \ldots, pa, a$ in succession and so reduce it to the special case.

Let λ be the highest type among the elements of the coset $X + a$; it exists, because $X + a$ has only a finite number of elements. Among all elements of type λ in $X + a$ let $a' = x_0 + a$ be one of greatest height in A^λ. If the height of a' in A^λ is $n - 1$ and if $a' = p^{n-1}\bar{a}$, where $\bar{a} \in A^\lambda$, then we put

$$\overline{X} = \{X, \bar{a}\}.$$

Then $\overline{X}$ is a finite subgroup and contains X as well as the element $a = a' - x_0$. We show that $\overline{X}$ *is a perfect subgroup of* A.

Since $p^n \bar{a} \in A$, every element of $\overline{X}$ has the form $\bar{x} = x + k\bar{a}$, where $x \in X$, $0 \leqq k < p^n$. If $\bar{x}$ is an element of type α and of height h in A^α

$$\bar{x} = x + k\bar{a} = p^h c, \quad c \in A^\alpha, \tag{1}$$

then the element $A^{\alpha+1} + \bar{x}$ of the factor group $A^\alpha/A^{\alpha+1} = \bar{A}^\alpha$ is also of

[1] Cf. p. 168.

height h (by the definition of $A^{\alpha+1}$). We have to show that we can find in $\overline{X}$ an element $\bar{x}'$ of type α such that

$$p^h(A^{\alpha+1}+\bar{x}')=A^{\alpha+1}+\bar{x}.$$

For $k=0$ and also for $\alpha<\lambda$ we have $k\bar{a}\in A^{\alpha+1}$. In these two cases the assertion follows from the fact that X is a perfect subgroup of A. If $\alpha=\lambda$ and k is divisible by p^h, $k=p^hk'$, then we have by (1) $x=p^h(c-k'\bar{a})$. Since $c-k'\bar{a}\in A^\lambda$ and X is perfect, it follows now that there exists an element x' in $A^\lambda\cap X$ such that

$$A^{\lambda+1}+x=p^h(A^{\lambda+1}+x');$$

hence

$$A^{\lambda+1}+\bar{x}=p^h(A^{\lambda+1}+x'+k'\bar{a}),$$

where obviously $x'+k'\bar{a}\in A^\lambda\cap\overline{X}$.

We now show that in all other cases (1) contradicts the choice of a'.

Let p^j be the highest power of p that divides k, $k=p^jk'$; since $k<p^n$, we have $j\leqq n-1$. k' and p are co-prime; therefore there exist integers m and l, $0<l<p$, such that $k'l=1+mp$. Multiplying both sides of (1) by lp^{n-j-1}, we obtain

$$lp^{n-j-1}x+p^{n-1}\bar{a}+p^nm\bar{a}=p^{n+h-j-1}(lc),$$

and from $p^n\bar{a}\in X$ it follows that

$$lp^{n-j-1}x+p^nm\bar{a}=x'\in X;$$

hence with $p^{n-1}\bar{a}=a'$ and $lc=c'\in A^\alpha$

$$x'+a'=p^{n+h-j-1}c'.$$

If now $\alpha>\lambda$, then it follows from $x'+a'\in A^\alpha$ that we can find in the coset $X+a'=X+a$ an element of type greater than λ, which contradicts the condition imposed on a'. If $\alpha=\lambda$ but k is not divisible by p^h, then $j\leqq h-1$; hence $n+h-j-1\geqq n$. We have therefore found in $X+a$ an element of type λ whose height in A^λ is greater than that of a', namely $n-1$, which again contradicts the choice of a'. This proves that $\overline{X}$ is a perfect subgroup.

We know that $p^n\bar{a}$ is an element of X and that its type is not less than λ. Since X is a perfect subgroup, we can find in it an element x_1, of type λ or equal to the null element, and an element x_2, of type not less than $\lambda+1$, such that

$$p^n\bar{a} = p^n x_1 + x_2.$$

If $\bar{\bar{a}} = \bar{a} - x_1$, then

$$p^n\bar{\bar{a}} = x_2, \qquad x_2 \in A^{\lambda+1}, \tag{2}$$

and again $\bar{X} = \{X, \bar{\bar{a}}\}$. All elements $k\bar{\bar{a}}, 0 < k < p^n$, lie outside X. We know, further, that the types of all elements of $\bar{X}$ outside X do not exceed λ, because we have proved above that for $k \neq 0$ and for $\alpha > \lambda$ equation (1) cannot hold. It follows that $\bar{A}^{\lambda}_{\bar{X}}$ is the direct sum of $\bar{A}^{\lambda}_{X}$ and of the cyclic subgroup of order p^n that is generated in $\bar{A}^{\lambda}$ by the element $\bar{\bar{a}} + A^{\lambda+1}$. The finite subgroup $\bar{A}^{\lambda}_{X}$ is a serving subgroup of the Ulm factor $\bar{A}^{\lambda}$, because $\bar{X}$ is perfect, and is, by a result of § 25, a direct summand of $\bar{A}_{\lambda}$. $\bar{A}^{\lambda}_{X}$ is also a direct summand of $\bar{A}^{\lambda}$ and we have shown, moreover, that $\bar{A}^{\lambda}$ contains a cyclic direct summand of order p^n whose intersection with $\bar{A}^{\lambda}_{X}$ is the null element.

We now proceed to consider B. $\bar{A}^{\lambda}_{X}$ and $\bar{B}^{\lambda}_{Y}$ are isomorphic subgroups, because φ is a type-preserving isomorphism between X and Y. $\bar{B}^{\lambda}_{Y}$, as a finite serving subgroup of B^{λ}, is a direct summand of it, and since by Prüfer's Second Theorem $\bar{B}^{\lambda}$ is a direct sum of cyclic groups and, by assumption, isomorphic to $\bar{A}^{\lambda}$, we can find in $\bar{B}^{\lambda}$ a cyclic direct summand of order p^n whose intersection with $\bar{B}^{\lambda}_{Y}$ is the null element. Let $b + B^{\lambda+1}$ be a generator of this cyclic subgroup. Then b is an element of type λ in B, and $p^n b \in B^{\lambda+1}$ If y_2 is the element corresponding to x_2 under φ, then $y_2 \in B^{\lambda+1}$ and B^{λ} contains an element b_0 such that $p^{n+1}b_0 = y_2 - p^n b$. Using the notation $\bar{b} = b + p b_0$, we have

$$p^n\bar{b} = y_2 \tag{3}$$

and we put

$$\bar{Y} = \{Y, b\}.$$

Note that $p^{n-1}\bar{b} \notin Y$. For from $p^{n-1}\bar{b} = y_0$, $y_0 \in Y$, it would follow that

$$y_0 - p^{n-1}b = p^n b_0.$$

On transition to B^{λ} this would lead to the existence of an element in the direct summand $\bar{B}^{\lambda}_{Y} + \{B^{\lambda+1} + b\}$ whose height in $\bar{B}^{\lambda}$ would be greater than the height of its component in the direct summand $\{B^{\lambda+1} + b\}$, and this is impossible. Hence it follows that $\bar{B}^{\lambda}_{Y}$ and $\{B^{\lambda+1} + \bar{b}\}$ form a direct sum in $\bar{B}^{\lambda}$

From $p^{n-1}b \in Y$ and from equations (2) and (3) and the fact that x_2 and y_2 correspond under φ it follows that $\bar{X}$ *and* $\bar{Y}$ *are isomorphic*: we

obtain an isomorphism $\bar{\varphi}$ between these subgroups if we map X onto Y according to φ and the element $\bar{\bar{a}}$ onto $\bar{b}$. The isomorphism $\bar{\varphi}$ extends φ. Moreover, *it is type preserving.* For if two elements $\bar{x}=x+k\bar{\bar{a}}$ and $\bar{y}=y+k\bar{b}$, $0\leqq k<p^n$, correspond under $\bar{\varphi}$, then $x\varphi=y$, so that x and y have equal type; hence $\bar{x}$ and $\bar{y}$ have equal type for $k=0$. But if $k\neq 0$ and the type of x and y is not λ, then $\bar{x}$ and $\bar{y}$ again have the same type, since $k\bar{\bar{a}}$ and $k\bar{b}$ have type λ and the type of a sum of two elements of *different* types is obviously equal to the smaller of the two types. Finally, if $k\neq 0$ and x and y are of type λ, then $\bar{x}$ and $\bar{y}$ are also of type λ, since in $\bar{A}^\lambda$ the subgroup $\bar{A}^\lambda_X$ and $\{A^{\lambda+1}+\bar{\bar{a}}\}$ form a direct sum (just as the subgroups $\bar{B}^\lambda_Y$ and $\{B^{\lambda+1}+\bar{b}\}$ do in $\bar{B}^\lambda$).

It remains to show that $\bar{Y}$ *is a perfect subgroup of* B. This can be done by repeating the reasoning that has been used above for proving that $\bar{X}$ is a perfect subgroup of A, provided that we now take instead of $\bar{a}$ the element $\bar{b}$, and instead of a' the element $p^{n-1}\bar{b}$. For $\bar{b}$ is of height 0 in $\bar{B}^\lambda$ and the types of all elements of the coset $Y+p^{n-1}\bar{b}$ are not higher than the type of $p^{n-1}\bar{b}$, namely λ; finally if we could find an element of type λ in this coset whose height in $\bar{B}^\lambda$ would be greater than $n-1$, then we would obtain a contradiction, because $\bar{B}^\lambda_Y+\{B^{\lambda+1}+b\}$ is a direct summand of $\bar{B}^\lambda$.

The proof of the lemma is now complete.

The proof of Ulm's Theorem now follows without any further difficulty. We enumerate all the elements of A and of B by means of the natural numbers. Then we take the subgroups $X_0=0$ and $Y_0=0$. Suppose that for all k, $0\leqq k\leqq n$, we have already found subgroups $X_k\in A$, $Y_k\in B$, satisfying all the conditions of the lemma, and that for each k, $k=0,1,\ldots,n-1$, the isomorphism φ_k between X_k and Y_k extends the preceding ones. Then we construct subgroups X_n and Y_n on the basis of the lemma, and for odd n we choose a as that element of A outside X_{n-1} which has the smallest suffix, while for even n we proceed similarly with an element of B. So we see that A is the union of the ascending sequence of subgroups

$$X_0\subset X_1\subset\ldots\subset X_n\subset\ldots$$

and B the union of the ascending sequence of subgroups

$$Y_0\subset Y_1\subset\ldots\subset Y_n\subset\ldots,$$

where X_n and Y_n are isomorphic, $n=0,1,\ldots$, and the isomorphism φ_n between them extends φ_{n-1}. Hence A and B are isomorphic. This completes the proof of Ulm's Theorem.

By means of Ulm's Theorem and the existence theorem of the preceding section we can now prove the following theorem (see Baer [5]) which is also of interest for the general theory of direct products.

If G is a countable reduced primary group, then any two direct decompositions of G have isomorphic refinements if and only if G is of type 1.

For if $\tau = 1$, then by Prüfer's Second Theorem G is the direct sum of cyclic groups, so that we need only appeal to results of § 24. If on the other hand $\tau > 1$, then let the Ulm factor G^σ, $0 \leqq \sigma < \tau$, be decomposable into the direct sum of cyclic groups of the following orders:

$$p^{n_{\sigma,1}}, \quad p^{n_{\sigma,2}}, \ldots, \quad p^{n_{\sigma,k}}, \ldots$$

where[1] $n_{\sigma,1} < n_{\sigma,2} < \ldots < n_{\sigma,k} < \ldots$. Let $\bar{G}^\sigma = A_\sigma + B_\sigma$, where A_σ is the direct sum of all cyclic direct summands of orders $p^{n_{\sigma,k}}$ for odd k in the given decomposition of $\bar{G}^\sigma$ while B_σ is their direct sum for even k. Then there exist groups A and B for which $A_0, A_1, \ldots, A_\sigma, \ldots$ and $B_0, B_1, \ldots, B_\sigma, \ldots$ are the sequences of Ulm factors. The Ulm factors of the direct sum $A + B$ coincide with the Ulm factors of G and therefore, by Ulm's Theorem,

$$G \simeq A + B.$$

But there exist also groups $\bar{A}$ and $\bar{B}$ with $B_0, A_1, \ldots, A_\sigma, \ldots$ and $A_0, B_1, \ldots, B_\sigma, \ldots$, as sequences of Ulm factors, and again

$$G \simeq \bar{A} + \bar{B}.$$

That these two direct decompositions of G cannot have isomorphic refinements follows easily from the theorem of the preceding section, which states that the Ulm factors of a direct sum are the direct sums of the corresponding Ulm factors of the summands.

The problem of conditions under which any two direct decompositions of a non-countable reduced primary group have isomorphic refinements is still open: it is not even known whether here the condition $\tau = 1$ is sufficient or necessary. We mention, without proof, a relevant result of Kulikov [2]: if a primary group G is the closure (in the sense of § 26) of a direct sum of cyclic groups, then every pair of direct decompositions of G has isomorphic refinements.

---

[1] Of course, this does not mean that in the decomposition of $\bar{G}^\sigma$ there occurs only one cyclic summand of a given order $p^{n_{\sigma,k}}$.

In conclusion, we consider the problem of an extension of Ulm's theorem to the non-countable case. So far no theorem is known which reduces the study of reduced primary groups of an arbitrary cardinal number to the study of groups without elements of infinite height and which in the countable case goes over into Ulm's Theorem. The theorem that is obtained from Ulm's Theorem by simply omitting the word "countable" is certainly wrong: counter-examples have been found by Kulikov [2]. The groups of these examples have countable type. Below we present a counter-example of a primary reduced group of type 2; this has been communicated to the author by L. Y. Kulikov and is published here for the first time.

KULIKOV'S EXAMPLE. We denote by z_i, $i = 1, 2, \ldots$, a cyclic group of order p^i, and by A the closure of the direct sum of all these cyclic groups (see § 26). Thus, A is the group of sequences of elements, one from each group Z_i, and in every such sequence the orders of all elements are bounded. Let B be the subgroup of A that consists of all those elements of order p in A that have only a finite number of non-null components, and C the subgroup that consists of all those elements of order p that have only a finite number of non-null components with odd indices while the components with even indices are not subject to any restrictions. It is clear that

$$B \subset C \subset A_1,$$

where A_1 is the lowest layer of A.

We shall now prove that *the groups* $H = A/B$ *and* $G = A/C$ *are non-isomorphic reduced primary groups of type* 2 *with isomorphic Ulm factors.*

We put $H^* = A_1/B$ and show that H^* consists of elements of infinite height in H. An arbitrary element h^* of H^* has the form $h^* = a + B$, where a is an element of A of order p; we denote the i-th component of a by z_i. If n is a fixed number, then Z_i, for every $i > n$, contains an element z_i' such that $p^n z_i' = z_i$. We put $z_i' = 0$ for $i \leqq n$. Then

$$z' = (z_1', z_2', \ldots, z_i', \ldots)$$

is an element of A of order p^{n+1}, and $p^n z' - a \in B$, that is, $p^n(z' + B) = h^*$. This shows that h^* has infinite height in H so that

$$H^* \subset H^1, \tag{4}$$

where H^1 is the subgroup of elements of infinite height in H.

Further, from $H = A/B$, $H^* = A_1/B$ there follows the isomorphism

$$H/H^* \simeq A/A_1.$$

However $A/A_1 \simeq pA$, since the mapping $a \to pa$, $a \in A$, is a homomorphism of A onto pA with kernel A_1. Therefore

$$H/H^* \simeq pA. \tag{5}$$

Since pA, like A, contains no element of infinite height, we get from (4) and (5)

$$H^1 = H^*, \tag{6}$$

$$H/H^1 \simeq pA. \tag{7}$$

We have therefore found the Ulm factors of H and have shown, in particular, that *H is a reduced group of type 2.*

Now let us find the Ulm factors of G. If we put $D = C/B$ then, using $G = A/C$, $H = A/B$, we have

$$G \simeq H/D. \tag{8}$$

From $D \subset H^*$ and (6) follows $D \subset H^1$ and therefore from (8)

$$G^1 \simeq H^1/D, \tag{9}$$

where G^1 is the subgroup of elements of infinite height in G: if $h + D$ has infinite height in H/D, then for every n there exist elements $h_n \in H$ and $d_n \in D$ such that $p^n h_n = h + d_n$; d_n has infinite height in H, however, and therefore h also has infinite height.

From (8) and (9) follows

$$G/G^1 \simeq H/H^1. \tag{10}$$

On the other hand H^1 has, by (6), the cardinal number of the continuum and consists of elements of order p. This is also true for G^1: from (9), (6), and the definitions of H^* and D it follows that

$$G^1 \simeq A_1/C;$$

but the factor group A_1/C consists of elements of order p and has the cardinal number of the continuum. By Prüfer's First Theorem we now obtain the isomorphism

$$G^1 \simeq H^1. \tag{11}$$

This shows that *G is a reduced group of type 2* and that *the Ulm factors of G are isomorphic to the corresponding Ulm factors of H.*

It remains to prove that the groups G and H are not isomorphic. Taking into account that $H^1 \subset H_1$, $G^1 \subset G_1$, where H_1 and G_1 are the lowest layers of H and G, respectively, it is sufficient for our purpose to show that *the factor groups H_1/H^1 and G_1/G^1 have different cardinal numbers.*

We know from (6) that $H^1 = A_1/B$. On the other hand, it is easy to see that $H_1 = L/B$, where L is the subgroup of A that consists of all elements of order p and those elements of order p^2 that have only a finite number of non-null components of order p^2. Hence it follows that

$$H_1/H^1 \simeq L/A_1,$$

and *the factor group L/A_1 is countable.*

We now consider the factor group G_1/G^1. First of all,

$$G^1 = A_1/C. \tag{12}$$

For since $D \subset H^1$, the complete inverse image of G^1 in the natural homomorphism of H onto $G \simeq H/D$ is H^1. However, it follows from (6) that A_1 is the complete inverse image of H^1 in the natural homomorphism of A onto $H = A/B$. Hence the complete inverse image of G^1 in the natural homomorphism of A onto $G = A/C$ is A_1; this proves (12).

On the other hand $G_1 = K/C$, where K is the subgroup of A that consists of all elements of order p and those elements of order p^2 that have only a finite number of components of order p^2 with odd indices, while there can be infinitely many components of order p^2 with even indices. Hence it follows from (12) that

$$G_1/G^1 \simeq K/A_1;$$

and *the factor group K/A_1 has the cardinal number of the continuum.*

We conclude that *the groups H and G are not isomorphic.*

§ 29. Mixed abelian groups

A mixed abelian group G is said to *split* if it is the direct sum of a periodic group and a torsion-free group. The periodic summand is then, of course, the periodic part F of G and the torsion-free summand is isomorphic to G/F.

Among the groups that can be split are all direct sums of cyclic groups, in particular, all finitely generated abelian groups, and also all complete

groups. Below we shall show, however, that not all mixed abelian groups can be split.

In view of this result, the fundamental problem in the theory of mixed abelian groups is to find splitting conditions, that is, conditions under which the study of mixed groups reduces to the study of periodic and of torsion-free groups.

In the course of the proof of the following theorem we shall construct some examples of groups that cannot be split.

Let F be a given periodic abelian group. *Every abelian group whose periodic part is isomorphic to F can be split if and only if F is the direct sum of a complete group and a group with elements of bounded orders.*

The following simple proof of the *sufficiency* of this condition is due to Kulikov [1].

Let $F = F_1 + F_2$, where F_1 is a complete group and F_2 a group with elements of bounded orders, and let F be the periodic part of an abelian group G. We have shown in § 23 that the complete group F_1 is a direct summand of G,

$$G = F_1 + G'.$$

The periodic part F' of G' is isomorphic to F_2, that is, its elements are of bounded orders and, since F' is a serving subgroup of G', it is a direct summand of G' by what has been proved in § 25. This shows that G can be split.

We now proceed to show the *necessity* of the condition and first prove the following lemma.

LEMMA. *If a periodic group F is the direct sum of two groups, $F = F' + F''$ and if there exists a group G that has F'' as its periodic part and cannot be split, then the group $H = F' + G$, whose periodic part is F, cannot be split either.*

For if there were a split

$$H = F + H_0 = F' + F'' + H_0,$$

where H_0 is torsion-free, then the factor group H/F', which is isomorphic to G, could also be split.

This lemma permits us to confine ourselves to the case when F is reduced. If we suppose further that the orders of the elements of F are not bounded, then only two cases can arise: either in the decomposition of F into the direct sum of primary groups there occur direct summands in which the

orders of the elements are not bounded, or the number of direct summands is infinite.

In the first case, we can assume by the lemma that F itself is primary. Thus, *let F be a p-primary group containing elements of arbitrarily high orders.* We denote by F_k, $k = 1, 2, \ldots$, the subgroup of F that consists of all elements whose height is not less than k. Further, we choose in F two systems of elements $a_1, a_2, \ldots, a_i, \ldots$ and $b_1, b_2, \ldots, b_i, \ldots$ with the following properties:

1) $b_{i+1} = b_i + p^i a_{i+1}$, $b_1 = a_1$,

2) the orders of the elements b_i increase unboundedly with i,

3) b_i has the smallest order among the elements of its coset with respect to F_i.

We construct these systems of elements in the following way: In one of the cosets of F_1 (but not in F_1) we choose any element of smallest order, say b_1, and put $a_1 = b_1$. Suppose that we have already chosen the elements b_i and a_i and that the order of b_i is p^j. Since F is a reduced group with elements of unbounded order, we can find an element x whose height k is finite and greater than $i + j$. Let y be a solution of the equation $p^k y = x$. We take the element $b_i + p^i y$ and denote by b_{i+1} one of the elements of smallest order in the coset $b_i + p^i y + F_{i+1}$. If

$$b_{i+1} = b_i + p^i y + p^{i+1} f, \quad f \in F,$$

then we put $a_{i+1} = y + pf$, so that $b_{i+1} = b_i + p^i a_{i+1}$. It remains to show that the order of b_{i+1} is greater than the order of b_i. Now from $p^j b_{i+1} = 0$ we would deduce $p^{i+j} y + p^{i+j+1} f = 0$, but since $i + j < k$,

$$p^k y = x = p^{k+1}(-f),$$

which contradicts the fact that the height of x is k.

We now construct an abelian group G. Its system of generators consists of all the elements of F and of a countable set of elements $v_1, v_2, \ldots, v_i, \ldots$, and its defining relations are the relations of commutativity, all the relations that hold between the elements of F and, finally, the relations

$$pv_{i+1} = v_i + a_i, \quad i = 1, 2, \ldots, \tag{1}$$

where the elements a_i are defined as in the preceding paragraph. Every consequence of the relations (1) can be written in the form

$$\sum_{i=1}^{n} k_i (pv_{i+1} - v_i - a_i) = 0, \tag{2}$$

where $n \geqq 1$, k_i are integers, and $k_n \neq 0$. However, the element v_{n+1} has in (2) a non-zero coefficient, and therefore it cannot follow from (1) that some element of F is equal to the null element in G, but not in F. In other words, *F is a subgroup of G.* We see, further, that from (1) there cannot follow a relation $kv_1 = a$, where $k \neq 0$, $a \in F$; that is, the order of v_1 is infinite. G/F is, therefore, a torsion-free group[1] and therefore *F is the maximal periodic subgroup of G.*

Assume now that F is a direct summand of G, so that $G = F + H$. Then $v_i = f_i + h_i$, $f_i \in F$, $h_i \in H$, $i = 1, 2, \ldots$. From (1) it follows, since $a_i \in F$, that

$$pf_{i+1} = f_i + a_i.$$

In particular $pf_2 = f_1 + a_1 = f_1 + b_1$. Suppose we have already proved that

$$p^{i-1}f_i = f_1 + b_{i-1}.$$

Then

$$p^i f_{i+1} = p^{i-1}f_i + p^{i-1}a_i = f_1 + b_{i-1} + p^{i-1}a_i = f_1 + b_i,$$

and since $p^i f_{i+1} \in F_i$ we find that for $i = 1, 2, \ldots$, the elements $-f_1$ and b_i lie in the same coset of F_i. Hence by the definition of b_i it follows that the order of f_1 is not less than that of b_i; but the orders of the elements b_i increase with i, and we obtain a contradiction because f_1 is of finite order. This shows that *F is not a direct summand in G.*

We now come to the second case where we assume that *F is the direct sum of an infinite set of reduced primary groups,* with respect to distinct prime numbers $p_1, p_2, \ldots, p_i, \ldots$

$$F = \sum_i F_{p_i}. \tag{3}$$

In each subgroup F_{p_i} we take an element a_i of zero height and construct an abelian group G in the following way: Its generators are all elements of F and in addition elements $v_0, v_1, \ldots, v_i, \ldots$; the defining relations are the relations of commutativity, all the relations that hold between the elements of F, and finally, the relations

$$p_i v_i = v_0 + a_i, \quad i = 1, 2, \ldots. \tag{4}$$

[1] It is easy to see that it is isomorphic to the group R_p of p-ic fractions, that is, fractions whose denominators are powers of p.

As in the preceding case it is easy to see that F is the maximal periodic subgroup of G.

Let us assume that F is a direct summand of G, so that $G = F + H$. Then $v_i = f_i + h_i$, $f_i \in F$, $h_i \in H$, $i = 0, 1, 2, \ldots$. From (4) it now follows, since $a_i \in F$, that

$$p_i f_i = f_0 + a_i, \quad i = 1, 2, \ldots. \tag{5}$$

Since f_0 is the sum of a finite number of components in the direct summands of the decomposition (3) we can find an index j such that the component of f_0 in F_{p_j} is the null element. If we denote the component of f_j in F_{p_j} by f_j', then (5) for $i = j$ leads to the equation

$$p_j f_j' = a_j,$$

which contradicts the fact that a_j has zero height in F_{p_j}.

This completes the proof of the theorem.

Conditions for a mixed group G to split can also be studied in the form of connections between properties of the periodic part F and of the factor group G/F. This problem has been considered by Baer [13], but he imposes certain restrictions on the torsion-free group G/F; these restrictions are known to be satisfied when this group is countable. The theorem proved above is, in fact, a corollary of the results of Baer. Another approach to the same problem, by way of the properties of the automorphisms of mixed groups, is contained in a paper by Mišina [2]. A criterion for the splitting of a group can be found in a paper by Lyapin [2]. We remark that so far no conditions have been established which a torsion-free group H must satisfy in order that every abelian group having H as the factor group with respect to its periodic part should split.

The problem whether a mixed group can be split must not be confused with the problem whether it can be decomposed. Here we have constructed examples of mixed abelian groups that cannot be split. However *every mixed abelian group G is decomposable into a direct sum* (Kulikov [1]).

For if the periodic part F of G is complete, then F is a direct summand of G. But if F is not complete then we can find, by results of § 25, a cyclic direct summand A of F. Then A is a serving subgroup of F and so is a serving subgroup of G; and since it is a finite group (so that the orders of its elements are bounded) it follows, again from § 25, that A is a direct summand of G.

CHAPTER VIII

TORSION-FREE ABELIAN GROUPS

§ 30. Groups of rank 1. Types of elements of torsion-free groups

Torsion-free abelian groups have been investigated much less thoroughly than primary abelian groups. The concept of the rank of a group (see § 19) is of prime importance, and groups of finite rank emerge as one of the main objects of study. The concept of a serving subgroup also plays a major rôle (see § 25). Other names used in the literature for serving subgroups in torsion-free abelian groups are *isolated*, or *inextensible*, or *closed*, or *division* subgroups.

In a torsion-free abelian group an equation

$$nx = a, \qquad n > 0, \tag{1}$$

cannot have more than one solution, because the difference of two solutions would be an element of finite order. Hence it follows that *H is a serving subgroup of a torsion-free abelian group G if and only if G/H is torsion-free.* From the uniqueness of the solution of (1) it follows that *the intersection of an arbitrary set of serving subgroups of a torsion-free abelian group G is itself a serving subgroup of G.* We can therefore speak of the serving subgroup of G that is *generated* by a given set M of elements of G, namely the intersection of all serving subgroups of G containing M; one such subgroup is known to exist—G itself.

The serving subgroup generated by a set M of a torsion-free group G consists of all elements of G that are linearly dependent (in the sense of § 19) *on the set M.*

For if an element a is linearly dependent on M, that is, if a multiple of a is contained in $\{M\}$, then the serving subgroup generated by M, which clearly contains $\{M\}$, also contains a. On the other hand, all the elements of G that are linearly dependent on M form a subgroup: the sum and difference of any two elements whose multiples lie in M have the same property. This subgroup contains M and is a serving subgroup of G: if $nb = a$ and $ka \in \{M\}$, then $(kn)b \in \{M\}$, that is, b is linearly dependent on M.

We know from § 23 that every abelian group can be embedded in a complete abelian group. We can now state that *every torsion-free abelian group*

can be embedded in a torsion-free complete group, in other words, in the direct sum of a set of groups of type R. This follows easily from the proof of the corresponding theorem of § 23, but can also be established directly: if a torsion-free group G is contained in a mixed complete group H, then the intersection of G with the periodic part of H is the null element, and therefore G is isomorphically mapped into the factor group in H of its periodic part, and this is a complete torsion-free group.

Every abelian torsion-free group G of finite rank n can be embedded in a complete abelian torsion-free group of rank n, that is, in a direct sum of n groups of type R.

For G can be embedded in some complete torsion-free group H. The serving subgroup G of H generated by G is itself complete. Moreover it has been proved above that every element of $\overline{G}$ is linearly dependent on G and therefore linearly dependent on every maximal linearly independent system of elements of G. Thus, the rank of $\overline{G}$ is n.

It follows, in particular, that *every torsion-free group of rank* 1 *is isomorphic to a subgroup of the additive group of rational numbers R.* Therefore, when we obtain a classification of all abelian torsion-free groups of rank 1, which is our next aim, we shall also obtain a classification, to within isomorphism, of all the subgroups of R.

We introduce an auxiliary concept. A *characteristic* is an arbitrary sequence of the form

$$a = (\alpha_1, \alpha_2, \ldots, \alpha_n, \ldots),$$

where each α_n is zero, or a natural number, or the symbol ∞. Two characteristics α and

$$\beta = (\beta_1, \beta_2, \ldots, \beta_n, \ldots)$$

are *equivalent* if $\alpha_n = \beta_n$ for all n except, possibly, a finite number for which both α_n and β_n are distinct from ∞. All characteristics therefore fall into disjoint classes of equivalent characteristics; these classes are called *types*[1] and are denoted by lower-case German letters $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, ...

Into the set of types we introduce a partial order in the following way: $\mathfrak{a} \leqq \mathfrak{b}$ if there exists a characteristic α of type $\mathfrak{a}$ and a characteristic β of type $\mathfrak{b}$ such that for all n we have $\alpha_n \leqq \beta_n$; of course, here we regard the symbol ∞ as greater than every natural number. The reader will have no difficulty in verifying the following statements:

[1] Other names are *overtype* and *genus*.

1) $\mathfrak{a} \leqq \mathfrak{a}$;
2) if $\mathfrak{a} \leqq \mathfrak{b}$ and $\mathfrak{b} \leqq \mathfrak{c}$, then $\mathfrak{a} \leqq \mathfrak{c}$;
3) if $\mathfrak{a} \leqq \mathfrak{b}$ and $\mathfrak{b} \leqq \mathfrak{a}$, then $\mathfrak{a} = \mathfrak{b}$, that is, the two types coincide.

Among all types the greatest is that which consists of the single characteristic

$$(\infty, \infty, \ldots, \infty, \ldots);$$

we shall call it the type R for a reason that will become apparent below. The smallest among all types is the type that contains the characteristic

$$(0, 0, \ldots, 0, \ldots);$$

we shall call it the *null* type.

Let $\mathfrak{a}$ and $\mathfrak{b}$ be two types. We take characteristics α and β in them and put

$$\gamma_n = \min(\alpha_n, \beta_n), \quad n = 1, 2, \ldots.$$

The type $\mathfrak{c}$ defined by the characteristic

$$(\gamma_1, \gamma_2, \ldots, \gamma_n, \ldots)$$

is easily seen to be independent of the choice of the characteristics α and β in $\mathfrak{a}$ and $\mathfrak{b}$. It is the greatest type which is less than, or equal to, both $\mathfrak{a}$ and $\mathfrak{b}$; we call it the *product* of the types $\mathfrak{a}$ and $\mathfrak{b}$, $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$. In a similar way we can speak of the product of any finite number of types.[1]

We can now proceed to *the classification of torsion-free abelian groups of rank* 1. Let $p_1, p_2, \ldots, p_n, \ldots$ be the sequence of all prime numbers in ascending order. Let G be a torsion-free abelian group of rank 1 and a an element of G other than the null element. With G we now associate a characteristic α: we put $\alpha_n = 0$ if $p_n x = a$ has no solution in G, $\alpha_n = k$ if $p_n^k x = a$ has a solution but $p_n^{k+1} x = a$ has no solution in G, and $\alpha_n = \infty$ if all equations $p_n^i x = a$, $i = 1, 2, \ldots$, have solutions in G. It is easy to verify that when a is replaced by ma, where m is a non-zero integer, then there is no change in α_n if it is ∞, but if it is finite and equal to $k \geqq 0$ and $m = p_n^l m'$, $(p_n, m') = 1$, then after the change it will be $\alpha_n = k + l$; in other words, in this case α is replaced by an equivalent characteristic. The same will happen if a is replaced by any other element b of G, except the null element, since a and b have a common multiple. Conversely, if β is a

[1] We could also show that among the types that are greater than, or equal to, the given types $\mathfrak{a}$ and $\mathfrak{b}$ there is a smallest. In other words, the set of types is a lattice (see § 43).

characteristic equivalent to α, then we can replace a by an element b by means of which G is associated with the characteristic β. For if $\alpha_n - \beta_n = \mu_n > 0$ for $n = i_1, i_2, \ldots, i_s$ and $\beta_n - \alpha_n = \nu_n > 0$ for $n = j_1, j_2, \ldots, j_t$, and if $\alpha_n = \beta_n$ for all other n then we can take b as the solution of the equation

$$p_{i_1}^{\mu_1} p_{i_2}^{\mu_2} \ldots p_{i_s}^{\mu_s} x = p_{j_1}^{\nu_1} p_{j_2}^{\nu_2} \ldots p_{j_t}^{\nu_t} a;$$

and it is easy to see that the equation has a solution in G.

So we see that *every abelian torsion-free group of rank* 1 *corresponds uniquely to a well-defined type. Non-isomorphic groups correspond to distinct types.*

For if G is associated with a characteristic α by means of an element a, then the equation $mx = a$ has a solution in G if and only if m is not divisible by a higher power of p_n than the α_n-th for every n for which $\alpha_n < \infty$; if b and c satisfy the equations $pb = a$, $qc = a$ with co-prime p and q, then the equation $(pq)x = a$ is satisfied by $tb + sc$, where $ps + qt = 1$. Therefore the homomorphism of G into the additive group of rational numbers R that carries the element a into the number 1 maps G onto the subgroup R_a of R that consists of all rational numbers whose denominators (in the reduced representation) are not divisible by a power of p_n higher than the α_n-th, $n = 1, 2, \ldots$, if $\alpha_n < \infty$, and by an arbitrary power of p_n if $\alpha_n = \infty$. However, R_a is the unique subgroup of R that contains the integers and has the property that it is associated with the characteristic α by means of the element 1. This shows that G *is determined by the characteristic* α *up to isomorphism.* We also obtain that *for every type* α *we can find a subgroup of* R *associated with it.*

Therefore there exists a one-to-one correspondence between all types and all non-isomorphic torsion-free groups of rank 1. The group R itself corresponds to the type R, which explains the name, the infinite cyclic group corresponds to the null type, and the additive group of p_n-ic fractions (that is, the rational numbers whose denominators are powers of the prime number p_n) to the type that contains the characteristic in which $\alpha_n = \infty$, and $\alpha_m = 0$ for $m \neq n$. We also mention that the additive group of rational numbers with square-free denominators corresponds to the type that contains the characteristic

$$(1, 1, \ldots, 1, \ldots).$$

If a torsion-free group G of rank 1 corresponds to the type α, then we shall say that G *is a group of type* α.

Our classification of groups of rank 1 is succinct and convenient. For example, the reader will easily prove that if G and H are two torsion-free groups of rank 1, of type $\mathfrak{a}$ and $\mathfrak{b}$ respectively, then *G is isomorphic to a subgroup of H if and only if* $\mathfrak{a} \leqq \mathfrak{b}$. It follows that *if each of the two groups G and H is isomorphic to a subgroup of the other, then they are isomorphic.* Our classification also gives an indication of the very great diversity of abelian torsion-free groups of rank 1; it shows, in particular, that the set of all these groups has the cardinal number of the continuum.

We now return to the consideration of arbitrary abelian torsion-free groups. Let G be such a group and let a be one of its elements other than the null element. The serving subgroup A of G that is generated by a is of rank 1, because we have shown above that every one of its elements is linearly dependent on a. This subgroup is, then, the largest subgroup of G of rank 1 containing a. We shall call the type of the subgroup A the *type of the element a*. In other words, the type of a is the type of that characteristic which we obtain when we put $\alpha_n = k$ if $p_n{}^k x = a$ but not $p_n{}^{k+1} = a$ can be solved in G, and $a_n = \infty$ if the equations of the form $p_n{}^k x = a$ can be solved in G for all k; here p_n, $n = 1, 2, \ldots$, is the set of all prime numbers in ascending order. It is in this sense that we shall sometimes speak of the characteristics of an element a of a group G.

We are now in a position to distinguish between elements (other than the null element) of a group G, by means of their types; this corresponds in a certain sense to the division of the elements of a primary abelian group into elements of finite and of infinite height. Torsion-free abelian groups can therefore be classified according to the types of the elements they contain. In particular, we could select as a special object of study the groups in which all elements other than the null element have one and the same type $\mathfrak{a}$. However, a single such restriction is insufficient for the development of a deeper theory. True, it is easy to see that groups in which all elements, other than the null element, have the type R are complete and are therefore well known; but the set of groups in which all non-null elements are, for example, of type null turn out to be difficult to classify.

We mention a few properties of types of elements of an abelian torsion-free group G that will be used in the following section:

I. *Two elements that are linearly dependent on one another have the same type.*

For these elements generate the same serving subgroup.

II. *If a and b are two elements of type $\mathfrak{a}$ and $\mathfrak{b}$ respectively, then the type of their sum $a + b$ (if it is not the null element) is greater than, or equal to, the product $\mathfrak{a}\mathfrak{b}$.*

For if the characteristics of a and b are α and β respectively, then $a+b$ is in any case divisible by every power of the prime number p_n whose exponent does not exceed $\min(\alpha_n, \beta_n)$. Simple examples show, however, that this element may also be divisible by higher powers of p_n provided that α_n and β_n are finite and equal.

III. *If* $G = A + B$, $a \in A$, $b \in B$, *and if* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are the types of* a *and* b *respectively, then the type of* $a+b$ *is* $\mathfrak{a}\mathfrak{b}$.

For in this case the characteristic γ of $a+b$ is such that, for all n, $\gamma_n = \min(\alpha_n, \beta_n)$.

Let G be an abelian torsion-free group and $\mathfrak{a}$ an arbitrary type. By $G(\mathfrak{a})$ we denote the set that consists of the null element and of all elements of G whose types are greater than or equal to $\mathfrak{a}$; if there are no such elements in G, then $G(\mathfrak{a}) = 0$. It follows from II. that $G(\mathfrak{a})$ *is a subgroup of* G, and I. shows that it is a *serving subgroup* of G. We denote by $G'(\mathfrak{a})$ the subgroup of G that is generated by all elements whose types are strictly greater than $\mathfrak{a}$. This subgroup is contained in $G(\mathfrak{a})$ and may be equal to it; in general, however, it need not even be a serving subgroup of $G(\mathfrak{a})$. The factor group

$$G^*(\mathfrak{a}) = G(\mathfrak{a})/G'(\mathfrak{a})$$

may therefore have elements of finite order.

These subgroups $G(\mathfrak{a})$, $G'(\mathfrak{a})$, and the factor group $G^*(\mathfrak{a})$ will be used in the following section.

§ 31. Completely decomposable groups

After having dealt with torsion-free groups of rank 1 in the preceding section it is now natural to proceed to the study of abelian torsion-free groups that are decomposable into the direct sum of groups of rank 1; such groups are called *completely decomposable* (or completely reducible). This class of groups is rather wide: apart from all groups of rank 1 it comprises all free abelian groups as well as all complete torsion-free abelian groups. On the other hand, we shall show later that by no means are all abelian torsion-free groups completely decomposable.

There exist several criteria for a torsion-free group to be completely decomposable (see Baer [15], Lyapin [6]). However, all these criteria are very cumbersome to formulate and do not lend themselves to a further development of the theory of completely decomposable groups; we shall

therefore not deal with them here. The problem of subgroups or factor groups of fully decomposable groups is also outside our scope: every abelian torsion-free group can be embedded in a complete torsion-free group and is a factor group of a free abelian group. We shall rather be interested in properties of direct decompositions of completely decomposable groups and begin with the following theorem (Baer [15]).

If a torsion-free abelian group G is completely decomposable, then any two decompositions of G into the direct sum of groups of rank 1 are isomorphic.

Suppose we have an arbitrary decomposition of G into the direct sum of groups of rank 1,

$$G = \sum_{\alpha} A_{\alpha}. \tag{1}$$

If G has elements of type $\mathfrak{a}$, then the subgroup $G(\mathfrak{a})$ (see the end of the preceding section) is the direct sum of all summands in (1) whose type is greater than or equal to $\mathfrak{a}$. For since direct summands are serving subgroups, the type of every non-null element of A_{α} is equal to the type of A_{α} itself, so that it remains to apply properties I-III of the preceding section. Similarly, $G'(\mathfrak{a})$ is the sum of all direct summands in (1) whose types are strictly greater than $\mathfrak{a}$. It follows that the sum of the direct summands in (1) whose type is equal to $\mathfrak{a}$ is isomorphic to the factor group $G^*(\mathfrak{a})$, that is, does not depend on the choice of the decomposition (1): every decomposition of G into the direct sum of groups of rank 1 contains as many summands of type $\mathfrak{a}$ as the rank of $G^*(\mathfrak{a})$ (if it is finite) or the cardinal number of $G^*(\mathfrak{a})$ (if its rank is infinite). This completes the proof.

The problem arises whether every direct decomposition of a completely decomposable group can be refined to a decomposition into the direct sum of groups of rank 1. In other words, *is every direct summand of a completely decomposable group itself completely decomposable?* A final answer to this question has not yet been obtained. The paper by Baer [15] contains a number of relevant partial results, some of which we shall now present.

We begin by considering a group that is the direct sum of *isomorphic* groups of rank 1 and prove the following theorem.

If an abelian torsion-free group G has a direct decomposition

$$G = \sum_{\alpha} A_{\alpha}, \tag{2}$$

in which all summands A_{α} have rank 1 and one and the same type $\mathfrak{a}$, and if B is a serving subgroup of G, then B is itself a direct sum of groups of rank 1 and of type $\mathfrak{a}$.

Suppose the index α runs through all ordinal numbers less than σ; we introduce the following notation:

$$G^{(\beta)} = \sum_{\alpha<\beta} A_\alpha,$$

$$B^{(\beta)} = B \cap G^{(\beta)}.$$

For every β we have

$$B^{(\beta)} \subseteq B^{(\beta+1)},$$

and either the equality sign holds or $B^{(\beta+1)}/B^{(\beta)}$ has rank 1 and type $\mathfrak{a}$. For this factor group is isomorphic to a subgroup of $G^{(\beta+1)}$ $G^{(\beta)}$ which is isomorphic to A_β, that is, it has rank 1 and type less than or equal to $\mathfrak{a}$. On the other hand, if $B^{(\beta+1)}$ contains an element x outside $B^{(\beta)}$, then the type of x in B and consequently in $B^{(\beta+1)}$ is equal to $\mathfrak{a}$, because B is a serving subgroup of G. The type of the image of x in $B^{(\beta+1)}/B^{(\beta)}$ cannot, therefore, be less than $\mathfrak{a}$. This proves our assertion.

If we can show that for $B^{(\beta)} \neq B^{(\beta+1)}$ we have a direct decomposition

$$B^{(\beta+1)} = B^{(\beta)} + C_\beta, \tag{3}$$

where C_β is a group of rank 1 and type $\mathfrak{a}$, then the theorem will follow because B is then the direct sum of all non-null subgroups C_β, $\beta < \sigma$. We go on, therefore, to prove that a decomposition (3) exists.

In $B^{(\beta+1)}$ we take an element x outside $B^{(\beta)}$ and we denote the coset $x + B^{(\beta)}$ by $\bar{x}$. If x is divisible by an integer n in $B^{(\beta+1)}$, then the same is true for $\bar{x}$ in $B^{(\beta+1)}/B^{(\beta)}$. The converse need not hold, but it follows from the equality of the types of x and $\bar{x}$ that there exists only a finite number of prime numbers

$$p_{i_1}, p_{i_2}, \ldots, p_{i_m}, \tag{4}$$

such that the value α_{i_k} of the characteristic of x for p_{i_k}, $k = 1, 2, \ldots, m$, is different from the value $\bar{\alpha}_{i_k}$ of the characteristic of $\bar{x}$; both numbers are then finite and

$$\alpha_{i_k} < \bar{\alpha}_{i_k}.$$

Let

$$\bar{h} = p_{i_1}^{\bar{\alpha}_{i_1}} p_{i_2}^{\bar{\alpha}_{i_2}} \ldots p_{i_m}^{\bar{\alpha}_{i_m}},$$

$$h = p_{i_1}^{\bar{\alpha}_{i_1} - \alpha_{i_1}} p_{i_2}^{\bar{\alpha}_{i_2} - \alpha_{i_2}} \ldots p_{i_m}^{\bar{\alpha}_{i_m} - \alpha_{i_m}}.$$

In $B^{(\beta+1)}/B^{(\beta)}$ there exists an element $\bar{y} = y + B^{(\beta)}$ such that

$$\bar{h}\bar{y} = \bar{x}, \tag{5}$$

so that x and $\bar{h}y$ lie in the same coset $\bar{x}$. Let h' be defined for $\bar{h}y$ in the same way as h was for x. Since $\bar{h}y$ is divisible by $\bar{h}$ it follows that h' cannot be divisible by any prime number of (4), so that

$$(h, h') = 1.$$

We can therefore find integers l, l' such that

$$lh + l'h' = 1. \tag{6}$$

The element

$$z = lhx + l'h'(\bar{h}y) \tag{7}$$

lies in $\bar{x}$, by (5) and (6). If p_j is an arbitrary prime number and if β_j is the value of the characteristic of z for p_j, then clearly $\beta_j \leqq \bar{\alpha}_j$. However, z is in any case divisible by every power of p_j that divides both summands of the right-hand side of (7), so that from the definition of h and h' we obtain $\beta_j \geqq \alpha_j$.

We can therefore find an element z in $\bar{x}$ whose characteristic in $B^{(\beta+1)}$ is the same as that of $\bar{x}$ in $B^{(\beta+1)}/B^{(\beta)}$. If we denote by C_β the serving subgroup of $B^{(\beta+1)}$ generated by z, then every coset of $B^{(\beta)}$ in $B^{(\beta+1)}$ contains precisely one element of C_β. This shows the existence of a direct decomposition (3) and concludes the proof of the theorem.

By applying this theorem to the case when B is a direct summand of G we obtain the following result.

If G is the direct sum of groups of rank 1 *and of one and the same type* $\mathfrak{a}$, *then every direct summand of G is also a direct sum of groups of rank* 1 *and type* $\mathfrak{a}$.

Now we prove the following more general theorem.[1]

Suppose that G is completely decomposable and that the set of types of the summands in the decomposition

$$G = \sum_{\alpha} A_\alpha \tag{8}$$

into the direct sum of groups of rank 1 *is finite. Then every direct summand of G is completely decomposable.*

For the proof we denote by

$$\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n \tag{9}$$

[1] The proof has been communicated to the author by L. Y. Kulikov.

the distinct types of summands that occur in (8), and by $D_i, i = 1, 2, \ldots, n$, the direct sum of summands of type $\mathfrak{a}_i$. Then

$$G = D_1 + D_2 + \ldots + D_n. \tag{10}$$

The theorem will be proved if we can show that the decomposition (10) and an arbitrary decomposition of G

$$G = \sum_\beta B_\beta, \tag{11}$$

have isomorphic refinements. For every B_β is then the direct sum of subgroups that are isomorphic to direct summands of D_i, $i = 1, 2, \ldots, n$, and therefore, by the above result, completely decomposable.

We shall prove the existence of isomorphic refinements of (10) and (11) by induction on n; for $n = 1$ there is nothing to prove. Let $\mathfrak{a}_1$ be one of the maximal types among (9) (in the sense of the partial order of types). Then the component of D_1 in the direct summand B_β of the second decomposition is equal to

$$C_\beta = D_1 \cap B_\beta;$$

it cannot be greater than this intersection, since every subgroup is homomorphically mapped onto its component; however by the choice of the type $\mathfrak{a}$, no element of D_1 can under any homomorphism go over into an element of G outside D_1. It follows that there exists a direct decomposition

$$D_1 = \sum_\beta C_\beta,$$

that is to say, we obtain the following refinement of (10):

$$G = \sum_\beta C_\beta + D_2 + \ldots + D_n. \tag{12}$$

The subgroup B_β contains the direct summand C_β of G; therefore we have, for every β, a direct decomposition $B_\beta = C_\beta + C'_\beta$ which leads to the following refinement of (11):

$$G = \sum_\beta C_\beta + \sum_\beta C'_\beta. \tag{13}$$

(12) and (13) now show that the subgroups

$$D_2 + \ldots + D_n, \quad \sum_\beta C'_\beta \tag{14}$$

are isomorphic; by the induction hypothesis they have isomorphic refinements. Substituting these in (12) and (13) we obtain isomorphic refinements of (10) and (11); this is what we had to show.

It follows from this theorem that *every direct summand of a completely decomposable group of finite rank is itself completely decomposable.*

On this problem of direct summands of completely decomposable groups some results have, in fact, been obtained that go further than what we have proved here. For example, Baer [15] has shown that the direct summands are completely decomposable even when the set of types of summands in (8) is no longer finite but only satisfies the *maximal condition* (in the sense of the partial ordering of types). Furthermore, Kulikov [3] has proved that the direct summands of every *countable* completely decomposable group are also completely decomposable.

§ 32. Other classes of abelian torsion-free groups

So far we have not yet come across any abelian torsion-free groups that are not completely decomposable. Such groups, however, do exist.

The unrestricted direct sum (see § 17) *of an infinite set of infinite cyclic groups is not completely decomposable.*

For let G be the unrestricted direct sum of infinitely many infinite cyclic groups. We take a countable subset and denote by G' the unrestricted direct sum of the subgroups occurring in it. If G were completely decomposable then, since all its elements are of type null in it, it would turn out to be a free group, and since G' is isomorphic to a subgroup of G, it would also be free. We can therefore assume that G itself is the unrestricted direct sum of a countable set of infinite cyclic groups.

If

$$a_1, a_2, \ldots, a_n, \ldots$$

are generators of these cyclic groups, then every element g of G can be written as an infinite sum of these generators with integer coefficients

$$g = k_1 a_1 + k_2 a_2 + \ldots + k_n a_n + \ldots . \tag{1}$$

We denote by H the set of elements of the form (1) that have the following property: for every natural number s almost all coefficients $k_1, k_2, \ldots, k_n, \ldots$ (that is: all but, possibly, a finite number) are

divisible by 2^s. The set H is a subgroup of G and has, just like G, the cardinal number of the continuum. If G is free, then H is also free, in other words, is the direct sum of a set of infinite cyclic groups; and then the factor group $H/2H$ (where $2H$ is the set of all elements of H that are divisible by 2) must also have the cardinal number of the continuum.

However $H/2H$ is, in fact, countable. For G contains a countable subgroup H' consisting of the elements of the form (1) that have only a finite number of non-zero coefficients k_n. If now h is an arbitrary element of H, then we can subtract from it an element h' of H' such that the difference $h - h'$ can be written in the form (1) with *all* coefficients divisible by 2. Thus

$$h - h' = 2h_0,$$

and it is easy to see that h_0 belongs to H, so that

$$h - h' \in 2H.$$

This shows that every coset of $2H$ in H contains an element of H', so that $H/2H$ is countable.

By the same method it can be proved more generally (see Baer [15]) that no unrestricted direct sum of an infinite set of groups of rank 1 and of one and the same type, other than R, can be completely decomposable. Moreover, in the paper by Mišina [1] it is shown that if a group G is the unrestricted direct sum of groups A_α of rank 1 (α ranging over an index set M) then G is completely decomposable if and only if among the groups A_α there is only a finite number not of type R.

The groups we have constructed above are, although not completely decomposable, at least decomposable into direct sums: from the unrestricted direct sum of cyclic groups we can always split off a cyclic direct summand. There exist, however, abelian torsion-free groups of rank greater than 1 which are not decomposable at all into a direct sum. This follows from a theorem of Baer [15]:

Every serving subgroup H of the additive group J of p-adic integers (see § 21) *is indecomposable; in particular, J itself is indecomposable.*

For consider the subgroup pJ consisting of the p-fold multiples of all elements of J. This contains precisely those p-adic integers that have in the representation (9) of § 21 a zero in the first place, that is, in which $k_1 = 0$. It follows that the index of pJ in J is p.

Therefore the index of pH in H is also p, so that the factor group H/pH is cyclic of order p. For

$$pH = H \cap pJ,$$

since H is a serving subgroup of J, and

$$J = H + pJ,$$

since the index of pJ in J is a prime number; it now remains to apply the isomorphism theorem

$$H/pH \simeq J/pJ.$$

If H is decomposable,

$$H = H_1 + H_2,$$

then H_1 and H_2, as serving subgroups of H, are also serving subgroups of J. Hence the factor groups H_1/pH_1 and H_2/pH_2 are cyclic of order p. But

$$pH = pH_1 + pH_2,$$

so that H/pH appears as a direct sum of two cyclic groups or order p, and this is a contradiction.

Since J has the cardinal number of the continuum we can find in it serving subgroups of any finite or infinite rank not exceeding the cardinal number of the continuum. It is still an open problem whether there exist indecomposable abelian torsion-free groups of an arbitrary infinite cardinal number.

Some other classes of abelian torsion-free groups, closely related to completely decomposable groups, are also studied in the paper by Baer [15]. For example, an abelian torsion-free group G is called *separable* if every finite set of elements of G is contained in a completely decomposable direct summand of G; obviously we can assume that this direct summand has finite rank. Every completely decomposable group is, of course, separable.

Every countable separable group G is completely decomposable.

For let the elements of G be $g_1, g_2, \ldots, g_n, \ldots$. We put $A_0 = 0$. Suppose we have already found a completely decomposable direct summand A_n of G, of finite rank, containing $g_1, g_2, \ldots, g_n$. Then we take as A_{n+1} a completely decomposable direct summand of G that has finite rank and contains g_{n+1} as well as a maximal linearly independent set of elements of A_n. Since A_{n+1} is a serving subgroup of G and A_n is contained in A_{n+1}, we must have a direct decomposition

$$A_{n+1} = A_n + B_{n+1}.$$

B_{n+1}, as a direct summand of a completely decomposable group of finite rank, is itself completely decomposable (see the preceding section). G is the union of the ascending sequence of subgroups A_n, $n = 0, 1, 2, \ldots$, and is therefore the direct sum of the completely decomposable groups B_n, $n = 1, 2, \ldots$; that is, G is completely decomposable.

In the non-countable case there exist separable groups that are not completely decomposable: *the unrestricted direct sum of an infinite set of infinite cyclic groups is separable* but, as we have shown above, not completely decomposable.

For let G be the unrestricted direct sum of infinite cyclic groups with generators a_α (α ranges over a certain index set). We show, first of all, that every element g of G is contained in a completely decomposable direct summand of G.

The element g, $g \neq 0$, has a representation

$$g = \sum_\alpha k_\alpha a_\alpha, \tag{2}$$

where the k_α are integers. We denote by $k(g)$ the smallest absolute value of the non-zero coefficients k_α,

$$k(g) = \min\,(|k_\alpha|, k_\alpha \neq 0).$$

If $k(g) = 1$, then there is an index β such that

$$k_\beta = \pm 1.$$

Then

$$G = \{g\} + G',$$

where G' consists of all the elements of G for which the coefficient of a_β in the representation (2) is equal to zero; G' is itself the unrestricted direct sum of infinite cyclic groups.

Now let $k(g)$ be arbitrary. We divide every coefficient k_α in (2) by $k(g)$:

$$k_\alpha = k(g)\, q_\alpha + r_\alpha, \quad 0 \leqq r_\alpha < k(g).$$

Then

$$g = k(g)\, g_1 + g_2,$$

where

$$g_1 = \sum_\alpha q_\alpha a_\alpha, \quad g_2 = \sum_\alpha r_\alpha a_\alpha.$$

Since there exists a β such that $k(g) = \pm k_\beta$, $q_\beta = \pm 1$, and therefore $k(g_1) = 1$. We have, then, a direct decomposition

$$G = \{g_1\} + G',$$

where G' consists of all the elements of G for which the coefficient of a_β in (2) is equal to zero. To these elements there belongs g_2, $g_2 \in G'$. But $k(g_2)$ is strictly less than $k(g)$, because all the coefficients r_α are strictly less than $k(g)$. We can therefore assume by induction that there exists a direct decomposition

$$G' = A + B,$$

where A contains g_2, is completely decomposable, and is a free group of finite rank, while B consists of all the elements of G for which the coefficients of a finite number of fixed a_α in (2) are equal to zero. g is now contained in the completely decomposable direct summand $\{g_1\} + A$ of G.

Finally, if $g_1, g_2, \ldots, g_n$ is a finite system of elements of G, then we can assume that there exists a direct decomposition

$$G = U + V,$$

where U is a completely decomposable direct summand containing $g_1, g_2, \ldots, g_{n-1}$ and V is the unrestricted direct sum of infinite cyclic groups. Then

$$g_n = u + v, \; u \in U, \; v \in V,$$

and since we have proved that there exists a direct decomposition

$$V = A + B$$

such that A is completely decomposable and contains v, the direct summand $U + A$ of G is also completely decomposable and contains all the given elements; the direct summand B is again the unrestricted direct sum of infinite cyclic groups. This proves that G is separable.

Other classes of abelian torsion-free groups are also studied in the paper by Baer [15], in particular direct sums of groups in which all non-null elements have one and the same type. Kontorovič [7] has shown that the

theory of this class of groups can be extended to non-commutative torsion-free groups in which, as in all abelian torsion-free groups, the equation

$$x^n = a,\ n > 0,$$

has at most one solution.

The theory of abelian torsion-free groups has also been developed in another direction; in § 30 we gave a classification of groups of rank 1; several classes of abelian torsion-free groups can be classified in a similar way. For example, Kuroš [6] has indicated a method of classifying the groups that are isomorphic to subgroups of the direct sum of a finite number of groups of type R_p (that is, groups isomorphic to the additive group of p-ic fractions); simplifications of some of the proofs are contained in a paper by Kaloujnine [1]. This classification by means of matrices with p-adic elements provided the first example of indecomposable abelian torsion-free groups of arbitrary finite rank—examples of this kind, of rank 2, had been found previously by Levi [1] and Pontryagin [1]. This method of classification has been carried over to the case of arbitrary abelian torsion-free groups of finite rank in papers by Derry [1] and Mal'cev [1];[1] they use systems of matrices with p-adic elements for all prime numbers p. An extension of this method to arbitrary countable abelian torsion-free groups has been given in a paper by Szekeres [1], and the assumption of countability of the groups can, in fact, easily be removed. However, in all these cases the classification of the groups turns out to be extremely complicated; it is hardly a help in the investigation of the groups, but is rather a method of describing them.

On the whole, the theory of abelian torsion-free groups is still very far from complete. For example, it is an open problem whether decompositions of an abelian torsion-free group of finite rank into direct sums of indecomposable groups are isomorphic—a counter-example in a relevant paper by B. Jónsson (Bull. Amer. Math. Soc. vol. 51 (1945), p. 364) is incorrect.

[1] See also § 40 and § 41 of the first edition of this book.

APPENDIXES

APPENDIXES

Appendix A (*page* 39)

[a] We consider permutations π on the set of n symbols $\{1, 2, \ldots, n\}$ and write them as right-hand operators. Positive and negative powers of π are defined in the obvious way; π^0 is the identity permutation. If $i\pi \neq i$, we say that the symbol i is *affected* by, or *moved* by, π; if $i\pi = i$, we say that i is *left invariant* by π. A permutation π is called *cyclic* or a *cycle* if of any two symbols moved by π each is carried into the other by a suitable power of π. In that case

$$\pi = \begin{pmatrix} a_1 & a_2 & \ldots & a_{k-1} & a_k & \ldots & i \ldots & j \ldots \\ a_2 & a_3 & \ldots & a_k & a_1 & \ldots & i \ldots & j \ldots \end{pmatrix};$$

we write $\pi = (a_1, a_2, \ldots, a_k)$ and call k the *length* of the cycle. A cycle of length two is called a *transposition*: $\pi = (b, c)$. Every cycle of length k can be written as a product of $k - 1$ transpositions. In fact,

$$(a_1, a_2, \ldots, a_k) = (a_1, a_2)\,(a_1, a_3) \ldots (a_1, a_{k-1})\,(a_1, a_k).$$

Every permutation π can be written as a product of disjoint cycles, unique apart from order of the factors. For let a and b be symbols of the set $\{1, 2, \ldots, n\}$. We say that a is *equivalent* to b if a power of π carries a into b, say $a\pi^l = b$. This is an equivalence relation, because the transitive and reflexive properties obviously hold and the symmetry follows from the fact that $b\pi^{-l} = a$. This equivalence relation splits the set $\{1, 2, \ldots, n\}$ into disjoint classes; each class is a cycle, and π is the product of these cycles.

We write $\pi = (a_1, \ldots, a_k)\,(b_1, \ldots, b_l)\,(c_1, \ldots, c_m) \ldots$; cycles of length 1 (that is, symbols left invariant by π) can be omitted. As an example:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 3 & 10 & 1 & 4 & 6 & 7 & 5 & 11 & 9 & 8 & 2 \end{pmatrix} = (13)\,(2\,10\,8\,11)\,(5\,6\,7).$$

Hence every permutation π can be written as a product of transpositions. If π has r cycles (cycles of length 1 being included in the count) then π can be written as a product of $n - r$ transpositions.

If a given permutation π on n symbols splits into r disjoint cycles, then the number of transpositions in all possible representations of π as a product of transpositions is always even or odd according as $n - r$ is even or odd.

We shall show first that, when π is multiplied by a transposition (b, c), then r is increased or decreased by 1 (hence $n - r$ is decreased or increased by 1), according as b and c lie in the same or in distinct cycles of π. For if

$$\pi = (b a_1 \ldots a_2 c a_3 \ldots a_4) \ldots,$$

then

$$\pi(bc) = (b a_1 \ldots a_2)(c a_3 \ldots a_4),$$

and r has been increased by 1. If

$$\pi = (b a_1 \ldots a_2)(c a_3 \ldots a_4) \ldots,$$

where one or both cycles may be of length 1, then

$$\pi(bc) = (b a_1 \ldots a_2 c a_3 \ldots a_4) \ldots$$

and r has been decreased by 1. Now the identity permutation has $r = n$, $n - r = 0$; hence the parity of the number of transpositions in all representations of π is fixed and is the same as that of $n - r$.

Appendix B (*page* 40)

[b] Example 14 falls under the type considered in 13 if the property α is taken to be: the mappings affect only a finite number of symbols. In current terminology, the group in 13 is also called the *unrestricted*, and the group in 14, the *restricted* symmetric group. Note that if the cardinal number of the set of symbols is $\mathfrak{m}$, then the restricted symmetric group is of cardinal number $\mathfrak{m}$, the unrestricted of cardinal number $2^{\mathfrak{m}}$. The unrestricted alternating group of infinite cardinal number cannot be defined.

Appendix C (*page* 48)

[c] It is often convenient to admit also an *empty* set of elements of a group G. In this case the subgroup generated by an empty set of elements is taken to be the trivial subgroup E.

Appendix D (*page* 52)

[d] The set of subgroups can, therefore, be *ordered* "by inclusion": we

agree to say that A_α *precedes* A_β whenever A_α is contained in A_β. The construction given in the text can be carried out under even more general conditions. Suppose that a set of subgroups A_α of G is given (where α ranges over an index set N) and that for any two subgroups A_α, A_β the set includes at least one subgroup A_γ containing both A_α and A_β. The set can then be *partially ordered* "by inclusion," the index set N becomes a *directed set*, and the union of the set of subgroups can be proved to be a subgroup of G, as in the text. As to partial order, see also § 43.

Appendix E (*page* 55)

[e]There exists another construction of a limit group of a set of groups $\{G_\alpha\}$, the so-called *inverse limit*. We begin by explaining the construction in the case of a simple sequence of groups. Suppose that

$$G_1, G_2, \ldots, G_n, \ldots \tag{1}$$

are groups and that for every n a homomorphic mapping φ_n of G_{n+1} onto G_n is given:

If $g_{n+1} \in G_{n+1}$, then $g_{n+1}\varphi_n \in G_n$, and for every $g_n \in G_n$ there is a g_{n+1} such that

$$g_n = g_{n+1}\varphi_n. \tag{2}$$

We again define a *thread* to be a sequence of elements

$$\gamma = g_1, g_2, \ldots,$$

in which, for $n = 1, 2, \ldots$, $g_n \in G_n$ and $g_{n+1}\varphi_n = g_n$. Then

$$\gamma^{-1} = g_1^{-1}, g_2^{-1}, \ldots$$

is also a thread, and if

$$\gamma' = g_1', g_2', \ldots,$$

is another thread, then $\gamma\gamma' = g_1 g_1', g_2 g_2', \ldots$ is also a thread. Under this multiplication the threads are easily seen to form a group, the *inverse limit* of the sequence (1) with the homomorphisms (2).

This construction can be extended to arbitrary partially ordered sets of groups $\{G_\alpha\}$, where α ranges over an index set N. Let the index set N be *directed*, that is, partially ordered with a transitive relation $\leqq$ such that for

every pair $\alpha, \beta \in N$ there exists a $\gamma \in N$ such that $\alpha \leqq \gamma$, $\beta \leqq \gamma$. Now suppose that for every pair G_α, G_β with $\alpha \leqq \beta$ a homomorphic mapping $\varphi_{\beta\alpha}$ of G_β onto G_α is given and that, whenever $\alpha \leqq \beta \leqq \gamma$, we have for every $g_\gamma \in G_\gamma$

$$g_\gamma \varphi_{\gamma\alpha} = g_\gamma \varphi_{\gamma\beta} \varphi_{\beta\alpha}.$$

We then define a *thread* as a set of elements $\{g_\alpha\}$ such that for every $\alpha \in N$ we have $g_\alpha \in G_\alpha$ and for every pair $\alpha, \beta \in N$ with $\alpha \leqq \beta$ the elements g_α and g_β are linked by the relation

$$g_\alpha = g_\beta \varphi_{\beta\alpha}.$$

The inverse of a thread and the product of two threads are defined in the obvious way, and under this multiplication the set of threads becomes a group, the *inverse limit* of the set $\{G_\alpha\}$ with the homomorphisms $\varphi_{\beta\alpha}$.

For applications of the inverse limit see Haimo [1], G. Higman [4], G. Higman and A. H. Stone [1].

Appendix F (*page* 77)

[f] This result can be generalized as in § 7. Instead of the sequence U_k, $k = 1, 2, \ldots$ of subgroups we can take any collection of subgroups U_α (where the index α ranges over an ordered set A) which is *ordered by inclusion* so that $U_\alpha \subset U_\beta$ when $\alpha < \beta$; it is even sufficient to assume that the groups U_α are *partially ordered* by inclusion, provided that for any two $\alpha, \beta \in A$ there exists a $\gamma \in A$ such that U_γ contains both U_α and U_β. (The index set then forms a *directed set.*) Furthermore, the subgroups U_α need not all be simple, provided that for every $\alpha \in A$ there exists a $\beta \in A$ with $\alpha < \beta$ such that U_β is simple. The union of the collections U_α of subgroups is then a simple group.

Appendix G (*page* 87)

[g] Even if the original is single-valued, the endomorphism need not have an inverse, because it may be an isomorphic mapping of the group *into* itself.

Let π be a mapping of a set M into itself. A *right inverse mapping* π_r^{-1} of π exists if and only if π is *one-to-one*; π_r^{-1} is then a mapping of M_π onto M. A *left inverse mapping* π_l^{-1} of π exists if and only if π is *onto*; π_l^{-1} is then a one-to-one mapping of M into itself. Hence an *inverse* mapping π^{-1} exists if and only if π is a one-to-one mapping of M onto itself or a "*permutation*" of M.

Consider the group of sequences of integers $(a_1, a_2, \ldots, a_n, \ldots)$ with addition of components as the group operation. Then the mapping

$$(a_1, a_2, \ldots) \rightarrow (a_2, a_3, \ldots)$$

is a homomorphic many-to-one mapping of the group onto itself and has a left inverse but no right inverse, whereas the mapping

$$(a_1, a_2, \ldots) \rightarrow (0, a_1, a_2, \ldots)$$

is a homomorphic one-to-one mapping of the group into itself and has a right inverse but no left inverse.

Appendix H (*page* 99)

[h] The author uses the term *metabelian*. But in current terminology a metabelian group is one whose derived group (see the end of § 14) is abelian. This class of groups is again much wider than that of nilpotent groups of class 2. In terms of the derived chain and lower central chain metabelian groups are characterized by the equation $G'' = E$, nilpotent groups of class 2 by $G_2 = E$.

Appendix I (*page* 119)

[i] It is more accurate to say that the representation of an element g of G is unique only apart from a finite number of factors that are the unit elements of subgroups H_α whose elements do not otherwise occur in the representation of g. In the applications of the direct product (see, for example, Chapter VI) it is sometimes desirable to retain such arbitrary unit elements as factors in order to avoid the need to distinguish various cases. Note that there is no ambiguity in the case of the direct product of a finite number of factors (p. 117), where the representation of each element g of G requires a factor from every subgroup H_i, $i = 1, 2, \ldots, n$. The parallelism between the cases of a finite and an infinite number of factors is restored in the synthetic definition of a direct product (p. 122), where again each element of the direct product to be constructed involves a factor from every group A_α.

Appendix J (*page* 120)

[i] The simplest illustration of these statements about components in a direct product is provided by Klein's Four-group V (see § 9). Let $a = (12)(34)$, $b = (13)(24)$, $c = (14)(23) = ab$. V is easily seen to be the direct product of its cyclic subgroups $\{a\}$ and $\{b\}$, $V = \{a\} \times \{b\}$, and in this decomposition the component of c in $\{a\}$ is a and in $\{b\}$ is b, so that the direct product of the components of $\{c\}$ is V. Furthermore, V has another decomposition $V = \{a\} \times \{c\}$, and in this decomposition the component of c in $\{a\}$ is the unit element.

Appendix K (*page* 125)

[k] The author uses the term "word" for what we have called "reduced word" and has no name for our "words," or strings of symbols x_a, x_a^{-1}. Our terminology is more in keeping with current usage.

Appendix L (*page* 128)

[l] The reader should bear in mind that "element of a free group" and "word" (even "reduced word") are conceptually two distinct objects. The same group element can be represented by different reduced words, because the set of generators of the free group can be altered without altering the group.

Appendix M (*page* 130)

[m] The reader should convince himself that in the Examples 2 and 3 the group R and the group of type p^∞ are, in fact, isomorphic to the groups defined by the relations of the text and not to factor groups of those groups. It should also be noted for later use (p. 165) that every torsion-free homomorphic image of R is an isomorphic image (if R/N is torsion free, then $N = 0$) and that every homomorphic image of a group of type p^∞ is itself of type p^∞ (p. 57).

Appendix N (*page* 151)

[n] The subgroup theorem can be supplemented by the following existence theorem (the proof is simple and can be left to the reader): *For every choice of the numbers* s, l_p, *and* β_{pi}, *subject to the conditions* (6), (7), *and* (8), G *contains at least one subgroup* H *with the prescribed invariants.*

Appendix O (*page* 162)

[o] Detailed studies of modules over principal ideal rings, with many exercises, are contained in the recent books by Bourbaki [1] and Kaplansky [3], § 12 ff.

Appendix P (*page* 170)

[p] In his definition of *height* the author does not attribute a height to the null element of a group. In this case the expression *group without elements of infinite height* is to be taken literally. On the other hand, to give but one example, the group G^1 of § 27 has to be described as consisting of all the elements of infinite height in G, *together with the null element.*

Appendix Q (*page* 193)

[q] A new proof of Ulm's Theorem (Kaplansky and Mackey [1]; see also Bourbaki, *Algèbre*, Chap. VII, § 2, Exercises, pp. 74-81 (1952)) extends it to countably generated torsion modules over a principal ideal ring. The authors also treat the case of countably generated modules over the p-adic integers (or more generally, over a complete discrete valuation ring) provided the torsion-free rank does not exceed 1, and they find that for a complete set of invariants the Ulm factors have to be supplemented by one further invariant, a certain equivalence class of sequences of ordinals. The new feature of this proof is that (in the language of group theory) the groups to be classified are no longer primary, but mixed. Torsion-free abelian groups have not yet been completely classified, even in the countable case. See also p. 221.

BIBLIOGRAPHY

BIBLIOGRAPHY

This Bibliography is that of the second Russian edition supplemented with a few additional references (marked by a dagger (†)) to the material of Vol. I. Vol. II will contain a separate bibliography consisting of references to relevant group-theoretical papers of recent years.

The transliteration of Russian names is that of the Mathematical Reviews, except in the case of a few names (Dietzmann, Fuchs-Rabinovič, Schmidt) where a different form is in more general use. Russian-language papers have been indicated by an asterisk (*), and the titles of such papers are given in English translation.

ADELSBERGER, H.

[1] *Über unendliche diskrete Gruppen*, J. reine angew. Math, vol. 163 (1930), pp. 103—124.

ADO, I. D.

*[1] *On nilpotent algebras and p-groups*, Doklady Akad. Nauk SSSR., vol. 40 (1943), pp. 339—342.

*[2] *On subgroups of the countable symmetric group*, Doklady Akad. Nauk SSSR., vol. 50 (1945), pp. 15—18.

*[3] *Locally finite p-groups with minimal condition for normal subgroups*, Doklady Akad. Nauk SSSR. vol. 54 (1946), pp. 475—478.

*[4] *Proof of the countability of a locally finite p-group with minimal condition for normal subgroups.* Doklady Akad. Nauk SSSR. vol. 58 (1947), pp. 523—524.

ARTIN, E.

[1] *The free product of groups*, Amer. J. Math., vol. 69 (1947), pp. 1—4.

BAER, R.

[1] *Zur Einführung des Scharbegriffs*, J. reine angew. Math., vol. 160 (1929), pp. 199—207.

[2] *Situation der Untergruppen und Struktur der Gruppe*, S.-B. Heidelberg. Akad., vol. 2 (1933), pp. 12—17.

[3] *Der Kern, eine charakteristische Untergruppe*, Comp. Math., vol. 1 (1934), pp. 254—283.

[4] *Erweiterung von Gruppen und ihren Isomorphismen*, Math. Zeit., vol. 38 (1934), pp. 375—416.

[5] *The decomposition of enumerable, primary, abelian groups into direct summands*, Quart. J. (Oxford), vol. 6 (1935), pp. 217—221.

[6] *The decomposition of abelian groups into direct summands*, Quart. J. (Oxford), vol. 6 (1935), pp. 222—232.

[7] *Types of elements and characteristic subgroups of abelian groups*, Proc. London Math. Soc., vol. 39 (1935), pp. 481-514.

[8] *Gruppen mit hamiltonschem Kern*, Comp. Math., vol. 2 (1935), pp. 241—246.

[9] *Zentrum und Kern von Gruppen mit Elementen unendlicher Ordnung*, Comp. Math., vol. 2 (1935), pp. 247—249.

[10] *Automorphismen von Erweiterungsgruppen*, Actualités Scient. et Industr., no. 205, Paris, 1935.

[11] *Die Kompositionsreihe der Gruppe aller eineindeutigen Abbildungen einer unendlichen Menge auf sich*, Studia Math., vol. 5 (1934), pp. 15—17.

[12] *Gruppen mit vom Zentrum wesentlich verschiedenem Kern und abelscher Faktorgruppe nach dem Kern*, Comp. Math., vol. 4 (1936), pp. 1—77.

[13] *The subgroup of the elements of finite order of an abelian group*, Ann. of Math., vol. 37 (1936), pp. 766—781.

[14] *Primary abelian groups and their automorphisms*, Amer. J. Math., vol. 59 (1937), pp. 99—117.

[15] *Abelian groups without elements of finite order*, Duke Math. J., vol. 3 (1937), pp. 68—122.

[16] *Dualism in abelian groups*, Bull. Amer. Math. Soc., vol. 43 (1937), pp. 121—124.

[17] *Groups with abelian central quotient group*, Trans. Amer. Math. Soc., vol. 44 (1938), pp. 357—386.

[18] *Groups with preassigned central and central quotient group*, Trans. Amer. Math. Soc., vol. 44 (1938), pp. 387—412.

[19] *The applicability of lattice theory to group theory*, Bull. Amer. Math. Soc., vol. 44 (1938), pp. 817—820.

[20] *The significance of the system of subgroups for the structure of the group*, Amer. J. Math., vol. 61 (1939), pp. 1—44.

[21] *Duality and commutativity of groups*, Duke Math. J., vol. 5 (1939), pp. 824—838.

[22] *Almost hamiltonian groups*, Comp. Math., vol. 6 (1939), pp. 382—406.

[23] *Groups with abelian norm quotient group*, Amer. J. Math., vol. 61 (1939), pp. 700—708.

[24] *Nilpotent groups and their generalization*, Trans. Amer. Math. Soc., vol. 47 (1940), pp. 393—434.

[25] *Sylow theorems for infinite groups*, Duke Math. J., vol. 6 (1940), pp. 598—614.

[26] *Abelian groups that are direct summands of every containing abelian group*, Bull. Amer. Math. Soc., vol. 46 (1940), pp. 800—806.

[27] *Automorphism rings of primary abelian operator groups*, Ann. of Math., vol. 44 (1943), pp. 192—227.

[28] *A theory of crossed characters*, Trans. Amer. Math. Soc., vol. 54 (1943), pp. 103—170.

[29] *The higher commutator subgroups of a group*, Bull. Amer. Math. Soc., vol. 50 (1944), pp. 143—160.

[30] *Groups without proper isomorphic quotient groups*, Bull. Amer. Math. Soc., vol. 50 (1944), pp. 267—278.

[31] *Crossed isomorphisms*, Amer. J. Math., vol. 66 (1944), pp. 341—404.

[32] *Representations of groups as quotient groups*, Trans. Amer. Math. Soc., vol. 58 (1945), pp. 295—419.

[33] *Absolute retracts in group theory*, Bull. Amer. Math. Soc., vol. 52 (1946), pp. 501—506.

[34] *The double chain condition in cyclic operator groups*, Amer. J. Math., vol. 69 (1947), pp. 37—45.

[35] *Splitting endomorphisms*, Trans. Amer. Math. Soc., vol. 61 (1947), pp. 508—516.

[36] *Endomorphism rings of operator loops*, Trans. Amer. Math. Soc., vol. 61 (1947), pp. 517—529.

[37] *Direct decompositions*, Trans. Amer. Math. Soc., vol. 62 (1947), pp. 62—98.

[38] *The role of the center in the theory of direct decompositions*, Bull. Amer. Math. Soc., vol. 54 (1948), pp. 167—174.

[39] *Direct decompositions into infinitely many summands*, Trans. Amer. Math. Soc., vol. 64 (1948), pp. 519—551.

[40] *Finiteness properties of groups*, Duke Math. J., vol. 15 (1948), pp. 1021—1032.

[41] *Groups with descending chain condition for normal subgroups*, Duke Math. J., vol. 16 (1949), pp. 1—22.

[42] *Extension types of abelian groups*, Amer. J. Math., vol. 71 (1949), pp. 461—490.

[43] *Die Schar der Gruppenerweiterungen*, Math. Nachr., vol. 2 (1949), pp. 317—327.

[44] *Free sums of groups and their generalizations*, Amer. J. Math., vol. 71 (1949), pp. 706—742; vol. 72 (1950), pp. 625—646, 647—670.

[45] *Endlichkeitskriterien für Kommutatorgruppen*, Math. Ann., vol. 124 (1952), pp. 161—177.

BAER, R. and LEVI, F.

[1] *Vollständige irreduzible Systeme von Gruppenaxiomen*, S.-B. Heidelberger Akad. Wiss., vol. 2 (1932), pp. 3—12 (Beitr. zur Algebra 18).

[2] *Freie Produkte und ihre Untergruppen*, Comp. Math., vol. 3 (1936), pp. 391—398.

BAER, R. and WILLIAMS, C.

[1] *Splitting criteria and extension types*, Bull. Amer. Math. Soc., vol. 55 (1949), pp. 729—743.

BAUER, M.

[1] *Über die alternierende Gruppe*, Mat. fiz. Lapok, vol. 39 (1932), pp. 25—26.

BEAUMONT, R. A.

[1] *Projections of non-abelian groups upon abelian groups containing elements of infinite order*, Amer. J. Math., vol. 64 (1942), pp. 115—136.

[2] *Projections of the prime-power abelian group of order p^m and type $(m-1, 1)$*, Bull. Amer. Math. Soc., vol. 48 (1942), pp. 866—870.

[3] *Groups with isomorphic proper subgroups*, Bull. Amer. Math. Soc., vol. 51 (1945), pp. 381—387.

BERLINKOV, M. L.

*[1] *Groups with a compact subgroup lattice*, Doklady Akad. Nauk SSSR., vol. 82 (1952), pp. 505—508.

BIRKHOFF, G.

[1] *On the combination of subalgebras*, Proc. Cambridge Phil. Soc., vol. 29 (1933), pp. 441—464.

[2] *Transfinite group series*, Bull. Amer. Math. Soc., vol. 40 (1934), pp. 847—850.

[3] *Subgroups of Abelian groups*, Proc. London Math. Soc., vol. 38 (1934), pp. 385—401.

[4] *Lattices and their applications*, Bull. Amer. Math. Soc., vol. 44 (1938), pp. 793—800.

[5] *Lattice Theory*, Amer. Math. Soc., New York (1940), 2nd ed. (1948).

[6] *The radical of a group with operators*, Bull. Amer. Math. Soc., vol. 49 (1943), pp. 751—753.

BIRKHOFF, G. and HALL, P.

[1] *On the order of groups of automorphisms*, Trans. Amer. Math. Soc., vol. 39 (1936), pp. 496—499.

BOURBAKI, N.

†[1] *Algèbre, Chap. VII (Modules sur les anneaux principaux)*, Actualités Scient. et Ind. no. 1179, § 2, Exercises.

BROWN, A. B.

[1] *Group invariants and torsion coefficients*, Ann. of Math., vol. 33 (1932), pp. 373—376.

BUNDGAARD, S. and NIELSEN, J.

[1] *On normal subgroups with finite index in F-groups*, Mat. Tidsskrift B, (1951), pp. 56—58.

BURNSIDE, W.

[1] *The Theory of Groups of Finite Order*, Cambridge (1897), 2nd ed. (1911).

[2] *On an unsettled question in the theory of discontinuous groups*, Quart. J., vol. 38 (1902), pp. 230—238.

[3] *On criteria for the finiteness of the order of a group of linear substitutions*, Proc. London Math. Soc., vol. 3 (1905), pp. 435—440.

ČARIN, V. S.

*[1] *Remark on the minimal condition for subgroups*, Doklady Akad. Mauk SSSR., vol. 66 (1949), pp. 575—576.

*[2] *On complete groups with a radical series of finite length*, Doklady Akad. Nauk SSSR., vol. 66 (1949), pp. 809—811.

*[3] *On the theory of locally nilpotent groups,* Mat. Sbornik, vol. 29 (1951), pp. 433—454.

ČERNIKOV, S. N.

*[1] *Extension of a theorem of Frobenius to infinite groups,* Mat. Sbornik, vol. 3 (1938), pp. 413—416.

*[2] *On a theorem of Frobenius,* Mat. Sbornik, vol. 4 (1938), pp. 531—539.

*[3] *Infinite special groups,* Mat. Sbornik, vol. 6 (1939), pp. 199—214.

*[4] *Infinite locally solvable groups,* Mat. Sbornik, vol. 7 (1940), pp. 35—64.

*[5] *On the theory of infinite special groups,* Mat. Sbornik, vol. 7 (1940), pp. 539—548.

*[6] *On groups with a Sylow set,* Mat. Sbornik, vol. 8 (1940), pp. 377—394.

*[7] *On the theory of locally solvable groups,* Mat. Sbornik, vol. 13 (1943), pp. 317—333.

*[8] *On infinite special groups with finite center,* Mat. Sbornik, vol. 17 (1945), pp. 105—130.

*[9] *On the theory of infinite p-groups,* Doklady Akad. Nauk SSSR., vol. 50 (1945), pp. 71—74.

*[10] *Complete groups with an ascending central series,* Mat. Sbornik, vol. 18 (1946), pp. 397—422.

*[11] *On the theory of finite p-extensions of abelian p-groups,* Doklady Akad. Nauk SSSR., vol. 58 (1947), pp. 1287—1289.

*[12] *Infinite groups with finite layers,* Mat. Sbornik, vol. 22 (1948), pp. 101—133.

*[13] *On the theory of complete groups,* Mat. Sbornik, vol. 22 (1948), pp. 319—348, 455—456.

*[14] *On the theory of special p-groups,* Doklady Akad. Nauk SSSR., vol. 63 (1948), pp. 11—14.

*[15] *On the theory of locally solvable groups with minimal condition for subgroups,* Doklady Akad. Nauk SSSR., vol. 65 (1949), pp. 21—24.

*[16] *On complete groups with ascending central series,* Doklady Akad. Nauk SSSR., vol. 70 (1950), pp. 965—968.

*[17] *On the centralizer of a complete abelian normal subgroup of an infinite periodic group,* Doklady Akad. Nauk SSSR., vol. 72 (1950), pp. 243—246.

*[18] *On the minimal condition for abelian subgroups,* Doklady Akad. Nauk SSSR., vol. 75 (1950), pp. 345—347.

*[19] *Periodic ZA-extensions of complete groups,* Mat. Sbornik, vol. 27 (1950), pp. 117—128.

*[20] *On special p-groups,* Mat. Sbornik, vol. 27 (1950), pp. 185—200.

*[21] *On locally solvable groups with minimal condition for subgroups,* Mat. Sbornik, vol. 28 (1951), pp. 119—129.

CHATELET, A.

[1] *Les groupes abéliens finis et les modules de points entiers* Paris, Lille (1925).

CLIFFORD, A. H.

[1] *Representations induced in an invariant subgroup*, Ann. of Math., vol. 38 (1937), pp. 533—550.

CLIFFORD, A. H. and MACLANE, S.

[1] *Factor-sets of a group in its abstract unit group*, Trans. Amer. Math. Soc., vol. 50 (1941), pp. 385—406.

COCKCROFT, W. H.

[1] *The word problem in a group extension*, Quart. J. Math. Oxford Ser. (2), vol. 2 (1951), pp. 123—134.

COXETER, H. S. M.

[1] *On simple isomorphism between abstract groups*, J. London Math. Soc., vol. 9 (1934), pp. 211—212.

[2] *Abstract groups of the form* $V_i^k = V_j^3 = (V_i V_j)^2 = 1$, J. London Math. Soc., vol. 9 (1934), pp. 213—219.

[3] *The groups determined by the relations* $S^l = T^m = (S^{-1}T^{-1}ST)^p = 1$, Duke Math. J., vol. 2 (1936), p. 61—73.

[4] *An abstract definition for the alternating group in terms of two generators*, J. London Math. Soc., vol. 11 (1936), pp. 150—156.

[5] *The abstract groups* $R^m = S^m = (RiSi)^{p_j} = 1$, $S^m = T^2 = (SiT)^{2p_j} = 1$, and $S^m = T^2 = (S^{-i}TSiT)^{p_j} = 1$, Proc. London Math. Soc., vol. 41 (1936), pp. 278—301.

[6] *The abstract groups* $G^{m,n,p}$, Trans. Amer. Math Soc., vol. 45 (1939), pp. 73—150.

[7] *A method for proving certain abstract groups to be infinite*, Bull. Amer. Math. Soc., vol. 46 (1940), pp. 246—251.

ČUNIHIN, S. A.

*[1] *On solvable groups*, Izvestiya NIIMM Tomsk Univ., vol. 2 (1938), pp. 220—223.

*[2] *On p-properties of groups*, Doklady Akad. Nauk SSSR., vol. 55 (1947), pp. 481—484.

*[3] *On the subgroups of relatively solvable groups*, Doklady Akad. Nauk SSSR., vol. 58 (1947), pp. 1295—1296.

*[4] *On* Π*-separable groups*, Doklady Akad. Nauk SSSR., vol. 59 (1948), pp. 443—445.

*[5] *On Sylow regular groups*, Doklady Akad. Nauk SSSR., vol. 60 (1948), pp. 773—774.

✓*[6] *On* Π*-properties of finite groups*, Mat. Sbornik, vol. 25 (1949), pp. 321—346.

[6] English translation of above: T72, Russian Translation Project, Amer. Math. Soc.

*[7] *On theorems of Sylow's type*, Doklady Akad. Nauk SSSR., vol. 66 (1949), pp. 165—168.

*[8] *On conditions for theorems of Sylow's type*, Doklady Akad. Nauk SSSR., vol. 69 (1949), pp. 735—737.

*[9] *On Sylow properties of finite groups*, Doklady Akad. Nauk SSSR., vol. 73 (1950), pp. 29—32.

*[10] *Sylow properties and semi-invariant subgroups*, Doklady Akad. Nauk SSSR., vol. 77 (1951), pp. 973—975.

DEDEKIND, R.

[1] *Über Gruppen, deren sämmtliche Teiler Normalteiler sind*, Math. Ann., vol. 48 (1897), pp. 548—561.

[2] *Über die von drei Moduln erzeugte Dualgruppe*, Math. Ann., vol. 53 (1900), pp. 371—403.

DE GROOT, J.

[1] *Exemple d'un groupe avec deux générateurs, contenant un sousgroupe commutatif sans un système fini de générateurs*, Nieuw Arch. Wiskunde, vol. 23 (1950), pp. 128—130.

DEHN, M.

[1] *Über unendliche diskontinuierliche Gruppen*, Math. Ann., vol. 71 (1912), pp. 116—144.

DERRY, D.

[1] *Über eine Klasse von Abelschen Gruppen*, Proc. London Math. Soc., vol. 43 (1937), pp. 490—506.

[2] *On finite abelian p-groups*, Bull. Amer. Math. Soc., vol. 45 (1939), pp. 874—881.

DICKSON, L. E.

[1] *Linear Groups, with an Exposition of the Galois Field theory*, Leipzig (1901).

DIETZMANN (Dicman), A. P.

*[1] *On p-groups*, Doklady Akad. Nauk SSSR., vol. 15 (1937), pp. 71—76.

[2] *Sur les groupes infinis*, C. R. Acad. Sci. Paris, vol. 205 (1937), pp. 952—953.

*[3] *On the centers of p-groups*, Trudy Sem. Teor. Grupp, (1938), pp. 30—34.

*[4] *Some theorems on infinite groups*, Sbornik pamyati Akad. Gravé, (1940), pp. 63—67.

*[5] *On multigroups of classes of conjugate elements of a group*, Doklady Akad. Nauk SSSR., vol. 49 (1945), pp. 323—326.

[6] *On an extension of Sylow's Theorem*, Ann. of Math., vol. 48 (1947), pp. 137—146.

*[7] *On Sylow's Theorem*, Doklady Akad. Nauk SSSR., vol. 59 (1948), pp. 1235—1236.

DIETZMANN, A. P., KUROŠ, A. G., and UZKOV, A. I.

[1] *Sylowsche Untergruppen von unendlichen Gruppen*, Mat. Sbornik, vol. 3 (1938), pp. 179—185.

DONYAHI, H. A.

*[1] *Linear representation of the free product of cyclic groups*, Ucenye zapiski Leningrad Univ., vol. 55 (1940), pp. 158—165.

DYCK, W.

[1] *Gruppentheoretische Studien*, Math. Ann., vol. 20 (1882), pp. 1—45; vol. 22 (1883), pp. 70—108.

DYUBYUK, P. E.

*[1] *On subgroups of finite index in infinite groups*, Mat. Sbornik, vol. 10 (1942), pp. 147—150.

DYUBYUK, P. E. and TURKIN, V. K.

[1] *Théorèmes sur les groupes infinis*, C. R. Acad. Sci. Paris, vol. 205 (1937), pp. 435—437.

*[2] *Theorems on infinite groups*, Mat. Sbornik, vol. 3 (1938), pp. 425—429.

ECKMANN, B.

[1] *Der Cohomologie-Ring einer beliebigen Gruppe*, Comment. Math. Helv., vol. 18 (1946), pp. 232—282.

EILENBERG, S. and MACLANE, S.

[1] *Group extensions and homology*, Ann. of Math., vol. 43 (1942), pp. 757—831.

[2] *Natural isomorphisms in group theory*, Proc. Nat. Acad. Sci. U.S.A., vol. 28 (1942), pp. 537—543.

[3] *General theory of natural equivalences*, Trans. Amer. Math. Soc., vol. 58 (1945), pp. 231—294.

[4] *Cohomology theory in abstract groups*, I, Ann. of Math., vol. 48 (1947), pp. 51—78.

[5] *Cohomology theory in abstract groups*, II, Ann. of Math., vol. 48 (1947), pp. 326—341.

[6] *Algebraic cohomology groups and loops*, Duke Math. J., vol. 14 (1947), pp. 435—463.

EVERETT, C. J.

[1] *The basis theorem for vector spaces over rings*, Bull. Amer. Math. Soc., vol. 51 (1945), pp. 531—532.

FADDEEV, D. K.

*[1] *On factor systems in abelian operator groups*, Doklady Akad. Nauk SSSR., vol. 58 (1947), pp. 361—364.

*[2] *On the homology theory in groups*, Izvestiya Akad. Nauk SSSR. Ser. Mat., vol. 16 (1952), pp. 17—22.

FEDERER, H. and JÓNSSON, B.

[1] *Some properties of free groups*, Trans. Amer. Math. Soc., vol. 68 (1950), pp. 1—27.

FEDOROV, YU. G.

*[1] *On infinite groups in which all non-trivial subgroups have finite index*, Uspehi Matem. Nauk, vol. 6 : 1 (1951), pp. 187—189.

FITTING, H.

[1] *Die Theorie der Automophismenringe Abelscher Gruppen und ihr Analogen bei nicht kommutativen Gruppen*, Math. Ann., vol. 109 (1933), p. 616.

[2] *Über die direkten Produktzerlegungen einer Gruppe in direkt unterlegbare Faktoren*, Math. Zeit., vol. 39 (1934), pp. 16—30.

[3] *Über die Existenz gemeinsamer Verfeinerungen bei direkten Produktzerlegungen einer Gruppe*, Math. Zeit., vol. 41 (1936), pp. 380—395.

[4] *Über den Automorphismen bereich einer Gruppe*, Math. Ann., vol. 114 (1937), pp. 84—98.

[5] *Die Gruppe der zentralen Automorphismen einer Gruppe mit Hauptreihe*, Math. Ann., vol. 114 (1937), pp. 355—372.

[6] *Beiträge zur Theorie der Gruppen endlicher Ordnung*, Jahresber. Deutsch. Math. Ver., vol. 48 (1938), pp. 77—141.

FOMIN, S. B.

[1] *Über periodische Untergruppen der unendlichen abelschen Gruppen*, Mat. Sbornik, vol. 2 (1937), pp. 1007—1009.

FRASCH, H.

[1] *Die Erzeugenden der Hauptkongruenzgruppen für Primzahlstufen*, Math. Ann., vol. 108 (1933), pp. 229—252.

FREUDENTHAL, H.

[1] *Teilweise geordnete Moduln*, Proc. Akad. Wet. Amsterdam, vol. 39 (1936), pp. 641—651.

FROBENIUS, G.

[1] *Über die Kongruenz nach einem aus zwei endlichen Gruppen gebildeten Doppelmodul*, J. reine angew. Math., vol. 101 (1887), pp. 273—299.

FROBENIUS, G. and STICKELBERGER, L.

[1] *Über Gruppen von vertauschbaren Elementen*, J. reine angew. Math., vol. 86 (1879), pp. 217—262.

FUCHS (Fouxe, Fuks)-RABINOVIC, D. I.

*[1] *On a representation of a free group*, Ucenye zapiski Leningrad Univ., vol. 55 (1940), pp. 154—157.

*[2] *On the non-simplicity of locally free groups*, Mat. Sbornik, vol. 7 (1940), pp. 327—328.

*[3] *Example of a group with a finite number of generators and a finite number of relations that does not admit an isomorphic representation by matrices of finite order*, Doklady Akad. Nauk SSSR., vol. 27 (1940), pp. 425—426.

*[4] *Example of a discrete group with a finite number of generators and relations that has no complete system of linear representations*, Doklady Akad. Nauk SSSR., vol. 29 (1940), pp. 549—550.

[5] *On the determinators of an operator of the free group*, Mat. Sbornik, vol. 7 (1940), pp. 197—208.

*[6] *On the groups of automorphisms of free products* I, Mat. Sbornik, vol. 8 (1940), pp. 265—276.

*[7] *On the groups of automorphisms of free products* II, Mat. Sbornik, vol. 9, (1941), pp. 183—220.

GEORG, E.

[1] *Über den Satz von Jordan-Hölder-Schreier*, J. reine angew. Math., vol. 180 (1939), pp. 110—120.

GLIVENKO, V. I.

[1] *Théorie générale des structures*, Actualités Scient. et Ind. No. 652, Paris (1938).

GLUŠKOV, V. M.

*[1] *On the normalizers of complete subgroups in a complete group*, Doklady Akad. Nauk SSSR., vol. 71 (1950), pp. 421—424.

*[2] *On the theory of ZA-groups*, Doklady Akad. Nauk SSSR., vol. 74 (1950), pp. 885—888.

*[3] *On locally nilpotent torsion-free groups*, Doklady Akad. Nauk SSSR., vol. 80 (1951), pp. 157—160.

*[4] *On some problems in the theory of nilpotent and locally nilpotent torsion-free groups*, Mat. Sbornik, vol. 30 (1952), pp. 79—104.

GOHEEN, H.

[1] *Proof of a theorem of Hall*, Bull. Amer. Math. Soc., vol. 47 (1941), pp. 143—144.

GOL'BERG, P. A.

*[1] *Infinite semi-simple groups*, Mat. Sbornik, vol. 17 (1945), pp. 131—142.

*[2] *Sylow Π-subgroups of locally normal groups*, Mat. Sbornik, vol. 19 (1946), pp. 451—460.

*[3] *Sylow bases of Π-separable groups*, Doklady Akad. Nauk SSSR., vol. 64 (1949), pp. 615—618.

GOL'FAND, YU. A.

*[1] *On the isomorphism of group extensions*, Doklady Akad. Nauk SSSR., vol. 60 (1948), pp. 1123—1125.

*[2] *Metaspecial groups*, Mat. Sbornik, vol. 27 (1950), pp. 229—248.

*[3] *On the automorphism group of the holomorph of a group*, Mat. Sbornik, vol. 27 (1950), pp. 333—350.

GOLOVIN, O. N.

*[1] *Factors without centers in direct decompositions of groups*, Mat. Sbornik, vol. 6 (1939), pp. 423—426.

*[2] *On associative operations in the set of groups*, Doklady Akad. Nauk SSSR., vol. 58 (1947), pp. 1257—1260.

*[3] *Nilpotent products of groups*, Mat. Sbornik vol. 27 (1950), pp. 427—454.

*[4] *Metabelian products of groups*, Mat. Sbornik, vol. 28 (1951), pp. 431—444.

*[5] *On the problem of an isomorphism of nilpotent decompositions of a group*, Mat. Sbornik, vol. 28 (1951), pp. 445—452.

[3]—[5] English translation of above: Russian Translation Project, Amer. Math. Soc.

GOLOVIN, O. N. and SADOVSKIĬ, L. E.

*[1] *On the automorphism groups of free products*, Mat. Sbornik, vol. 4 (1938), pp. 505—514.

GRAEV, M. I.

*[1] *On the theory of complete direct products of groups*, Mat. Sbornik, vol. 17 (1945), pp. 85—104.

*[2] *Direct sums of cycles in modular lattices*, Mat. Sbornik, vol. 19 (1946), pp. 439—450.

*[3] *Isomorphisms of direct decompositions in modular lattices*, Izvestiya Akad. Nauk SSSR. Ser. Mat., vol. 11 (1947), pp. 33—46.

GRÜN, O.

[1] *Beiträge zur Gruppentheorie*, I, J. reine angew. Math., vol. 174 (1935), pp. 1—14.

[2] *Über eine Faktorgruppe freier Gruppen*, I, Deutsche Math., vol. 1 (1936), pp. 772—782.

[3] *Zusammenhang zwischen Potenzbildung und Kommutatorbildung*, J. reine angew. Math., vol. 182 (1940), pp. 158—177.

[4] *Beiträge zur Gruppentheorie*, II, J. reine angew. Math., vol. 186 (1948), pp. 165—169.

[5] *Beiträge zur Gruppentheorie*, III, Math. Nachr., vol. 1 (1948), pp. 1—24.

[6] *Beiträge zur Gruppentheorie*, IV, Math. Nachr., vol. 3 (1949), pp. 77—94.

GRUŠKO, I. A.

*[1] *Solution of the word problem in groups with certain relations of a special form*, Mat. Sbornik, vol. 3 (1938), pp. 543—551.

*[2] *On the bases of a free product of groups*, Mat. Sbornik, vol. 8 (1940), pp. 169—182.

GUHA, U.

[1] *On the endomorphic mapping* $\{m\}$ *of a group*, Bull. Calcutta Math. Soc., vol. 38 (1946), pp. 101—107.

HAAR, A.

[1] *Über unendliche kommutative Gruppen*, Math. Zeit., vol. 33 (1931), pp. 129—159.

[2] *Über die Gruppencharaktere gewisser unendlicher Gruppen*, Acta Litt. Sci. Szeged, vol. 5 (1932), pp. 172—186.

HAIMO, F.

†[1] *Preservation of divisibility in quotient groups*, Duke Math. J., vol. 15 (1948), pp. 347—356.

HALL, M.

[1] *Group rings and extensions*, I, Ann. of Math., vol. 39 (1938), pp. 220—234.

[2] *Coset representations in free groups*, Trans. Amer. Math. Soc., vol. 67 (1949), pp. 421—432.

[3] *Subgroups of finite index in free groups*, Canadian J. Math., vol. 1 (1949), pp. 187—190.

[4] *A topology for free groups and related groups*, Ann. of Math., vol. 52 (1950), pp. 127—139.

HALL, M. and RADO, T.

[1] *On Schreier systems in free groups*, Trans. Amer. Math. Soc., vol. 64 (1948), pp. 386—408.

HALL, P.

[1] *A note on soluble groups*, J. London Math Soc., vol. 3 (1928), pp. 98—105.

[2] *A contribution to the theory of groups of prime-power order*, Proc. London Math. Soc., vol. 36 (1933), pp. 29—95.

[3] *On a theorem of Frobenius*, Proc. London Math. Soc., vol. 40 (1935), pp. 468—501.

[4] *A characteristic property of soluble groups*, J. London Math. Soc., vol. 12 (1937), pp. 198—200.

[5] *Complemented groups*, J. London Math. Soc., vol. 12 (1937), pp. 201—204.

[6] *On the Sylow systems of a soluble group*, Proc. London Math. Soc., vol. 43 (1937), pp. 316—323.

[7] *The classification of prime-power groups*, J. reine angew. Math., vol. 182 (1940), pp. 130—141.

[8] *Verbal and marginal subgroups*, J. reine angew. Math., vol. 182 (1940), pp. 156—157.

[9] *On groups of automorphisms*, J. reine angew. Math., vol. 182 (1940), pp. 194—204.

[10] *The construction of soluble groups*, J. reine angew. Math., vol. 182 (1940), pp. 206—214.

HIGMAN, G.

[1] *Note on a theorem of R. Baer*, Proc. Cambr. Phil. Soc., vol. 45 (1949), pp. 321—327.

[2] *A finitely related group with an isomorphic proper factor group*, J. London Math. Soc., vol. 26 (1951), pp. 59—61.

[3] *A finitely generated infinite simple group*, J. London Math. Soc., vol. 26 (1951), pp. 61—64.

†[4] *Unrestricted free products, and varieties of topological groups*, J. London Math. Soc., vol. 27 (1952), pp. 73—81.

HIGMAN, G, NEUMANN, B. H., and NEUMANN, H.

[1] *Embedding theorems for groups*, J. London Math. Soc., vol. 24 (1949), pp. 247—254.

HIGMAN, G. and STONE, A. H.

†[1] *On inverse systems with trivial limits*, J. London Math. Soc., vol. 29 (1954), pp. 233—236.

HIRSCH, K. A.

[1] *On infinite soluble groups*, I, Proc. London Math. Soc., vol. 44 (1938), pp. 53—60.

[2] *On infinite soluble groups*, II, Proc. London Math. Soc., vol. 44 (1938), pp. 336—344.

[3] *On skew-groups*, Proc. London Math. Soc., vol. 45 (1939), pp. 357—368.

[4] *On infinite soluble groups*, III, Proc. London Math. Soc., vol. 49 (1946), pp. 184—194.

[5] *Eine kennzeichnende Eigenschaft nilpotenter Gruppen*, Math. Nachr., vol. 4 (1951), pp. 47—49.

HÖLDER, O.

[1] *Die Gruppen der Ordnungen* p^3, pq^2, pqr, p^4, Math. Ann., vol. 43 (1893), pp. 301—412.

[2] *Bildung zusammengesetzter Gruppen*, Math. Ann., vol. 46 (1895), pp. 321—422.

HOPKINS, C.

[1] *Non-abelian groups whose groups of isomorphisms are abelian*, Ann. of Math., vol. 29 (1928), pp. 508—520.

[2] *An extension of a theorem of Remak*, Ann. of Math., vol. 40 (1939), pp. 636—638.

HUREWICZ, W.

[1] *Zu einer Arbeit von O. Schreier*, Hamburg. Abh., vol. 8 (1930), pp. 307—314.

IWASAWA, K.

[1] *Über die endichen Gruppen und die Verbände ihrer Untergruppen*, J. Fac. Sci. Imp. Univ. Tokyo, vol. 4 (1941), pp. 171—199.

[2] *Einige Sätze über freie Gruppen*, Proc. Acad. Tokyo, vol. 19 (1943), pp. 272—274.

[3] *On the structure of infinite M-groups*, Jap. J. Math., vol. 18 (1943), pp. 709—728.

JABBER, M. A.

[1] *On S-groups*, Bull. Calcutta Math. Soc., vol. 35 (1943), pp. 111—113.

JENNINGS, S. A.

[1] *A note on chain conditions in nilpotent rings and groups*, Bull. Amer. Math. Soc., vol. 50 (1944), pp. 759—763.

JONES, A. W.

[1] *The lattice isomorphisms of certain finite groups*, Duke Math. J., vol. 12 (1945), pp. 541—560.

KALAŠNIKOV, V. A. and KUROŠ, A. G.

*[1] *Free products of groups with amalgamated subgroups of the centers*, Doklady Akad. Nauk SSSR. (1935), No. 5, pp. 285—286.

KALOUJNINE, L.

[1] *Bemerkung zu einer Arbeit von Herrn A. Kurosch*, Hamburg, Abh., vol. 12 (1938), pp. 247—255.

[2] *Une méthode de construction de sous-groupes infra-invariants*, C. R. Acad. Sci. Paris, vol. 208 (1939), pp. 1869—1871.

[3] *Sur les p-groupes de Sylow du groupe symétrique du degré p^m*, C. R. Acad. Sci. Paris, vol. 221 (1945), pp. 222—224.

[4] *La structure du p-gruope de Sylow du groupe symétrique du degré p^3*, C. R. Acad. Sci. Paris, vol. 222 (1946), 1424—1425.

[5] *Sur les p-groupes de Sylow du groupe symétrique du degré p^m, (Suite centrale ascendante et descendante)*, C. R. Acad. Sci. Paris, vol. 223 (1946), pp. 703—705.

[6] *Sur les p-groupes de Sylow du groupe symétrique de degré p^m, (Sous-groupes caractéristiques, sous-groupes parallelotopiques)*, C. R. Acad. Sci. Paris. vol. 224 (1947), pp. 253—255.

[7] *Sur le groupe P_∞ des tableaux infinis*, C. R. Acad. Sci. Paris, vol. 224 (1947), pp. 1097—1099.

[8] *Sur les groupes abéliens primaires sans éléments de hauteur infinie*, C. R. Acad. Sci. Paris, vol. 225 (1947), pp. 713—715.

[9] *Sur les sous-groupes centraux d'un produit complet de groupes abéliens*, C. R. Acad. Sci. Paris, vol. 229 (1949), pp. 1289—1291.

[10] *Caractérisation des certains sous-groupes centraux d'un produit complet de groupes abéliens*, C. R. Acad. Sci. Paris, vol. 230 (1950), pp. 1633—1634.

[11] *Sur quelques propriétés des groupes d'automorphismes d'un groupe abstrait*, C. R. Acad. Sci. Paris, vol. 230 (1950), pp. 2067—2069.

[12] *Sur quelques propriétés des groupes d'automorphismes d'un groupe abstrait (Généralisation d'un théorème de M. Ph. Hall)*, C. R. Acad. Sci. Paris, vol. 231 (1950), pp. 400—402.

KALOUJNINE, L. and KRASNER, M.

[1] *Le produit complet des groupes de permutations et le problème d'extension des groupes*, C. R. Acad. Sci. Paris, vol. 227 (1948), pp. 806—808.

[2] *Produit complet des groupes de permutations et problème d'extension des groupes*, Acta Sci. Math., Szeged, vol. 13 (1950), pp. 208—230; vol. 14 (1951), pp. 39—66, 69—82.

KAPLANSKY, I.

[1] *A note on groups without isomorphic subgroups*, Bull. Amer. Math. Soc., vol. 51 (1945), pp. 529—530.

[2] *Elementary divisors and modules*, Trans. Amer. Math. Soc., vol. 66 (1949), pp. 464—491.

†[3] *Infinite Abelian Groups*, Univ. of Michigan Publ. in Math., No. 2 (1954).

KAPLANSKY, I. and MACKEY, G. W.

†[1] *A generalization of Ulm's Theorem*, Summa Brasil. Math., vol. 2 (1951), pp. 195—202.

KASAČKOV, B. V.

*[1] *On theorems of Sylow's type*, Doklady Akad. Nauk SSSR., vol. 80 (1951), pp. 5—7

*[2] *On a local theorem in the theory of groups*, Doklady Akad. Nauk SSSR., vol. 83 (1952), pp. 525—528.

KEMHADZE, S. S.

*[1] *On the regularity of p-groups for $p=2$*, Soobšč. Akad. Nauk Gruzim SSSR., vol. 11 (1950), pp. 607—611.

*[2] *Uniqueness bases in infinite regular p-groups*, Ukrain. Mat. Ž., vol. 4 (1952), pp. 57—64.

KIOKEMEISTER, F.

[1] *A note on the Schmidt-Remak theorem*, Bull. Amer. Math. Soc., vol. 53 (1947), pp. 957—958.

KIŠKINA, Z. M.

*[1] *Endomorphisms of torsion-free p-primitive abelian groups*, Izvestiya Akad. Nauk SSSR. Ser. Mat., vol. 9 (1945), pp. 201—232.

KONTOROVIČ, P. G.

*[1] *On some properties of semi-simple products*, Doklady Akad. Nauk SSSR., vol. 22 (1939), pp. 557—559.

*[2] *Invariantly covered groups*, Mat. Sbornik, vol. 8 (1940), pp. 423—430.

*[3] *Groups with a separation basis*, I, Mat. Sbornik, vol. 12 (1943), pp. 56—70.

*[4] *Groups with a separation basis*, II, Mat. Sbornik, vol. 19 (1946), pp. 287—308.

*[5] *Groups with a separation basis*, III, Mat. Sbornik, vol. 22 (1948), pp. 79—100.

*[6] *Groups with a separation basis*, IV, Mat. Sbornik, vol. 26 (1950), pp. 311—320.

*[7] *On the theory of noncommutative torsion-free groups*, Doklady Akad. Nauk SSSR., vol. 59 (1948), pp. 213—216.

*[8] *Invariantly covered groups*, II, Mat. Sbornik, vol. 28 (1951), pp. 79—88.

KOŘINEK, V.

[1] *Sur la décomposition d'un groupe en produit direct des sousgroupes*, Čas. mat. fys., vol. 66 (1937), pp. 261—286; vol. 67 (1938), pp. 209—210.

[2] *Les groupes qui ne contiennent pas des sousgroupes caractéristiques propres*, Věstn. Kral Česke Spol. Nauk (1938), pp. 1—20.

[3] *Bemerkung über charakteristisch einfache Gruppen*, Věstn. Kral. Česke Spol. (1940), pp. 1—8.

[4] *Der Schreiersche Satz und das Zassenhaussche Verfahren in Verbänden*, Věstn. Kral Česke Spol. Nauk (1941), pp. 1—29.

KÖTHE, G.

[1] *Verallgemeinerte Abelsche Gruppen mit hyperkomplexem Operatorenring*, Math. Zeit., vol. 39 (1934), pp. 31—44.

KRASNER, M.

[1] *Une généralisation de la notion de sous-groupe invariant*, C. R. Acad. Sci. Paris, vol. 208 (1939), pp. 1867—1869.

KRULL, W.

[1] *Über verallgemeinerte endliche Abelsche Gruppen*, Math. Zeit., vol. 23 (1925), pp. 161—196.

[2] *Theorie und Anwendung der verallgemeinerten Abelschen Gruppen*, S.-B. Heidelberger Akad. Wiss. Math. Nat. Kl. (1926), pp. 1—32.

[3] *Matrizen, Moduln und verallgemeinerte Abelsche Gruppen in Bereich der ganzen algebraischen Zahlen*, S.-B. Heidelberger Akad. Wiss. Math. Nat. Kl. 2. Abh. (Beitr. zur Algebra, 19), pp. 13—38.

KULAKOV, A. A.

[1] *Über die Anzahl der eigentlichen Untergruppen und der Elemente von gegebener Ordnung in p-Gruppen*, Math. Ann., vol. 104 (1931), pp. 778—793.

KULIKOV, L. YA.

*[1] *On the theory of abelian groups of arbitrary cardinal number*, Mat. Sbornik, vol. 9 (1941), pp. 165—182.

*[2] *On the theory of abelian groups of arbitrary cardinal number*, Mat. Sbornik, vol. 16 (1945), pp. 129—162.

†*[3] *On direct decompositions of groups*, Ukrain. Mat. Ž., vol. 4 (1952), pp. 230—275, 347—372.

†[3] English translation of above: Russian Translation Project, Amer. Math. Soc.

KUROŠ, A. G.

[1] *Zur Zerlegung unendlicher Gruppen*, Math. Ann., vol. 106 (1932, pp. 107—113.

[2] *Über freie Produke von Gruppen*, Math. Ann., vol. 108 (1933), pp. 26—36.

[3] *Die Untergruppen der freien Produkte von beliebigen Gruppen*, Math. Ann., vol. 109 (1934), pp. 647—660.

[4] *Eine Verallgemeinerung des Jordan-Hölderschen Satzes*, Math. Ann., vol. 111 (1935), pp. 13—18.

[5] *Über absolute Eindeutigkeit der direkten Produktzerlegungen einer Gruppe*, Mat. Sbornik, vol. 1 (1936), pp. 345—350.

[6] *Primitive torsionsfreie abelsche Gruppen vom endlichen Range*, Ann. of Math., vol. 38 (1937), pp. 175—203.

*[7] *Some recent trends and some outstanding problems in the theory of infinite groups*, Uspehi Mat. Nauk, vol. 3 (1937), pp. 5—15.

[8] *Zum Zerlegungsproblem der Theorie der freien Produkte*, Mat. Sbornik, vol. 2 (1937), pp. 995—1001.

*[9] *Some remarks on the theory of infinite groups*, Mat. Sbornik, vol. 5 (1939), pp. 347—354.

*[10] *Locally free groups*, Doklady Akad. Nauk SSSR., vol. 24 (1939), pp. 99—101.

*[11] *The Jordan-Hölder Theorem in arbitrary lattices*, Sbornik pamyati akad. Grave (1940), pp. 110—116.

*[12] *On the theory of partially ordered systems of finite sets*, Mat. Sbornik, vol. 5 (1939), pp. 343—346.

*[13] *Isomorphisms of direct decompositions*, Izvestiya Akad. Nauk SSSR. Ser. Mat., vol. 7 (1943), pp. 185—202.

*[14] *Composition systems in infinite groups*, Mat. Sbornik, vol. 16 (1945), pp. 59—72.

*[15] *Sylow subgroups of zero-dimensional topological groups*, Izvestiya Akad. Nauk SSSR. Ser. Mat., vol. 9 (1945), pp. 65—78.

*[16] *Isomorphisms of direct decompositions*, II, Izvestiya Akad. Nauk SSSR. Ser. Mat., vol. 10 (1946), pp. 47—72.

KUROŠ, A. G. and ČERNIKOV, S. N.

✓*[1] *Solvable and nilpotent groups*, Uspehi, Mat. Nauk, vol. 2: 3 (1947), pp. 18—59.

[1] English translation of above: T 94, Russian Translation Project, Amer. Math. Soc.

LEVI, F.

[1] *Abelsche Gruppen mit abzählbaren Elementen*, Dissertation, Leipzig (1917).

[2] *Über die Untergruppen freier Gruppen*, Math. Zeit., vol. 32 (1930), pp. 315—318.

[3] *Über die Untergruppen der freien Gruppen*, II, Math. Zeit., vol. 37 (1933), pp. 90—97.

[4] *The commutatorgroup of a free product*, J. Indian Math. Soc., vol. 4 (1940), pp. 136—144.

[5] *On the number of generators of a free product and a lemma of Alexander Kurosch*, J. Indian Math. Soc., vol. 5 (1941), pp. 149—155.

[6] *Groups in which the commutator operation satisfies certain algebraic conditions*, J. Indian Math. Soc., vol. 6 (1942), pp. 87—97.

[7] *Notes on group theory*, J. Indian Math. Soc., vol. 8 (1944), pp. 1—9, 44—56, 78—91; vol. 9 (1945), pp. 37—42.

LEVI, F. and VAN DER WAERDEN, B. L.

[1] *Über eine besondere Klasse von Gruppen*, Hamburg. Abh., vol. 9 (1932), pp. 154—158.

LEWIS, P. E.

[1] *Characters of abelian groups*, Amer. J. Math., vol. 64 (1942), pp. 81—105.

LIVŠIC, A. H.

*[1] *On the Jordan-Hölder Theorem in lattices*, Mat. Sbornik, vol. 24 (1949), pp. 227—235.

*[2] *On the theory of direct decompositions of groups*, Doklady Akad. Nauk SSSR., vol. 64 (1949), pp. 289—292.

*[3] *Direct decompositions of complete modular lattices*, Mat. Sbornik, vol. 28 (1951), pp. 481—502.

LOCHER, L.

[1] *Die Untergruppen des freien Gruppen*, Comment. Math. Helv., vol 6 (1933), pp. 76—82.

LORENZEN, P.

[1] *Ein Beitrag zur Gruppenaxiomatik*, Math. Zeit., vol. 49 (1944), pp. 313—327.

[2] *Eine Bemerkung zum Schreierschen Verfeinerungssatz*, Math. Zeit., vol. 49 (1944), pp. 647—653.

LUBELSKI (Lyubel'skiĭ), S.

[1] *Zur Verschärfung des Jordan-Hölderschen Satzes*, Mat. Sbornik, vol. 9 (1941), pp. 277—280.

LYAPIN, E. S.

[1] *Über die Ordnung der Automorphismengruppe einer endlichen Gruppe*, Mat. Sbornik, vol. 1 (1936), pp. 887—905.

*[2] *On the decomposition of torsion-free abelian groups of finite rank into a direct sum of groups of rank* 1, Mat. Sbornik, vol. 3 (1938), pp. 167—177.

*[3] *On the decomposition of abelian groups into direct sums of groups of rank* 1, Izvestiya Akad. Nauk SSSR. Ser. Mat. (1939), pp. 141—148.

*[4] *Some properties of decompositions of torsion-free abelian groups into direct sums*, Doklady Akad. Nauk SSSR., vol. 24 (1939), pp. 8—10.

*[5] *Decomposition of countable torsion-free abelian groups into direct sums of groups of rank* 1, Doklady Akad. Nauk SSSR., vol. 24 (1939), pp. 11—13.

*[6] *On the decomposition of abelian groups into direct sums of rational groups*, Mat. Sbornik, vol. 8 (1940), pp. 205—237.

[6] English translation of above: Russian Translation Project, Amer. Math. Soc.

*[7] *Complete operations in classes of associative systems and groups*, Ucenye Zapiski Ped. Inst. Herzen, Leningrad, vol. 86 (1949), pp. 93—106.

LYNDON, R. C.

[1] *The cohomology theory of group extensions*, Duke Math. J., vol. 15 (1948), pp. 271—292.

[2] *New proof for a theorem of Eilenberg and MacLane*, Ann. of Math., vol. 50 (1949), pp. 731—735.

[3] *Cohomology theory of groups with a single defining relation*, Ann. of Math., vol. 52 (1950), pp. 650—665.

MACLANE, S.

[1] *Cohomology theory in abstract groups*, III, Ann. of Math., vol. 50 (1949), pp. 736-761.

[2] *Duality for groups*, Bull. Amer. Math. Soc., vol. 56 (1950), pp. 485—516.

MAGNUS, W.

[1] *Über diskontinuierliche Gruppen mit einer definierenden Relation (Der Freiheitssatz)*, J. reine angew. Math., vol. 163 (1930), pp. 141—165.

[2] *Untersuchungen über einige unendliche diskontinuierliche Gruppen*, Math. Ann., vol. 105 (1931), pp. 52—74.

[3] *Das Identitätsproblem für Gruppen mit einer definierenden Relation*, Math. Ann., vol. 106 (1932), pp. 295—307.

[4] *Über n-dimensionale Gittertransformationen*, Acta Math., vol. 64 (1935), pp. 353—367.

[5] *Über den Beweis des Hauptidealsatzes*, J. reine angew. Math., vol. 170 (1934), pp. 235—240.

[6] *Beziehungen zwischen Gruppen und Idealen in einem speziellen Ring*, Math. Ann., vol. 111 (1935), pp. 259—280.

[7] *Über Beziehungen zwischen höheren Kommutatoren*, J. reine angew. Math., vol. 177 (1937), pp. 105—115.

[8] *Neuere Ergebnisse über auflösbare Gruppen*, Jber. Deutsch. Math. Verein, vol. 47 (1937), pp. 69—78.

[9] *Über freie Faktorgruppen und freie Untergruppen gegebener Gruppen*, Monatsh. Math. Phys., vol. 47 (1939), pp. 307—313.

[10] *On a theorem of Marshall Hall*, Ann. of Math., vol. 40 (1939), pp. 764—768.

[11] *Allgemeine Gruppentheorie*, Enzyklopadie der math. Wiss., 2. Aufl. (1939).

[12] *Über Gruppen und zugeordnete Liesche Ringe*, J. reine angew. Math, vol. 182 (1940), pp. 142—149.

[13] *A connection between the Baker-Hausdorff formula and a problem of Burnside*, Ann of Math., vol. 52 (1950), pp. 111—126.

MAL'CEV, A. I.

*[1] *Torsion-free abelian groups of finite rank*, Mat. Sbornik, vol. 4 (1938), pp. 45—68.

*[2] *On isomorphic representations of infinite groups by matrices*, Mat. Sbornik, vol. 8 (1940), pp. 405—422.

*[3] *On a general method of obtaining local theorems in the theory of groups*, Učenye Zapiski Ivan. Ped. Inst. Phys. Mat. Fac., vol 1 (1941), pp. 3—9.

*[4] *On groups of finite rank*, Mat. Sbornik, vol. 22 (1948), pp. 351—352.

*[5] *On a class of homogeneous spaces*, Izvestiya Akad. Nauk SSSR. Ser. Mat., vol. 13 (1949), pp. 9—32.

*[6] *Nilpotent torsion-free groups*, Izvestiya Akad. Nauk SSSR. Ser. Mat., vol. 13 (1949), pp. 201—212.

*[7] *Generalized nilpotent algebras and their adjoint groups*, Mat. Sbornik, vol. 25 (1949), pp. 347—366.

*[8] *On infinite solvable groups*, Doklady Akad. Nauk SSSR., vol. 67 (1949), pp. 23—25.

*[9] *On algebras with identical defining relations*, Mat. Sbornik, vol. 26 (1950), pp. 19—33.

*[10] *On some classes of infinite solvable groups*, Mat. Sbornik, vol. 28 (1951), pp. 567—588.

MEIER-WUNDERLI, H.

[1] *Über endliche p-Gruppen, deren Elemente der Gleichung* $x^p = 1$ *genügen*, Comment. Math. Helv., vol. 24(1950), pp. 18—45.

MILLS, W. H.

[1] *Multiple holomorphs of finitely generated abelian groups*, Trans. Amer. Math. Soc., vol. 71 (1951), pp. 379—392.

†[2] *On the non-isomorphism of certain holomorphs*, Trans. Amer. Math Soc., vol. 74 (1953), pp. 428—443.

MIŠINA, A. P.

*[1] *On complete direct sums of torsion-free abelian groups of rank* 1, Ukrain. Mat. Ž., vol. 2 (1950), pp. 64—70.

*[2] *Some conditions for the splitting of mixed abelian groups*, Ukrain. Mat. Ž., vol. 3 (1951), pp. 218—232.

MUHAMMEDZAN, H. H.

*[1] *On the theory of infinite groups with ascending central series*, Doklady Akad. Nauk SSSR., vol. 65 (1949), pp. 269—272.

*[2] *On groups with ascending central series*, Mat. Sbornik, vol. 28 (1951), pp. 185—196.

MYAGKOVA, N. N.

*[1] *On groups of finite rank*, Izvestiya Akad. Nauk SSSR. Ser. Mat., vol. 13 (1949), pp. 495—512.

NAGAO, H.

[1] *Über die Beziehungen zwischen dem Erweiterungssatz von O. Schreier und dem von K. Shoda*, Proc. Japan Acad., vol. 21 (1945), pp. 359—362.

NEUMANN, B. H.

[1] *Die Automorphismengruppe der freien Gruppen*, Math. Ann., vol. 107 (1932), pp. 367—386.

[2] *Über ein gruppentheoretisch-arithmetisches Problem*, S.-B. Preuss Akad. (1933), pp. 429—444.

[3] *Decomposition of groups*, J. London Math. Soc., vol. 10 (1935), pp. 3—6.

[4] *Identical relations in groups*, I, Math. Ann., vol. 114 (1937), pp. 506—525.

[5] *Some remarks on infinite groups*, J. London Math. Soc., vol. 12 (1937), pp. 120—127.

[6] *Groups whose elements have bounded orders*, J. London Math. Soc., vol. 12 (1937), pp. 195—198.

[7] *Adjunction of elements to groups*, J. London Math. Soc., vol. 18 (1943), pp. 4—11.

[8] *On the number of generators of a free product*, J. London Math. Soc., vol. 18 (1943), pp. 12—20.

[9] *A two-generator group isomorphic to a proper factor group*, J. London Math. Soc., vol. 25 (1950), pp. 247—248.

[10] *On a special class of infinite groups*, Nieuw Archief voor Wiskunde, vol. 23 (1950), pp. 117—127.

NEUMANN, B. H. and NEUMANN, H.

[1] *A remark on generalized free products*, J. London Math. Soc., vol. 25 (1950), pp. 202—204.

[2] *Zwei Klassen charakteristischer Untergruppen und ihre Faktorgruppen*, Math. Nachr., vol. 4 (1951), pp. 106—125.

NEUMANN, H.

[1] *Generalized free products with amalgamated subgroups*, Amer. J. Math., vol. 70 (1948), pp. 590—625; vol. 71 (1949), pp. 491—540.

[2] *Generalized free sums of cyclical groups*, Amer. J. Math., vol. 72 (1950), pp. 671—685.

[3] *On an amalgam of abelian groups*, J. London Math. Soc., vol. 26 (1951), pp. 228—232.

NIELSEN, J.

[1] *Die Isomorphismen der allgemeinen, unendlichen Gruppe mit zwei Erzeugenden*, Math. Ann., vol. 78 (1917), pp. 385—397.

[2] *Über die Isomorphismen unendlicher Gruppen ohne Relation*, Math. Ann., vol. 79 (1918), pp. 269—272.

[3] *Om Regning med ikke-kommutative Faktorer og dens Anvendelse i Gruppeteorien*, Mat. Tidsskrift B, (1921), pp. 77—94.

[4] *Die Isomorphismengruppe der freien Gruppen*, Math. Ann., vol. 91 (1924), pp. 169—209.

NISNEVIČ, V. L.

*[1] *On groups that have an isomorphic representation by matrices over a commutative field*, Mat. Sbornik, vol. 8 (1940), pp. 395—404.

NOVIKOV, P. S.

*[1] *On the algorithmic insolvability of the identity problem*, Doklady Akad. Nauk SSSR., vol. 85 (1952), pp. 709—712.

ORE, O.

[1] *On the foundation of abstract algebra*, I, Ann. of Math., vol. 36 (1935), pp. 406—437.

[2] *On the foundation of abstract algebra*, II, Ann. of Math., vol. 37 (1936), pp. 265—292.

[3] *Direct decompositions*, Duke Math. J., vol. 2 (1936), pp. 581—596.

[4] *Structures and group theory*, I, Duke Math. J., vol. 3 (1937), pp. 149—174.

[5] *On the theorem of Jordan-Hölder*, Trans. Amer. Math. Soc., vol. 41 (1937), pp. 266—275.

[6] *Structures and group theory*, II, Duke Math. J., vol. 4 (1938), pp. 247—269.

[7] *On the application of structure theory to groups*, Bull. Amer. Math. Soc., vol. 44 (1938), pp. 801—806.

[8] *A remark on the normal decompositions of groups*, Duke Math. J., vol. 5 (1939), pp. 172—173.

[9] *Contributions to the theory of groups of finite order*, Duke Math. J., vol. 5 (1939), pp. 431—460.

[10] *A remark on groups which are the direct product of their Sylow groups*, Monatsh. Math. Phys., vol. 48 (1939), pp. 41—42.

[11] *Theory of monomial groups*, Trans. Amer. Math. Soc., vol. 51 (1942), pp. 15—64.

[12] *Some remarks on commutators*, Proc. Amer. Math. Soc., vol. 2 (1951), pp. 307—314.

PEIFFER, R.

[1] *Über Identitäten zwischen Relationen*, Math. Ann., vol. 121 (1949), pp. 67—99.

PETROPAVLOVSKAYA, P. V.

*[1] *On the determination of a group by the lattice of its subsystems*, Mat. Sbornik, vol. 29 (1951), pp. 63—78.

PICKERT, G.

[1] *Remaksche Zerlegung für Gruppen mit Paarungen*, Math. Zeit., vol. 53 (1951), pp. 456—462.

PLOTKIN, B. I.

*[1] *On the theory of non-commutative torsion-free groups*, Doklady Akad. Nauk SSSR., vol. 73 (1950), pp. 655—657.

*[2] *On the theory of locally nilpotent groups*, Doklady Akad. Nauk SSSR., vol. 76 (1951), pp. 639—641.

*[3] *On the theory of non-commutative torsion-free groups*, Mat. Sbornik, vol. 30 (1952), pp. 197—212.

PONTRYAGIN, L. S.

[1] *The theory of topological commutative groups*, Ann. of Math., vol. 35 (1934), pp. 361—388.

PRÜFER, H.

[1] *Unendliche Abelsche Gruppen von Elementen endlicher Ordnung*, Dissertation (1921).

[2] *Untersuchungen über die Zerlegbarkeit der abzählbaren primären Abelschen Gruppen*, Math. Zeit., vol. 17 (1923), pp. 35—61.

[3] *Theorie der Abelschen Gruppen*, I, Math. Zeit., vol. 20 (1924), pp. 165—187.

[4] *Theorie der Abelschen Gruppen*, II, Math. Zeit., vol. 22 (1925), pp. 222—249.

REIDEMEISTER, K.

[1] *Knoten und Gruppen*, Hamburg. Abh., vol. 5 (1926), pp. 7—23.

[2] *Über unendliche diskrete Gruppen*, Hamburg. Abh., vol. 5 (1926), pp. 33—39.

[3] *Einführung in die komkinatorische Topologie*, Braunschweig (1932), New York [Chelsea] (1953).

[4] *Über Identitäten von Relationen*, Hamburg. Abh., vol. 16 (1949), pp. 114—118.

RELLA, T.

[1] *Über Abelsche Operatorgruppen*, J. reine angew. Math., vol. 167 (1932), pp. 235—247.

REMAK, R.

[1] *Über die Zerlegung der endlichen Gruppen in direkte unzerlegbare Faktoren*, J. reine angew. Math., vol. 139 (1911), pp. 293—308.

[2] *Über die Zerlegung der endlichen Gruppen in direkte unzerlegbare Faktoren*, J. reine angew. Math., vol. 153 (1923), pp. 131—140.

[3] *Über die Darstellung der endlichen Gruppen als Untergruppen direkter Produkte*, J. reine angew. Math., vol. 163 (1930), pp. 1—44.

[4] *Über die erzeugenden invarianten Untergruppen der subdirekten Darstellungen endlicher Gruppen*, J. reine angew. Math., vol. 164 (1931) pp. 197—242.

[5] *Über Untergruppen direkter Produkte von drei Faktoren*, J. reine angew. Math., vol. 166 (1931), pp. 65—100.

ROTTLAENDER, A.

[1] *Nachweis der Existenz nicht-isomorpher Gruppen von gleicher Situation der Untergruppen*, Math. Zeit., vol. 28 (1928), pp. 641—653.

SADOVSKIĬ, L. E.

*[1] *On lattice isomorphisms of free groups*, Doklady Akad. Nauk SSSR., vol. 32 (1941), pp. 171—174.

*[2] *Lattice isomorphisms of free groups and free products*, Mat. Sbornik, vol. 14 (1944), pp. 155—173.

*[3] *On lattice isomorphisms of free products of groups*, Mat. Sbornik, vol. 21 (1947), pp. 63—82.

SANOV, I. N.

*[1] *Solution of the Burnside problem for the exponent* 4, Ucenye Zapiski Leningrad Univ., vol. 55 (1940), pp. 166—170.

*[2] *A property of a certain representation of a free group*, Doklady Akad. Nauk SSSR., vol. 57 (1947), pp. 657—659.

*[3] *On the Burnside problem*, Doklady Akad. Nauk SSSR., vol. 57 (1947), pp. 759—761.

*[4] *On a system of relations in periodic groups with prime power periods*, Izvestiya Akad. Nauk SSSR. Ser. Mat., vol. 15 (1951), pp. 477—502.

*[5] *A connection between periodic groups with prime power periods and Lie rings*, Izvestiya Akad. Nauk SSSR. Ser. Mat., vol. 16 (1952), pp. 23-58.

SATO, S.

[1] *On groups and the lattices of subgroups*, Osaka Math. J., vol. 1 (1949), pp. 135—149.

SCHMEIDLER, W.

[1] *Bemerkungen zur Theorie der abzählbaren Abelschen Gruppen*, Math. Zeit., vol. 6 (1920), pp. 274—280.

SCHMIDT, O. J. (Šmidt, O. Yu.)

[1] *Über die Zerlegung endlicher Gruppen in direkte unzerlegbare Faktoren*, Izvestiya Kiev Univ. (1912), pp. 1—6.

[2] *Sur les produits directs*, Bull. Soc. Math. France, vol. 41 (1913), pp. 161—164.

*[3] *Abstract Theory of Groups*, Kiev (1916), 2nd ed. Moscow (1933).

[4] *Über unendliche Gruppen mit endlicher Kette*, Math. Zeit., vol. 29 (1928), pp. 34—41.

*[5] *New proof of a theorem by A. Kulakov in the theory of groups*, Mat. Sbornik, vol. 39 (1932), No. 1—2, pp. 66—71.

*[6] *On infinite special groups*, Mat. Sbornik, vol. 8 (1940), pp. 363—375.

*[7] *Infinite solvable groups*, Mat. Sbornik, vol. 17 (1945), pp. 145—162.

SCHOLZ, A.

[1] *Die Behandlung der Zweistufigen Gruppe als Operatorengruppe*, S.-B. Heidelberger Akad. Wiss. Math. Nat. Kl., vol. 2 (1933), pp. 17—22.

SCHREIER, J. and ULAM, S.

[1] *Sur le groupe des permutations de la suite des nombres naturels*, C. R. Acad. Sci. Paris, vol. 197 (1933), pp. 737—738.

[2] *Über die Permutationsgruppe der natürlichen Zahlenfolge*, Studia Math., vol. 4 (1933), pp. 134—141.

[3] *Über die Automorphismen der Permutationsgruppe der natürlichen Zahlenfolge*, Fund. Math., vol. 28 (1937), pp. 258—260.

SCHREIER, O.

[1] *Über die Gruppen* $A^aB^b=1$, Hamburg. Abh., vol. 3 (1924), pp. 167—169.

[2] *Über die Erweiterung von Gruppen*, I, Monatsh. Math. Phys., vol. 34 (1926), pp. 165—180.

[3] *Über die Erweiterung von Gruppen*, II, Hamburg. Abh., vol. 4 (1926), pp. 321—346.

[4] *Die Untergruppen der freien Gruppen*, Hamburg. Abh., vol. 5 (1927) pp. 161—183.

[5] *Über den Jordan-Hölderschen Satz*, Hamburg. Abh., vol. 6 (1928), pp. 300—302.

SCHUR, I.

[1] *Über Gruppen periodischer linearer Substitutionen*, S.-B. Preuss. Akad. (1911), pp. 619—627.

[2] *Über die Darstellungen der endlichen Gruppen durch gebrochene lineare Substitutionen*, J. reine angew. Math., vol. 127 (1904), pp. 20—50.

SCOTT, W. R.

[1] *Algebraically closed groups*, Proc. Amer. Math. Soc., vol. 2 (1951), pp. 118—121.

[2] *Groups and cardinal numbers*, Amer. J. Math., vol. 74 (1952), pp. 187—197.

SEKI, T.

[1] *Über die Existenz der Zerfällungsgruppe in der Erweiterungstheorie der Gruppen*, Tôhoku Math. J., vol. 48 (1941), pp. 235—238.

SERRE, J.-P.

[1] *Cohomologie des extensions de groupes*, C. R. Acad. Sci. Paris, vol. 231 (1950), pp. 643—646.

[2] *Sur un théorème de T. Szele*, Acta. Sci. Math. Szeged, vol. 13 (1950), pp. 190—191.

SESEKIN, N. F.

*[1] *On the theory of torsion-free special groups*, Doklady Akad. Nauk SSSR., vol. 70 (1950), pp. 185—188.

SHIFFMANN, M.

[1] *The ring of automorphisms of an abelian group*, Duke Math. J., vol. 6 (1940), pp. 579—597.

SHODA, K.

[1] *Über die Automorphismen einer endlichen Abelschen Gruppe*, Math. Ann., vol. 100 (1928), pp. 674—686.

[2] *Über die charakteristischen Untergruppen einer endlichen Abelschen Gruppe*, Math. Zeit., vol. 31 (1930), pp. 611—624.

[3] *Über den Automorphismenring bzw. die Automorphismengruppe einer endlichen Abelschen Gruppe*, Proc. Acad. Tokyo, vol. 6 (1930), pp. 9—11.

[4] *Gruppentheoretischer Beweis des Äquivalenz und Enthaltenseinsatzes in der Theorie der Matrizen mit ganzen Koeffizienten*, Proc. Acad. Tokyo, vol. 6 (1930), pp. 217—219.

[5] *Über die Automorphismen einer endlichen zerlegbaren Gruppe*, J. Fac. Sci. Univ. Tokyo, vol. 2 (1930), pp. 25—50.

[6] *Über direkt zerlegbare Gruppen*, J. Fac. Sci. Univ. Tokyo, vol. 2 (1930), pp. 51—72.

[7] *Bemerkungen über vollständig reduzible Gruppen*, J. Fac. Sci. Univ. Tokyo, vol. 2 (1931), pp. 203—209.

[8] *Über die Schreiersche Erweiterungstheorie*, Proc. Acad. Tokyo, vol. 19 (1943), pp. 518—519.

SHÛ, S.

[1] *On the common representative system of residue classes of infinite groups*, J. London Math. Soc., vol. 16 (1941), pp. 101—104.

SINKOV, A.

[1] *Families of groups generated by two operators of the same order*, Trans. Amer. Math. Soc., vol. 35 (1933), pp. 372—385.

[2] *The groups determined by the relations* $S^l = T^m = (S^{-1}T^{-1}ST)^p = 1$, II, Duke Math. J., vol. 2 (1936), pp. 74—83.

[3] *On the group-defining relations* $(2, 3, 7; p)$, Ann. of Math., vol. 38 (1937), pp. 577—584.

SKOPIN, A. I.

*[1] *Factor groups of an upper central series in a free group*, Doklady Akad. Nauk SSSR., vol. 74 (1950), pp. 425—428.

SMIRNOV, D. M.

*[1] *On the theory of locally nilpotent groups*, Doklady Akad. Nauk SSSR., vol. 76 (1951), pp. 643—646.

SPECHT, W.

[1] *Eine Verallgemeinerung der Permutationsgruppen*, Math. Zeit., vol. 37 (1933), pp. 321—341.

SPEISER, A.

[1] *Die Theorie der Gruppen von endlicher Ordnung*, 1923, 2 Aufl. (1927), 3 Aufl. (1937).

STEINITZ, E.

[1] *Rechteckige Systeme und Moduln in algebraischen Zahlkörpern*, Math. Ann., vol. 71 (1912), pp. 297—345.

SULTANOV, R. M.

*[1] *On the decomposition of torsion-free abelian groups into a direct sum of cyclic groups*, Naucn. Zapiski Univ. Lvov. Ser. Phys. Mat., vol. 2 (1947), pp. 108—115.

SUZUKI, M.

[1] *On the lattice of subgroups of finite groups*, Trans. Amer. Math. Soc., vol. 70 (1951), pp. 345—371.

[2] *On the L-homomorphisms of finite groups*, Trans. Amer. Math. Soc., vol. 70 (1951), pp. 372—386.

SYLOW, L.

[1] *Théorèmes sur les groupes de substitutions*, Math. Ann., vol. 5 (1872), pp. 584—594.

SZEKERES, G.

[1] *Countable abelian groups without torsion*, Duke Math. J., vol. 15 (1948), pp. 293—306.

SZELE, T.

[1] *Sur la décomposition directe des groupes abéliens*, C. R. Acad. Sci. Paris, vol. 229 (1949), pp. 1052—1053.

[2] *Die unendliche Quaternionengruppe*, Acad. Repub. Pop. Romîne Bul. Sti. Sect. Sti. Mat. Fiz., vol. 1 (1949), pp. 799—802.

[3] *Über die Abelschen Gruppen mit nullteilerfreiem Endomorphismenring*, Publ. Math. Debrecen., vol. 1 (1949), pp. 89—91.

[4] *Die Abelschen Gruppen ohne eigentliche Endomorphismen*, Act. Sci. Math. Math. Szeged, vol. 13 (1950), pp. 54—56.

SZELE, T. and SZELPAL, I.

[1] *Über drei wichtige Gruppen*, Acta. Sci. Math. Szeged, vol. 13 (1950), pp. 192—194.

TAKAHASI, M.

[1] *Bemerkungen über den Untergruppensatz im freien Produkte*, Proc. Acad. Tokyo, vol. 20 (1944), pp. 589—594.

[2] *On partitions of free products of groups*, Osaka Math. J., vol. 1 (1949), pp. 49—51.

[3] *Note on locally free groups*, J. Osaka City Univ., vol. 1 (1950), pp. 65—70.

TARTAKOVSKIĬ, V. A.

*[1] *On the extinction process*, Doklady Akad. Nauk SSSR., vol. 58 (1947), pp. 1605—1608.

*[2] *On the identity problem for certain types of groups*, Doklady Akad. Nauk SSSR., vol. 58 (1947), pp. 1909—1910.

*[3] *The sieve method in the theory of groups*, Mat. Sbornik, vol. 25 (1949), pp. 3—50.

*[4] *Application of the sieve method to the solution of the identity problem in certain types of groups*, Mat. Sbornik, vol. 25 (1949), pp. 251—274.

*[5] *Solution of the identity problem for groups with a K-reducible basis for $K > 6$*, Izvestiya Akad. Nauk SSSR. Ser. Mat., vol. 13 (1949), pp. 483—494.

[3]—[5] English translation of above: Russian Translation Project, Amer. Math. Soc.

*[6] *On primitive composition*, Mat. Sbornik, vol. 30 (1952), pp. 39—52.

TAUSSKY, O.

[1] *Über isomorphe Abbildungen von Gruppen*, Math. Ann., vol. 108 (1933), pp. 615—620.

TEICHMÜLLER, O.

[1] *Der Elementarteilersatz für nichtkommutative Ringe*, S.-B. Preuss. Akad. (1937), pp. 169—177.

THRALL, R. M.

[1] *A note on a theorem by Witt*, Bull. Amer. Math. Soc., vol. 47 (1941), pp. 303—308.

THRELFALL, W.

[1] *Gruppenbilder*, Abh. math.-phys. klasse Sachs. Akad., vol. 41, No. 6 (1932), pp. 1—59.

TIETZE, H.

[1] *Über die topologischen Invarianten mehrdimensionaler Mannigfaltigkeiten*, Monatsh. Math. Phys., vol. 19 (1908), pp. 1—118.

TOVBIN, A. V.

*[1] *On the existence of a center in infinite and finite groups*, Doklady Akad. Nauk SSSR., vol. 31 (1941), p. 198.

TURING, A. M.

[1] *The extensions of a group*, Compositio Math., vol. 5 (1938), pp. 357—367.

ULM, H.

[1] *Zur Theorie der abzählbar-unendlichen Abelscher Gruppen*, Math. Ann., vol. 107 (1933), pp. 774—803.

[2] *Zur Theorie der nicht-abzählbaren primären Abelschen Gruppen*, Math. Zeit., vol. 40 (1935), pp. 205-207.

UZKOV, A. I.

*[1] *On the Jordan-Hölder Theorem*, Mat. Sbornik, vol. 4 (1938), pp. 31—43.

[1] English translation of above: Russian Translation Project, Amer. Math. Soc.

VAN DER WAERDEN, B. L.

[1] *Gruppen von linearen Transformationen*, Ergebnisse der Mathematik (1935), New York [Chelsea] (1949).

[2] *Free products of groups*, Amer. J. Math., vol. 70 (1948), pp. 527—528.

VAN KAMPEN, E. R.

[1] *On some lemmas in the theory of groups*, Amer. J. Math., vol. 55 (1933), pp. 268—273.

VILENKIN, N. YA.

*[1] *Direct decompositions of topological groups*, I, Mat. Sbornik, vol. 19 (1946), pp. 85—154.

WALL, G. E.

†[1] *Finite groups with class-preserving outer automorphisms*, J. London Math. Soc., vol. 22 (1947), pp. 315—320.

WEVER, F.

[1] *Über Regeln in Gruppen*, Math. Ann., vol. 122 (1950), pp. 334—339.

WHITEHEAD, J. H. C.

[1] *On certain sets of elements in a free group*, Proc. London Math. Soc., vol. 41 (1936), pp. 48—56.

[2] *On equivalent sets of elements in a free group*, Ann. of Math., vol. 37 (1936), pp. 782—800.

[3] *On group extensions with operators*, Quart. J. Math. Oxford Ser. (2), vol. 1 (1950), pp. 219—228.

WHITMAN, P. M.

[1] *Groups with a cyclic group as lattice-homomorph*, Ann. of Math., vol. 49 (1948), pp. 347—351.

WHITNEY, H.

[1] *Tensor products of abelian groups*, Duke Math. J., vol. 4 (1938), pp. 495—528.

WIELANDT, H.

[1] *Eine Kennzeichnung der direkten Produkte von p-Gruppen*, Math. Zeit., vol. 41 (1936), pp. 281—282.

[2] *Eine Verallgemeinerung der invarianten Untergruppen*, Math. Zeit., vol. 45 (1939), pp. 209—244.

[3] *p-Sylowgruppen und p-Faktorgruppen*, J. reine angew. Math., vol. 182 (1940), pp. 180—183.

WITT, E.

[1] *Treue Darstellung Liescher Ringe*, J. reine angew. Math., vol. 177 (1937), pp. 152—160.

ZAPPA, G.

[1] *Remark on a recent paper of O. Ore*, Duke Math. J., vol. 6 (1940), pp. 511—512.

[2] *Sui gruppi di Hirsch supersolubili*, Rend. Sem. Mat. Univ. Padova, vol. 12 (1941), pp. 1—11, pp. 62—80.

[3] *Sul comportamente degli elementi periodici in un gruppo di Dedekind infinito*, Comment. Math. Helv., vol. 18 (1945), pp. 42—44.

[4] *Sui sottogruppi finiti dei gruppi di Hirsch*, Giorn. Mat. Battaglini, vol. 2 (1948), pp. 55—70.

[5] *Sulla condicione perchè un emitropismo inferiore tipico tra due gruppi sia un omotropismo*, Giorn. Mat. Battaglini, vol. 4 (1951), pp. 80—101.

ZASSENHAUS, H.

[1] *Zum Satz von Jordan-Hölder-Schreier*, Hamburg. Abh., vol. 10 (1934), pp. 106—108.

[2] *Lehrbuch der Gruppentheorie*, vol. I, (1937).

[2] *The Theory of Groups*, New York [Chelsea] (1949) ; 2nd ed. [*in prep.*]

[3] *Beweis eines Satzes über diskrete Gruppen*, Hamburg. Abh., vol. 12 (1938), pp. 289—312.

ZIPPIN, L.

[1] *Countable torsion groups*, Ann. of Math., vol. 36 (1935), pp. 86—99.

INDEX

AUTHOR INDEX

INDEX

ISBN 0-8284-0107-1

9 780828 401074

CHEL/107