THE THEORY OF GROUPS

THE THEORY OF GROUPS

BY

A. G. KUROSH

TRANSLATED FROM THE RUSSIAN
AND EDITED BY

K. A. HIRSCH

VOLUME TWO

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

CONTENTS

PART THREE:

GROUP-THEORETICAL CONSTRUCTIONS

PART FOUR:

SOLVABLE AND NILPOTENT GROUPS

PART THREE

GROUP-THEORETICAL CONSTRUCTIONS

CHAPTER IX

FREE PRODUCTS AND FREE GROUPS

§ 33. Definition of a free product

The importance of the direct product of groups, introduced in § 17, has been illustrated in the chapters on abelian groups. Another equally useful construction of this type is the free product of groups. Like the direct product, the free product provides a method of constructing a new group from given groups. It differs from the direct product in that the definition does not require the elements of distinct factors to be permutable. The precise definition of a free product is as follows.

A group G is said to be the *free product* of its subgroups A_α (α ranges over some index set) if the subgroups A_α generate G, that is, if every element g of G is the product of a finite number of the elements of the A_α,

$$g = a_1 a_2 \dots a_n, \quad a_i \in A_{\alpha_i}, \quad i = 1, 2, \dots, n, \tag{1}$$

and if every element g of G, $g \neq 1$, has a *unique* representation in the form (1) subject to the condition that all the elements a_i are different from the unit element and that in (1) no two adjacent elements are in the same subgroup A_α—although the product (1) may, in general, contain several factors from one and the same subgroup.

The free product is denoted by the symbol

$$G = \prod_\alpha {}^* A_\alpha, \tag{2}$$

and if G is the free product of a finite number of subgroups $A_1, A_2, \dots, A_k$, by the symbol

$$G = A_1 * A_2 * \dots * A_k.$$

The subgroups A_α are called the *free factors* of the free decomposition (2) of G. The expression (1) (under the restrictions imposed on it) is called the *normal form* (or *irreducible representation*) of the element g in the decomposition (2), and the number n the *length* of g in this decomposition; we write $n = l(g)$.

From the uniqueness of the normal form of an element it follows that the intersection of any free factor A_α in (2) with the subgroup of G generated by the remaining factors is E.

Suppose that a group G is decomposable into the free products of proper subgroups. If (2) is such a decomposition, then we take two elements, a_1 and a_2, different from the unit element and belonging to distinct free factors of (2). From the definition of the free product it follows that the products a_1a_2 and a_2a_1 are different elements of G, so that G is necessarily non-commutative, even if all the free factors A_α in (2) are abelian. Further, all the products

$$a_1a_2,\ a_1a_2a_1a_2,\ \ldots,\ (a_1a_2)^n,\ \ldots$$

are distinct elements of G, so that G necessarily has elements of infinite order even if all the free factors A_α are periodic. So we see that *abelian groups and periodic groups (in particular, finite groups) cannot be free products.*

Among the groups that are decomposable into free products are the free groups; in fact, *a non-cyclic free group is the free product of infinite cyclic groups.* For let x_α be a system of free generators of a free group W. If $\{x_\alpha\} = A_\alpha$, then G is clearly generated by the subgroups A_α and every element of W, that is, every word in the symbols x_α can be written uniquely as a product of powers of the elements x_α. W is, therefore, the free product of its infinite cyclic subgroups A_α.[1]

As in the case of direct products we can speak of the *free product of an arbitrary collection of groups* on the basis of a construction that is a natural generalization of the construction by means of which free groups were introduced in § 18.

Let an arbitrary set of groups A_α be given. A *word* is an ordered system of elements

$$w = a_1a_2 \ldots a_n, \tag{3}$$

where the length $n \geqq 1$, where every a_i is an element, other than the unit element, of a group A_{α_i}, and where any two adjacent elements a_i and a_{i+1} belong to different groups A_α. In addition we shall regard the case $n = 0$ as corresponding to the *empty word.* If (3) and

$$w' = a_1'a_2'\ldots a_m' \tag{4}$$

[1] Note that in the case of a free group the concept of the length of an element as defined above does not coincide with the similar concept introduced in § 18.

are two words, then we define the product of w by w' in the following way: let

$$a_1' = a_n^{-1}, \quad a_2' = a_{n-1}^{-1}, \ \ldots, \ a_i' = a_{n-i+1}^{-1}, \quad 0 \leqq i \leqq \min(n, m),$$

but $a_{i+1}' \neq a_{n-i}^{-1}$. If the elements a_{n-i} and a_{i+1}' belong to distinct subgroups A_α, then we put

$$ww' = a_1 a_2 \ldots a_{n-i} a_{i+1}' a_{i+2}' \ldots a_m';$$

but if a_{n-i} and a_{i+1}' lie in the same subgroup A_α and $a_{n-i} a_{i+1}' = \overline{a}$, then

$$ww' = a_1 a_2 \ldots a_{n-i-1} \overline{a} a_{i+2}' \ldots a_m'.$$

In other words, in order to obtain the product of w by w' we write down these words in juxtaposition and then carry out the necessary *cancellations* and *contractions* (or *amalgamations*).

The empty word plays the rôle of the unit element in the multiplication of words so defined; the inverse of (3) is the word

$$w^{-1} = a_n^{-1} \ldots a_2^{-1} a_1^{-1}.$$

The proof of the associative law of multiplication, although not essentially different from the corresponding proof of § 18, is technically very complicated. We can avoid these complications in the following way (van der Waerden [2]).

We denote by M the set of all words defined above and by S_M the unrestricted symmetric group of all one-to-one mappings of M onto itself. Let A_α be one of the given groups and let a be an element of A_α other than 1. The element a defines a mapping of M into itself: if a word w with the representation (3) does not end with an element of A_α—in particular if it is empty—then we map w onto the word

$$wa = a_1 a_2 \ldots a_n a.$$

If now $a_n \in A_\alpha$ and $a_n a = a' \neq 1$, then we regard as the image of w the word

$$a_1 a_2 \ldots a_{n-1} a'.$$

Finally, if $a_n \in A_\alpha$ and $a_n a = 1$, then the image of w shall be the word

$$a_1 a_2 \ldots a_{n-1}.$$

If, however, $a = 1$, then the identity mapping of M onto itself shall correspond to a.

If b is any other element of A_α, then the mapping corresponding to ab is obviously the product of the mappings corresponding to a and to b in the sense of their being performed in succession. In particular, when the mappings corresponding to a and a^{-1} are performed in succession, then we obtain the identity mapping. Therefore, the mapping corresponding to an arbitrary element a of A_α is a one-to-one mapping of M onto itself, that is, an element of S_M. Distinct mappings correspond to distinct elements of A_α, since the mapping corresponding to a, $a \neq 1$, carries the empty word into a itself.

We have obtained an isomorphic mapping of A_α into some subgroup $\hat{A}_\alpha$ of S_M; the image of an element a under this mapping will be denoted by $\hat{a}$. We perform this process for all α, and we denote by $\hat{G}$ the subgroup of S_M generated by all the subgroups $\hat{A}_\alpha$. Every element of $\hat{G}$ can be written uniquely as a word in the elements of the $\hat{A}_\alpha$: if w is an arbitrary word of M and (3) its representation, then

$$\hat{a}_1 \hat{a}_2 \ldots \hat{a}_n$$

is the permutation that carries the empty word into precisely w. In other words, $\hat{G}$ is the free product of its subgroups $\hat{A}_\alpha$.

Multiplication in $\hat{G}$ is carried out by the same rule as was laid down in the above definition of the multiplication of words. Thus, the set M of all words now appears as a group which we denote by $\bar{G}$. The words of length 1 corresponding to the elements of one group A_α form, together with the empty word, a subgroup $\bar{A}_\alpha$ of $\bar{G}$, which is isomorphic to A_α. The isomorphism between the groups $\bar{G}$ and $\hat{G}$ shows that $\bar{G}$ is the *free product of its subgroups $\bar{A}_\alpha$, and these are isomorphic to the given groups A_α.*

We shall now show that the definition of a free product can also be put into another form that uses generators and relations.

Let

$$G = \prod_\alpha^* A_\alpha$$

and let each group A_α be given by a system[1] *of generators $\mathfrak{M}_\alpha$ and a system of defining relations Φ_α in these generators. Then the union $\mathfrak{M}$ of all the sets $\mathfrak{M}_\alpha$ is a system of generators of G, and the union Φ of all the sets Φ_α is a set of*

[1] Systems with different indices are here assumed to be disjoint. [*Trans.*]

defining relations. Conversely, if a group G is given by a system of generators $\mathfrak{M}$ and a system of defining relations Φ such that $\mathfrak{M}$ falls into disjoint proper subsystems $\mathfrak{M}_\alpha$ and Φ into disjoint subsystems Φ_α, where in Φ_α there occur only generators from the set $\mathfrak{M}_\alpha$, then G is isomorphic to the free products of the groups A_α where A_α is the group with $\mathfrak{M}_\alpha$ as a set of generators and with Φ_α as a set of defining relations.

Both parts of the theorem follow from these considerations: suppose there is given a system of disjoint sets $\mathfrak{M}_\alpha$, and, for each α, a set of relations Φ_α written by means of the symbols of $\mathfrak{M}_\alpha$. We denote the union of all the $\mathfrak{M}_\alpha$ by $\mathfrak{M}$ and the union of all the Φ_α by Φ. Then, by § 18, there exists a group G having $\mathfrak{M}$ as a system of generators and Φ as a system of defining relations. On the other hand, we denote by $\bar{A}_\alpha$ the group with $\mathfrak{M}_\alpha$ as a system of generators and Φ_α as a system of defining relations, and by $\bar{G}$ the free product of all the groups $\bar{A}_\alpha$

$$\bar{G}=\prod_\alpha{}^* \bar{A}_\alpha,$$

which exists in view of the construction described above. Then $\mathfrak{M}$ is a system of generators for $\bar{G}$, but in order to obtain a system of defining relations it may be necessary to add to Φ a number of further relations. Therefore, by von Dyck's Theorem $\bar{G}$ is isomorphic to a factor group of G. If A_α is the subgroup of G generated by $\mathfrak{M}_\alpha$ then the natural homomorphism of G onto $\bar{G}$ maps A_α homomorphically onto $\bar{A}_\alpha$. However, since all the relations of Φ_α, which is a system of defining relations for $\bar{A}_\alpha$, are also satisfied in A_α, this mapping is an isomorphism. Finally, every element of G can be written (possibly in more than one way) as a word in the elements of the $\bar{A}_\alpha$. Under the homomorphic mapping of G onto $\bar{G}$ this element goes over into the corresponding word in the elements of $\bar{A}_\alpha$. But since in G distinct words consisting of elements of $\bar{A}_\alpha$ are distinct group elements, this will hold equally in G for words consisting of elements of A_α. This proves that G and $\bar{G}$ are isomorphic.

The following is yet another approach to the concept of a free product:

If a group G is generated by subgroups A_α (where α ranges over an index set), then G is the free product of these subgroups if and only if for every group H and every set of homomorphic mappings φ_α of each A_α into H there exists a homomorphic mapping φ, of G into H, that coincides with φ_α on each A_α.

For if

$$G = \prod_{\alpha}^{*} A_{\alpha}$$

and if a group H and homomorphisms φ_{α} are given, then the required homomorphism φ is defined as follows: If

$$w = a_1 a_2 \ldots a_n$$

is a word of G and $a_i \in A_{\alpha_i}$, $i = 1, 2, \ldots, n$, then

$$w\varphi = a_1\varphi_{\alpha_1} \cdot a_2\varphi_{\alpha_2} \ldots a_n\varphi_{\alpha_n}.$$

For the proof of the converse we need only take as H the free product of the groups A_{α} in the sense of the above construction and as the homomorphism φ_{α} the identity mapping of A_{α} onto itself. The homomorphism φ whose existence is now assumed turns into an isomorphic mapping of G onto H.

Using the most convenient form of the definition each time the reader will have no difficulty in proving the following simple properties of free products:

I. *If* $G = \prod_{\alpha}^{*} A_{\alpha}$ *and if every subgroup* A_{α} *is itself a free product,* $A_{\alpha} = \prod_{\beta}^{*} B_{\alpha\beta}$, *then* G *is the free product of all* $B_{\alpha\beta}$. This new free product is called a *refinement* of the original free product.

II. *If a free decomposition of a group* G *is given, then we obtain another free decomposition if we split the set of free factors of the given decomposition into disjoint subsystems and take the products of all factors within each subsystem.* In particular, every group that is decomposable into a free product can be represented as the free product of two groups.

III. *If* $G = \prod_{\alpha}^{*} A_{\alpha}$ *and if in each factor* A_{α} *a subgroup* A_{α}' *is chosen,* $E \subseteq A_{\alpha}' \subseteq A_{\alpha}$, *then the subgroup generated in* G *by all subgroups* A_{α}' *is the free product of these subgroups.*

IV. *If* $G = A * B$ *and if* N *is the normal subgroup of* G *generated by* B, *then* $A \simeq G/N$.

For the transition to the factor group of N is equivalent to the addition of relations which equate all generators of B to the unit element. After this, however, there remain only the generators and defining relations of A.

An interesting example of a free product is the *modular group*, that is, the group of linear fractional transformations of the complex plane,

$$z' = \frac{az+b}{cz+d},$$

where a, b, c, d, are rational integers and the determinant $ad - bc = 1$. It can be shown that the modular group is the free product of two finite cyclic groups, one of order 2 and the other of order 3.[b]

§ 34. Subgroups of a free product

The following fundamental theorem on the subgroups of a free product was first proved by Kuroš [3], and again by Baer and Levi [2], Takahasi [1].[1 c]

KUROŠ'S SUBGROUP THEOREM: *If*

$$G = \prod_{\alpha}^{*} A_{\alpha} \tag{1}$$

and if H is an arbitrary subgroup of G, then there exists a free decomposition of H

$$H = F^{*} \prod_{\beta}^{*} B_{\beta},$$

where F is a free group and every B_β is conjugate in G to a subgroup of one of the free factors A_α.

Proof. Throughout the present section we shall use the terms *length* of a given element, *normal form*, and so on, with reference to the free decomposition (1) of G. Furthermore, we introduce the following definitions.

If an element g of G has even length $l(g) = 2k$, say,

$$g = a_{-k} \dots a_{-1} a_1 \dots a_k,$$

then $a_{-k} \dots a_{-1}$ will be called the *left half*, $a_1 \dots a_k$ the *right half*, of g. If $l(g) = 2k + 1$ and

$$g = a_{-k} \dots a_{-1} a_0 a_1 \dots a_k,$$

then $a_{-k} \dots a_{-1}$ will be called the *left half*, $a_1 \dots a_k$ the *right half* and a_0 the *middle*, of g. If, moreover, the left and right halves of g are inverses, so that $a_{-i} = a_i^{-1}$, $i = 1, 2, \dots, k$, then g will be called a *transform*.

[1] The author has had no access to this paper.

A transform is conjugate to its middle and has the same order. Every element of G that is not a transform has infinite order.

We now define subgroups Φ_μ of H (where μ is an ordinal number). Let $\Phi_0 = E$. If the subgroups Φ_μ have already been defined for all μ less than ν, and if K_ν is the subgroup generated by all these Φ_μ then let l_ν be the smallest length of an element of H outside K_ν. If among these elements there is a transform, then we choose one of them, $g_\nu^{-1} a g_\nu$, where $a \in A_{\alpha_\nu}$, and where the first element in the normal form of g_ν does not belong to A_{α_ν}, and we put

$$\bar{A}_\nu = H \cap g_\nu^{-1} A_{\alpha_\nu} g_\nu.$$

In particular, for $l_\nu = 1$ the chosen transform is simply an element a of some A_{α_ν} and therefore

$$\bar{A}_\nu = H \cap A_{\alpha_\nu}.$$

But if there are no transforms of length l_ν among the elements of H outside K_ν, in particular if l_ν is even, then we put $\bar{A}_\nu = E$.

We now take an element f_{ν_1} in H, but not in $\{K_\nu, \bar{A}_\nu\}$, whose right half is g_ν and whose middle, if it exists, belongs to A_{α_ν}. If $\bar{A}_\nu = E$, then f_{ν_1} shall be an arbitrary element of length l_ν in H, but not in K_ν, its right half will be denoted by g_ν and the free factor A_α in which the middle of l_ν lies (for odd l_ν) by A_{α_ν}. If the elements $f_{\nu\delta}$ have already been chosen for all ordinal numbers δ, $\delta < \sigma$, and if in H, but outside the subgroup generated by K_ν, $\bar{A}_\nu$ and by all the elements $f_{\nu\delta}$, $\delta < \sigma$, there are still elements of length l_ν having g_ν as their right half and some element of A_{α_ν} as their middle, then we denote one of these elements by $f_{\nu\sigma}$. This process stops at a certain ordinal number σ_ν. We now denote by Φ_ν the subgroup of H that is generated by $\bar{A}_\nu$ and all the elements $f_{\nu\delta}$, $\delta < \sigma_\nu$. Obviously, we then have $K_{\nu+1} = \{K_\nu, \Phi_\nu\}$, and when λ is a limit ordinal number K_λ is the union of the ascending sequence of subgroups K_ν, $\nu < \lambda$. The process of constructing subgroups Φ_μ and K_ν comes to an end at an ordinal number τ such that $K_\tau = H$.

We shall take as *generators* of Φ_μ the elements $f_{\mu\delta}$, $\delta < \sigma_\mu$, the elements $f_{\mu\delta}^{-1}$, and also all the elements of $\bar{A}_\mu$, except 1. We shall take as generators of K_ν the generators of all the subgroups Φ_μ, $\mu < \nu$. In what follows we shall speak of generators of the subgroups Φ_μ and K_ν only in this special sense.

Let U be one of the subgroups Φ_μ or K_ν. Its generators will be denoted by $u_1, u_2, \ldots$. A product[1] $u_1 u_2 \ldots u_k$ will be called a *word* in U if no

[1] Here and in what follows, the notation $u_1 u_2 \ldots u_k$ is adopted to avoid the cumbrous $u_{i_1} u_{i_2} \ldots u_{i_k}$. [*Trans.*]

two adjacent factors are inverses nor belong to one and the same subgroup $\bar{A}_\mu$. In speaking of the *length* of a word we shall always means the length of its normal form with respect to the decomposition (1) of G. In particular, a word $u_1 u_2 \dots u_k$ will be called *simple* if its length is equal to the greatest length of the factors u_i.[1] Simple words of U will be denoted by u', u'', ... Finally we shall say that between two simple words u' and u'' there exists a link of the *first, second,* or *third kind,* according as the length of the product $u'u''$ is *greater than, equal to,* or *less than* the greater of $l(u')$, $l(u'')$.

We shall now proceed to prove the following statement:

The subgroup Φ_μ is the free product of A_μ and of the infinite cyclic groups generated by the elements $f_{\mu\delta}$, $\delta < \sigma_\mu$.

This is clearly equivalent to the fact that every non-empty word of Φ_μ (in the special sense defined above) is distinct from the unit element of G, that is, has a non-empty normal form in the decomposition (1). We first prove Lemma 1.

LEMMA 1. *Any two elements $f_{\mu\delta_1}$ and $f_{\mu\delta_2}$, $\delta_1 < \delta_2$, have distinct left halves.*

This is clear for l_μ even, because the right halves of the given elements are both equal to g_μ. But if l_μ is odd and the left halves of $f_{\mu\delta_1}$ and $f_{\mu\delta_2}$ are equal, then $f_{\mu\delta_1}^{-1} f_{\mu\delta_2}$ is an element of A_μ so that $f_{\mu\delta_2}$ lies in the subgroup generated by A_μ and $f_{\mu\delta_1}$, in contradiction to the choice of the elements $f_{\mu\delta}$.

We shall now denote the generators of Φ_μ by v_1, v_2, ..., and the simple words by v', v'', ... Among the simple words of Φ_μ there occur the following:

1) Every word consisting of a single factor v_1.

2) Every word of the form $v_1 v_2$, if the right half of v_1 is g_μ and the left half of v_2 is g_μ^{-1}. For if $l(v_1 v_2) < l_\mu$, then $v_1 v_2 \in K_\mu$, that is, both v_1 and v_2 lie in a subgroup generated by other elements of K_μ, and this cannot hold for one of the two elements.

3) Every word of the form $v_1 v_2 v_3$, where $v_2 \in \bar{A}_\mu$, v_1 is an element $f_{\mu\delta_1}$, and v_3 an element $f_{\mu\delta_2}^{-1}$, and where the indices δ_1 and δ_2 may be distinct or equal.

The cases 1)-3) exhaust all simple words of Φ_μ; this is shown by the following result:

If $v_1 v_2 \dots v_n$ is a word of Φ_μ, then its factors can be bracketed.

[1] So that its length is l_μ if $U = \Phi_\mu$.

$$v_1 v_2 \dots v_n = (v_1 \dots v_{i_1})(v_{i_1+1} \dots v_{i_2}) \dots (v_{i_{k-1}+1} \dots v_n),$$

in such a way that every word $v_{i_{j-1}+1} \dots v_{i_j}$ *is a simple word* $v^{(j)}$ *of one of the forms* 1)-3),

$$v_1 v_2 \dots v_n = v' v'' \dots v^{(k)},$$

and that between any two adjacent simple words $v^{(j)}$, $v^{(j+1)}$ *there is a link of the first kind.*

This theorem is true for $n = 1$. If it is proved for $n - 1$, then

$$v_1 v_2 \dots v_{n-1} = v' v'' \dots v^{(m)}.$$

Now $v^{(m)}$ is a simple word of one of the forms 1)-3); therefore its right half is the same as the right half of v_{n-1}. If this right half is g_μ, and if the left half of v_n is g_μ^{-1}, then the product $v^{(m)} v_n$ is a simple word of the form 2) or 3). In all other cases the link between $v^{(m)}$ and v_n is of the first kind, by Lemma 1 and the definition of the elements $f_{\mu\delta}$, so that v_n can be taken as a new simple word.

It follows from this theorem that every non-empty word of Φ_μ has a non-empty normal form in the decomposition (1), and this proves our assertion about the subgroup Φ_μ.

We pass on to the consideration of the subgroup K_ν. Our aim is to prove the following theorem.

The subgroup K_ν *is the free product of all the subgroups* $\bar{A}_\mu$, $\mu < \nu$, *other than* E, *and of all the infinite cyclic groups generated by the elements* $f_{\mu\delta}$, $\delta < \sigma_\mu$, $\mu < \nu$.

This is an immediate consequence of the following theorem (in which $u_1, u_2, \dots$ denote the generators of K_ν, and $u', u'', \dots$ its simple words).

(A) *If* $u_1 u_2 \dots u_n$ *is an arbitrary word of* K_ν, *then its factors can be bracketed,*

$$u_1 u_2 \dots u_n = (u_1 \dots u_{i_1})(u_{i_1+1} \dots u_{i_2}) \dots (u_{i_{k-1}+1} \dots u_n),$$

in such a way that every word

$$u^{(j)} = u_{i_{j-1}+1} \dots u_{i_j}$$

is simple, that is,

$$u_1 u_2 \dots u_n = u' u'' \dots u^{(k)},$$

and that between any two adjacent simple words $u^{(j)}$, $u^{(j+1)}$ *there is a link of the first kind.*

For it follows easily from (A) that *the length of every word of K_ν that is not simple exceeds the length of each of its factors*, so that every non-empty word of K_ν has a non-empty normal form.

Theorem (A) will be proved by induction on ν; for $K_1 = E$ it is obvious, and for $K_2 = \Phi_1$ it has been proved above. If ν is a limit ordinal number then the theorem follows from the remark that in this case every word of K_ν is already a word of some subgroup K_μ with $\mu < \nu$. It remains to assume Theorem (A) for a subgroup K_ν with a certain ν and to prove it for $K_{\nu+1}$.

LEMMA 2. *If $u_1 u_2 \dots u_k$ is a simple word of K_ν, then every segment $u_1 u_2 \dots u_s$, $s \leqq k$, (and every segment $u_t \dots u_k$, $t \geqq 1$) is also simple.*

If any segments of the given word (at the beginning, say) are not simple, then there exists an s, $s < k$, such that $u_1 \dots u_s$ is not simple, while $u_1 \dots u_s u_{s+1}$ is simple. By (A) we have

$$u_1 \dots u_s = u' \dots u^{(r)}, \quad r > 1.$$

In this case the length of $u_1 \dots u_s$ exceeds the length of each factor, that is, of each simple word $u' \dots u^{(r)}$. If between the simple words $u^{(r)}$ and u_{s+1} there is a link of the first or second kind, then the length of $u_1 \dots u_s u_{s+1}$ also exceeds the length of each factor, and this contradicts the fact that it is simple. But if the link between $u^{(r)}$ and u_{s+1} is of the third kind, then the product $u^{(r)} u_{s+1}$ is a word whose length is less than that of one of its factors, and this contradicts Theorem (A).

LEMMA 3. *In the normal form of the simple word $u_1 \dots u_k$ of K_ν the left half of u_1 and the right half of u_k are preserved without any changes, and the middles of these elements (in the case of odd length) can only be replaced by elements, other than the unit element, of the same free factor.*

By Lemma 2 the word $u_1 \dots u_{k-1}$ is simple, so that its length is equal to the maximal length of its factors; $u_1 \dots u_k$ has the same property. Therefore the link between the simple words $u_1 \dots u_{k-1}$ and u_k must be of the second kind. It follows that the cancellations cannot affect the right half of u_k, and that its middle can only undergo an amalgamation. The argument for u_1 proceeds on similar lines.

LEMMA 4. *Every word w of K_ν having a transform as its normal form is of the form*

$$w = u_n^{-1} \dots u_1^{-1} u_0 u_1 \dots u_n,$$

where u_0 is a transform, that is, belongs to one of the subgroups A_μ, $\mu < \nu$.

Let $w = u_1 u_2 \dots u_k$. If $u_1 = u_k^{-1}$, then we can consider the word

$$u_1^{-1} w u_1 = u_2 \dots u_{k-1},$$

whose normal form is also a transform. If u_1 and u_k belong to one and the same subgroup $\bar{A}_\mu$, $\mu < \nu$, then we can consider the word

$$u_1^{-1} w u_1 = u_2 \dots u_{k-1} (u_k u_1).$$

We can therefore assume that u_1 and u_k are not inverses and do not belong to one and the same subgroup $\bar{A}_\mu$. The lemma will be proved if we can show that in this case $k = 1$.

Let $k > 1$. If w is not a simple word then, by (A), w can be written as a product of simple words between which there are links of the first kind

$$w = u' u'' \dots u^{(r)}, \quad r > 1.$$

However, since the normal form of w is a transform, that is, since its left and right halves are inverses, the product $u^{(r)} u'$ is a word in which the cancellations go so far that the link between the factors is of the third kind. The length of $u^{(r)} u'$ is therefore less than the length of one of the factors, in contradiction to Theorem (A).

Now let w be a simple word. There exists, then, a factor u_i such that $l(w) = l(u_i)$ and $l(u_i) \geqq l(u_j)$ for all $j \neq i$. We can assume that u_i is not one of the elements $f_{\mu\delta}^{-1}$, $\mu < \nu$, since otherwise we could consider the word w^{-1}. We can assume, further, that $i = k$, since for $i < k$ we could consider the word

$$u_{i+1} \dots u_k w u_k^{-1} \dots u_{i+1}^{-1} = u_{i+1} \dots u_k u_1 \dots u_i;$$

whose normal form is again a transform; by the above arguments this new word can again be taken to be simple.

If $u_k \in \Phi_\mu$, that is, if the right half of u_k is g_μ and the middle belongs to A_{a_μ}, then by Lemma 3 the right half of w is also equal to g_μ and the middle belongs to A_{a_μ}. However, since the normal form of w is a transform, its left half is equal to g_μ^{-1}. If $\bar{A}_\mu \neq E$, then $w \in \bar{A}_\mu$. Now

$$u_1 u_2 \dots u_k w^{-1} = 1;$$

if $u_k \notin \bar{A}_\mu$, then the left-hand side is a word, while for $u_k \in \bar{A}_\mu$ we obtain a word after amalgamating the factors u_k and w^{-1}. So we see that the assumption $k > 1$ leads to a contradiction to Theorem (A). If $\bar{A}_\mu = E$, then w is already contained in a subgroup K_λ with $\lambda < \mu$, that is, it can be expressed by the generators of that subgroup

$$w = u_1' u_2' \dots u_l'.$$

In this case we obtain an equation

$$u_1 \dots u_k u_l'^{-1} \dots u_1'^{-1} = 1,$$

which again is impossible, because the left-hand side is a word of K_ν.

Lemma 5. $K_\nu \cap \bar{A}_\nu = E$.

For it follows from the definition of $\bar{A}_\nu$ that there exists in $\bar{A}_\nu$ an element w, other than the unit element, that does not belong to K_ν. Suppose there is an element w', other than the unit element, that belongs to both $\bar{A}_\nu$ and K_ν. From $w' \in K_\nu$ and Lemma 4 it follows that

$$w' = u_n^{-1} \dots u_1^{-1} u_0 u_1 \dots u_n,$$

where $u_0 \in \bar{A}_\mu$, $\mu < \nu$. The normal forms of w and w' differ from one another only in that their middles are distinct elements of one and the same subgroup A_α. It follows that the element $u_1 \dots u_n w u_n^{-1} \dots u_1^{-1}$ must belong to $\bar{A}_\mu$, but then $w \in K_\nu$, because all the elements u_i, $i = 1, 2, \dots, n$, are known to lie in K_ν.

We now proceed to the proof of Theorem (A) for the subgroup $K_{\nu+1}$. Throughout the following we shall denote by $u_1, u_2, \dots$ the generators of K_ν, by $u', u'', \dots$ the simple words of K_ν, and by $v_1, v_2, \dots$ and $v', v'', \dots$ the generators and the simple words of Φ_ν. From the construction of Φ_μ and the definition of a simple word there follows the inequality $l(u') \leqq l(v')$, for any u' and v', that is, $l(u') \leqq l_\nu$.

Lemma 6. *If $l(u') < l(v')$, then a link of the third kind cannot occur between the simple words u' and v'.*

For if we had a link of the third kind between the factors of the product $u'v'$, say, and if $v' = v_1 \dots v_k$ (here $k \leqq 3$ by what has been proved above about the simple words of Φ_μ), then the length of the product $u'v_1$ would already be less than l_ν so that $u'v_1 \in K_\nu$ and $v_1 \in K_\nu$. The latter is impossible, however, by Lemma 5, if $v_1 \in \bar{A}_\nu$, or by the definition of the elements $f_{\nu\sigma}$, if v_1 is one of these elements or the inverse of one.

Lemma 7. *If $\mu < \nu$ and if the left half of an element h of H coincides with the left half of one of the elements $f_{\mu\sigma}$, while the middle of h (for odd l_μ) belongs to A_{α_μ}, then h is contained in $K_{\mu+1}$ and therefore in K_ν.*

For $l(h^{-1}f_{\mu\sigma}) \leqq l_\mu$. If this is a strict inequality, then $h^{-1}f_{\mu\sigma} \in K_\mu$, and therefore $h \in K_{\mu+1}$. But if $l(h^{-1}f_{\mu\sigma}) = l_\mu$, then the right half of $h^{-1}f_{\mu\sigma}$ is equal to g_μ, and its middle is contained in A_{α_μ}. All the elements of this kind belong to $K_{\mu+1}$, so that $h^{-1}f_{\mu\sigma} \in K_{\mu+1}$, and again $h \in K_{\mu+1}$.

LEMMA 8. *If $l(u')=l(v')$, then only a link of the first kind can occur between the simple words u' and v'.*

Let $u'=u_1u_2\dots u_k$, $v'=v_1\dots v_m$ and suppose that there is a link of the second or third kind between the factors of the product $u'v'$. Then there is also a link of the second or third kind between u' and v_1. If $l(u_j)=l(u')=l_\nu$, but when $j<k$, $l(u_i)<l_\nu$ for $j<i\leqq k$, then there is a link of the second kind between $u_{j+1}\dots u_k$ and v_1 so that $l(u_{j+1}\dots u_kv_1)=l_\nu$. For a link of the third kind is excluded by Lemma 6, since the word $u_{j+1}\dots u_k$ is simple, by Lemma 2, so that $l(u_{j+1}\dots u_k)<l_\nu$; while a link of the first kind would imply a link of the first kind between u' and v_1.

By Lemma 3, the right half of the simple word $u_1\dots u_j$ coincides with the right half of u_j, and its middle belongs to the same free factor A_α as the middle of u_j. Since there must be a link of the second or third kind between $u_1\dots u_j$ and $u_{j+1}\dots u_kv_1$, and since these words have the same length, the left half of $u_{j+1}\dots u_kv_1$ is the inverse of the right half of u_j and their middles belong to one and the same free factor. Hence we deduce that

$$u_{j+1}\dots u_kv_1\in K_\nu,$$

either from the definition of Φ_μ, if u_j belongs to A_μ or is equal to an element $f_{\mu\alpha}$, $\mu<\nu$, or from Lemma 7, if u_j is equal to some $f_{\mu\alpha}^{-1}$. But then $v_1\in K_\nu$ which is impossible.

The case of the product $v'u'$ is treated similarly.

LEMMA 9. *If $l(u')<l_\nu$ and if there is a link of the second kind between the factors of the products $v'u'$ and $u'v''$, then only a link of the first kind can occur between $v'u'$ and v''.*

If $v'=v_{11}\dots v_{1s}$, $v''=v_{21}\dots v_{2t}$ and if there is a link of the second or third kind between $v'u'$ and v'', then there will also be a link of the second or third kind between $v_{1j}u'$ and v_{21} (and also between v_{1j} and $u'v_{21}$). This is, however, impossible if the right half of v_{1j} is equal to g_ν and the left half of v_{21} is equal to g_ν^{-1}, because the cancellations would not, then, cancel out the entire word u'.

Now let the left half of v_{21} be equal to g_ν^{-1}, but the right half of v_{1j} different from g_ν; then the left half of v_{1j} is necessarily equal to g_ν^{-1}. Since by hypothesis there is a link of the second or third kind between $v_{1j}u'$ and v_{21}, the right half of $v_{1j}u'$ is equal to g_ν, that is, $v_{1j}u'\in\bar{A}_\nu$. Hence $v_{1j}\in\{K_\nu, A_\nu\}$, and this contradicts the definition of the elements

When the right half of v_{1j} is equal to g_ν but the left half of v_{21} is different from g_ν^{-1}, we use a similar argument.

Finally, let the right half of v_{1j} be different from g_ν and the left half of v_{21} be different from g_ν^{-1}. By our hypothesis on the link between $v_{1j}u'$ and v_{21} we now obtain that the product $v_{1j}u'v_{21}$ is either a transform contained in $\bar{A}_\nu$ or is the unit element. In both cases one of the elements v_{1j}, v_{21} will lie in the subgroup generated by $K_\nu, \bar{A}_\nu$, and other elements. However, since v_{1j} is different from v_{21} as well as from v_{21}^{-1}—the cancellations in the product $v_{1j}u'v_{21}$ must cancel out u' entirely—we obtain a contradiction to the definition of the elements $f_{\nu\sigma}$. This completes the proof of Lemma 9.

The proof of Theorem (A) for $K_{\nu+1}$ now goes through without any difficulty; for we can now show that *every word of $K_{\nu+1}$ is a product of simple words of one of the forms* 1) u', 2) v', 3) $u'v'$, 4) $v'u'$, and 5) $u'v'u''$ *with links of the first kind between them.*

For if w is a word of $K_{\nu+1}$, then after amalgamating adjacent elements of K_ν and of Φ_ν, we represent w as a product of words from K_ν and from Φ_ν, alternatingly. By the induction hypothesis for the case of words of K_ν and by what we have proved earlier for the case of words of Φ_ν, every one of these words can be represented as a product of simple words with links of the first kind between them. Lemmas 6, 8, and 9 show that two adjacent simple words, one in K_ν, the other in Φ_ν, give, by amalgamation, a simple word; in the case considered in Lemma 9 the word u' can be amalgamated arbitrarily with v' or with v''. We see that w can, in fact, be represented as a product of simple words of the form 1)-5) with links of the first kind between them.

Theorem (A) is therefore true for all subgroups K_ν, and so for H, which is equal to K_τ. In other words, H is the free product of all the subgroups $\bar{A}_\nu$, $\nu < \tau$—and these subgroups are, by definition, conjugate to subgroups of the free factors A_α—and of all the infinite cyclic subgroups

$$\{f_{\nu\sigma}\},\ \sigma < \sigma_\nu,\ \nu < \tau.$$

This completes the proof of the theorem on the subgroups of free products.

The free decomposition of H that we have obtained has the following properties: If g is an arbitrary element of G and A_α an arbitrary free factor of the initial decomposition of G, and if the intersection $D = H \cap g^{-1}A_\alpha g$ is different from E, then we can find in the decomposition of H a free factor that is conjugate to D in H. For if d is an element of D, other than 1, then $d = g^{-1}a_\alpha g$, $a_\alpha \in A_\alpha$. The application of Lemma 4 of the present section shows that d is conjugate in H to an element of one of the subgroups $\bar{A}_\mu$, that is,

$$d = g^{-1}a_\alpha g \in h^{-1}\bar{A}_\mu h, \text{ where } h \in H.$$

But from $\bar{A}_\mu \subseteq g_\mu^{-1}\bar{A}_{\alpha_\mu}g_\mu$ it follows that

$$d \in (g_\mu h)^{-1}A_{\alpha_\mu}(g_\mu h),$$

and so

$$a_\alpha \in (g_\mu h g^{-1})^{-1}A_{\alpha_\mu}(g_\mu h g^{-1}).$$

Hence it follows that $\alpha = \alpha_\mu$ and $g_\mu h g^{-1} = a'_{\alpha_\mu} \in A_{\alpha_\mu}$, that is, $g = a'^{-1}_{\alpha_\mu} g_\mu h$. Now

$$D = H \cap g^{-1}A_\alpha g = H \cap (a'^{-1}_{\alpha_\mu} g_\mu h)^{-1}A_{\alpha_\mu}(a'^{-1}_{\alpha_\mu} g_\mu h) =$$

$$= h^{-1}(H \cap g_\mu^{-1}A_{\alpha_\mu}g_\mu)\,h = h^{-1}\bar{A}_\mu h,$$

and this proves our statement.

§ 35. Isomorphism of free decompositions. Free products with an amalgamated subgroup

Two free decompositions of a group G,

$$G = F_1 * \prod_\alpha{}^* A_\alpha = F_2 * \prod_\beta{}^* B_\beta,$$

are called *isomorphic* if F_1 and F_2 are isomorphic free groups and if a one-to-one correspondence between the factors A_α and B_β can be established such that corresponding factors are conjugate in G. Using the concept of a refinement of a free decomposition of a group, introduced in § 33, we can now prove the following theorem (see Kuroš [2], [3], Baer and Levi [2]):

Any two free decompositions of an arbitrary group possess isomorphic refinements.

For let

$$G = \prod_\alpha{}^* A_\alpha = \prod_\beta{}^* B_\beta. \tag{1}$$

If

$$A_\alpha = F_\alpha * \prod_\gamma{}^* A_{\alpha\gamma} \tag{2}$$

is a free decomposition of A_α as obtained from the second decomposition (1) by the construction of the preceding section, and if

$$B_\beta = F'_\beta * \prod_\delta{}^* B_{\beta\delta} \tag{3}$$

is such a decomposition of B_β with respect to the first decomposition (1), then the subgroup

$$B_{\beta\delta} = B_\beta \cap g^{-1}A_\alpha g$$

is conjugate to $gB_\beta g^{-1} \cap A_\alpha$. But by the remark at the end of the preceding section this intersection is also conjugate to one of the subgroups $A_{\alpha\gamma}$. Therefore we can find for every $B_{\beta\delta}$ a subgroup $A_{\alpha\gamma}$ that is conjugate to it in G.

We now set up refinements of the decompositions (1), replacing all A_α and B_β by their decompositions (2) and (3):

$$G = \prod_\alpha{}^* F_\alpha {}^* \prod_{\alpha,\gamma}{}^* A_{\alpha\gamma} = \prod_\beta{}^* F'_\beta {}^* \prod_{\beta,\delta}{}^* B_{\beta\delta}. \tag{4}$$

Note that two distinct subgroups $A_{\alpha\gamma}$ and $A_{\alpha'\gamma'}$ cannot be conjugate in G, since they occur as free factors in a free decomposition of G. Every $B_{\beta\delta}$ is therefore conjugate to one and only one subgroup $A_{\alpha\gamma}$; conversely every $A_{\alpha\gamma}$ is conjugate to one of the $B_{\beta\delta}$. We can therefore set up a one-to-one correspondence between the subgroups $A_{\alpha\gamma}$ and the subgroups $B_{\beta\delta}$ such that corresponding subgroups are conjugate in G. Now the subgroups $\prod_{\alpha,\gamma}{}^* A_{\alpha\gamma}$ and $\prod_{\beta,\delta}{}^* B_{\beta\delta}$ generate the same normal subgroup of G and therefore, by property IV of § 33, the free groups $\prod_\alpha{}^* F_\alpha$ and $\prod_\beta{}^* F'_\beta$ are isomorphic. This proves the isomorphism of the free decompositions (4).

In this chapter we shall call a group *indecomposable* if it cannot be represented as the free product of proper subgroups. From the theorem just proved we immediately obtain the following result.

If a group G has free decompositions with indecomposable factors, then any two such decompositions of G are isomorphic, and every free decomposition of G can be refined to a decomposition with indecomposable factors.

Note that, whereas the theorem on the existence of isomorphic refinements has been proved for arbitrary groups, this last result refers to a special class of groups only: *there exist groups that are decomposable into free products but not into free products of indecomposable groups* (see Kuroš [8]).

The definition of the isomorphism of two free decompositions contains, in particular, a statement on the isomorphism of two free groups. There arises the problem of conditions under which two free groups are isomorphic. Since a free group is completely determined by its rank, that is, by the cardinal number of its free generators, the problem obviously reduces to

whether two free groups with different ranks can be isomorphic. This question is answered by the following theorem (Schreier [4]):

The rank of a free group is an invariant of the group, that is, it does not depend on the choice of a system of free generators.

This theorem shows that an isomorphism of two free groups implies the equality of their ranks: in an isomorphic mapping of one of the groups onto the other, the images of a given system of free generators of the first group form a system of free generators of the second group.

For the proof of the theorem we take the factor group of the commutator group K in the free group W. Since the transition to the factor group of the commutator group is equivalent to the assumption that all the generators are permutable, the factor group W/K is a free abelian group and the cosets of K that contain the elements of the given system of free generators of W are a basis of this free abelian group. The invariance of the rank of W now follows from the invariance of the rank of an abelian group, which was proved in § 19.

When the theorem on the subgroups of a free product is applied to the case of a free group, that is, a free product of infinite cyclic groups, it leads to the following theorem.

NIELSEN-SCHREIER THEOREM. *Every subgroup of a free group is itself a free group.*

For every subgroup that is conjugate in some group to a subgroup of an infinite cyclic group is itself an infinite cyclic group.

We shall come back to this theorem in the following section. Here we shall prove, as another application of the theorem on subgroups of a free product, the following theorem (Baer and Levi [2]):

No group can be decomposable both into a free product and into a direct product.

Suppose that

$$G = A * B = C \times D,$$

where A, B, C, D are subgroups other than the unit subgroup. Since no element of a free factor of a group, except the unit element, can be permutable with an element not in that free factor, we should obtain from $A \cap C \neq E$ and from the permutability of the elements of C and D that $A \supset D$ and also that $A \supset C$, so that $A = G$, which is impossible. Therefore $A \cap C = A \cap D = E$. Similarly, $B \cap C = B \cap D = E$. Since C is a normal subgroup of G, the intersection of C with any subgroup conjugate to A or

to B is also E. Now we apply the theorem on the subgroups of a free product to C and obtain that C is a free group. The same holds for D. From $A \cap D = E$ it follows, further, that the component (see § 17) of A in the factor C of the direct decomposition $G = C \times D$ is isomorphic to A itself. By the Nielsen-Schreier Theorem this component, as a subgroup of a free group, is itself a free group. Thus we see that A, and B as well, are free groups and that their free product G is also a free group. However, this leads to a contradiction, since a free group cannot be decomposable into a direct product: if such a decomposition existed, then we could find a subgroup of a free group that is the direct product of two infinite cyclic groups, and this contradicts the Nielsen-Schreier Theorem.

Problems concerning the groups of automorphisms of free groups and free products occupy an important place in the theory. Generators and defining relations of the group of automorphisms of a free group of arbitrary finite rank were set up by Nielsen [1, 2, 4] (see also B. H. Neumann [1]). The problem of conditions under which one of two given systems of elements of a free group goes over into the other under some automorphism of the group is treated in a paper by J. H. C. Whitehead [2]. Groups of automorphisms of free products of a finite number of arbitrary indecomposable groups were considered in a special case by Golovin and Sadovskiĭ [1] and in the general case by Fuchs-Rabinovič [6, 7]. All these results, however, are very awkward to formulate, and we shall not pursue the matter any further.

Free products with an amalgamated subgroup. In some connections an even more general construction than that of the free product turns out to be useful. Let A_α be groups, where α ranges over a set of indices, and let a proper subgroup B_α be chosen in every A_α such that all these subgroups are isomorphic to a fixed group B. By φ_α we denote a specific isomorphic mapping of B_α onto B; then $\psi_{\alpha\beta} = \varphi_\alpha \varphi_\beta^{-1}$ is an isomorphic mapping of B_α onto B_β.

The free product of the groups A_α with the amalgamated subgroup B is defined as the factor group G of the free product of the groups A_α with respect to the normal subgroup generated by all elements of the form $b_\alpha b_\beta^{-1}$, where $b_\beta = b_\alpha \psi_{\alpha\beta}$, where b_α ranges over the whole subgroup B_α, and where α and β are all possible index pairs. In other words, if every group A_α is given by a system of generators $\mathfrak{M}_\alpha$ and a system of defining relations Φ_α between these generators, then G has as a system of generators the union of all sets $\mathfrak{M}_\alpha$, as a system of defining relations the union of the sets Φ_α, and, in addition, all relations obtained by identifying those elements of different

subgroups B_α and B_β which are mapped by the isomorphisms φ_α and φ_β onto one and the same element of B. The subgroups B_α are "amalgamated," as it were, in accordance with the isomorphisms $\psi_{\alpha\beta}$.

This definition does not enable us immediately to clarify the structure of G: it could conceivably happen that the introduction of additional defining relations gives rise to amalgamations among the groups A_α that are not provided for by the isomorphisms $\psi_{\alpha\beta}$, or that it replaces some groups A_α by factor groups, and so on. We must, therefore, look into the matter more closely.

In every group A_α we select a representative from each right coset of B_α, assuming only that the representative of B_α itself is the unit element. We denote by $\bar{a}_\alpha$ the representative of the coset in which a_α lies, so that

$$a_\alpha = b_\alpha \bar{a}_\alpha, \qquad b_\alpha \in B_\alpha. \tag{5}$$

A *word* shall be an expression

$$b\bar{a}_1\bar{a}_2 \dots \bar{a}_n, \tag{6}$$

where $n \geqq 0$, where b is any element of B, possibly the unit element, where every $\bar{a}_i$ is a representative, other than the unit element, of a right coset of B_α in A_α, for some α, and where, finally, adjacent representatives $\bar{a}_i$, $\bar{a}_{i+1}$ $i = 1, 2, \dots, n-1$, lie in distinct groups A_α.

If G is the free product of the groups A_α with the amalgamated subgroup B, then every element of G can be expressed in the form (6) *in one and only one way.*

That such an expression exists is very easy to see. Let $a_1 a_2 \dots a_n$ be an element of the free product of the groups A_α in the normal form, $a_i \in A_{\alpha_i}$. If $n = 1$, then the required expression is given by (5). Let us assume, then, that we have already proved that

$$a_2 a_3 \dots a_n = b\bar{a}_2'\bar{a}_3' \dots \bar{a}_m',$$

where the right-hand side is a word in the present sense, and let

$$b\varphi_{\alpha_1}^{-1} = b_1, \quad a_1 b_1 = a_1', \quad a_1' = b_1'\bar{a}_1', \quad b_1'\varphi_{\alpha_1} = b'.$$

If $\bar{a}_1' = 1$, then

$$a_1 a_2 \dots a_n = b'\bar{a}_2' \dots \bar{a}_m',$$

where the right-hand side is a word. But if $\bar{a}_1' \neq 1$ and if $\bar{a}_1'$ and $\bar{a}_2'$ lie in different groups A_α, then the required expression is

$$a_1 a_2 \dots a_n = b' a_1' a_2' \dots a_m',$$

Finally, if $\bar{a}_1'$ and $\bar{a}_2'$ lie in one and the same A_α, then let

$$\bar{a}_1' \bar{a}_2' = b_\alpha \bar{a}_1'', \quad b_\alpha \varphi_\alpha = b'';$$

now if $\bar{a}_1'' \neq 1$, then

$$a_1 a_2 \dots a_n = (b' b'') \bar{a}_1'' \bar{a}_3' \dots \bar{a}_m',$$

and if $\bar{a}_1'' = 1$, then

$$a_1 a_2 \dots a_n = (b' b'') \bar{a}_3' \dots \bar{a}_m'.$$

We remark that if this process is actually applied to the product $a_1 a_2 \dots a_n$, beginning from the right-hand end, then it leads to a well-defined word of the form (6). We shall call this process the *reduction* of the product $a_1 a_2 \dots a_n$. In order to prove the uniqueness of the representation (6) we can make use of the method that we have already applied in § 33. We denote by M the set of all words of the form (6), and by S_M the unrestricted symmetric group on M. If a is an element of A_α, then we associate with a the following mapping $\hat{a}$ of M into itself. Let (6) be an arbitrary word. Considering it as an element of the free product of the groups A_α, we multiply it by a on the right, go over to the normal form, and then apply the reduction process. We shall consider the new word so obtained as corresponding to the word (6) under the mapping $\hat{a}$.

If a is the unit element of A_α, then the mapping associated with it is the identity mapping of M onto itself. A simple verification (though involving several distinctions of case) will show that the mapping associated with the product of two elements a and a' of A_α coincides with the result of carrying out the mappings $\hat{a}$ and $\hat{a}'$ in succession. In particular, the element a^{-1} is associated with the inverse mapping of $\hat{a}$, and $\hat{a}$ is therefore a one-to-one mapping onto the whole of M.

Note that for $a \neq 1$, $a = b\bar{a}$, the word 1 is carried into the word $b\bar{a}$, which is different from 1, so that the mapping $\hat{a}$ is not the identity. We therefore obtain an isomorphic mapping of A_α onto a subgroup $\hat{A}_\alpha$ of S_M. Let $\hat{G}$ be the subgroup S_M generated by all $\hat{A}_\alpha$. All the defining relations for G are obviously satisfied in $\hat{G}$, and the expression of the elements of G in the form (6) is unique. For if $b_\alpha \psi_{\alpha\beta} = b_\beta$, then the mappings $\hat{b}_\alpha$ and $\hat{b}_\beta$ clearly coincide, and this gives a unique meaning to the symbol $\hat{b}$. The mapping

$$\hat{b}\hat{\bar{a}}_1 \hat{\bar{a}}_2 \dots \hat{\bar{a}}_n \tag{7}$$

now carries the word 1 into (6), so that distinct products (7) are distinct elements of $\hat{G}$. Hence follows the uniqueness of the expression of the elements of G as words.

We can now easily establish a number of properties of the free product G of groups A_α with an amalgamated subgroup B.

The groups A_α are contained in G as subgroups, and they generate G and intersect pairwise in the amalgamated subgroup B.

For the word on the right-hand side of (5) is different from the word 1 if $a_\alpha \neq 1$. If $a_\alpha \notin B_\alpha$ and a_β is an arbitrary element of A_β, $\beta \neq \alpha$, then the reduction of the product $a_\beta^{-1} a_\alpha$ leads to a word ending with $\bar{a}_\alpha$, so that it is different from 1.

Every element of G having finite order is conjugate in G to an element of one of the subgroups A_α.

Let g be an element of G, of finite order k,

$$g^k = 1,$$

written in the form (6). If $n \leqq 1$, there is nothing to prove. If $n > 1$, and if the elements $\bar{a}_1$ and $\bar{a}_n$, in this expression belong to the same subgroup A_α, then after transforming by $\bar{a}_n^{-1}$ and subsequent reduction, we go over to a word of shorter length. We can therefore, assume that $n > 1$ and that $\bar{a}_1$ and $\bar{a}_n$ lie in distinct subgroups A_α and then show that this case cannot occur. We write the word (6) k times in succession and each time combine the factors b and $\bar{a}_1$. Owing to our hypothesis we obtain the normal form of the product of certain elements of the groups A_α; moreover, these elements lie outside the corresponding subgroups B_α. In carrying out the reduction, we can therefore never arrive at a representative equal to the unit element: if an element of A_α outside B_α is multiplied on the left by an element of B_α, we obtain an element outside B_α, and so the reduction cannot lead to the word 1.

If C_α is the intersection of B_α with the center of A_α, then the center of G is the intersection of all the subgroups $C_\alpha \varphi_\alpha$ of B.

It is clear that the intersection of all the subgroups $C_\alpha \varphi_\alpha$ lies in the center of G. On the other hand, let

$$g = b\bar{a}_1\bar{a}_2 \ldots \bar{a}_n$$

be an element of the center of G. If $n \geqq 1$ and $\bar{a}_n \in A_\alpha$, then in an arbitrary group A_β, $\beta \neq \alpha$, we take an arbitrary element a' ouside B_β. The reductions of the products ga' and $a'g$ are known to lead to distinct words. But

if $n = 0$, that is, $g = b$, then b lies in one of the subgroups C_α and we are again led to a contradiction if we take as a' an element of A_α that is not permutable with $b\varphi_\alpha^{-1}$.

The problem of subgroups of a free product with an amalgamated subgroup would require the study of an even more general construction: instead of the amalgamation of one and the same subgroup B in all the groups A_α it is assumed that in every pair of groups A_α, A_β a subgroup $B_{\alpha\beta}$ is amalgamated, where the choice of these subgroups $B_{\alpha\beta}$ in the group A_α is properly coordinated. This construction is studied in papers by Hanna Neumann [1-3]. It is interesting also because a special case is the union of an ascending sequence of groups introduced in § 7.

§ 36. Subgroups of Free Groups

The Nielsen-Schreier theorem, which we deduced in the preceding section from the theorem on the subgroups of a free product, was proved by Nielsen [3] for the case of free groups of finite rank and later by Schreier [4] for arbitrary free groups. Schreier's method was substantially simplified by Hurewicz [1]. Another proof of the theorem was given by Levi [2]. There also exist some topological proofs (Reidemeister [3], Locher [1]). Recently a new proof has been published by Federer and Jónsson [1].

In view of the great importance of this theorem we shall give a second proof, namely the one by Hurewicz, which does not depend on the general theory of free products.

Let G be a free group with a system of free generators a_α, where α ranges over an index set, and let U be a subgroup of G. In every right coset Ug we choose a representative $\bar{g}$ such that the unit element is the representative of the coset U, that is, $\bar{1} = 1$. The choice of representatives shall be subject to the following condition: If an element that is written as the word $a_{\alpha_1}^{\varepsilon_1} a_{\alpha_2}^{\varepsilon_2} \dots a_{\alpha_n}^{\varepsilon_n}$, $\varepsilon_i = \pm 1$, is the representative of its coset, then *every segment*

$a_{\alpha_1}^{\varepsilon_1} a_{\alpha_2}^{\varepsilon_2} \dots a_{\alpha_k}^{\varepsilon_k}$, $k \leqq n$, *must also be the representative of its coset.*

We now show that such a choice of representatives is possible. Let l be the minimal length of words in the coset Ug and let the required choice of representatives already be made for cosets with smaller minimal length; for $l = 0$—that is, for U—this is feasible. We now take one of the elements of minimal length in Ug, say

$$g = a_{\beta_1}^{\eta_1} a_{\beta_2}^{\eta_2} \dots a_{\beta_l}^{\eta_l}, \quad \eta_i = \pm 1.$$

The element $g' = a_{\beta_1}^{\eta_1} a_{\beta_2}^{\eta_2} \dots a_{\beta_{l-1}}^{\eta_{l-1}}$ defines a coset Ug' in which a representative with the required properties has already been chosen. If this representative is $\bar{g}' = a_{\alpha_1}^{\varepsilon_1} a_{\alpha_2}^{\varepsilon_2} \dots a_{\alpha_k}^{\varepsilon_k}$, then $g' = u\bar{g}'$, $u \in U$, so that

$$g = u\bar{g}' a_{\beta_l}^{\eta_l}.$$

The element $\bar{g}' a_{\beta_l}^{\eta_l}$, which lies in Ug can now be taken as $\bar{g}$. Its representation

$$\bar{g} = a_{\alpha_1}^{\varepsilon_1} a_{\alpha_2}^{\varepsilon_2} \dots a_{\alpha_k}^{\varepsilon_k} a_{\beta_l}^{\eta_l}$$

is a reduced word, since l is the minimal length of elements in Ug (hence $k = l - 1$) and every segment of g is the representative of its coset.

Let $\bar{g}$ be an arbitrary representative from among those we have chosen and a_α an arbitrary generator. We consider the product $\bar{g}a_\alpha \overline{\bar{g}a_\alpha}^{-1}$. Clearly this does not depend on the choice of an element g in the coset that has $\bar{g}$ as its representative, and if we put $\bar{g} = u_1 g$, $\overline{\bar{g}a_\alpha} = u_2 \overline{ga_\alpha}$, where $u_1, u_2 \in U$, then

$$\bar{g}a_\alpha \overline{\bar{g}a_\alpha}^{-1} = u_1 u_2^{-1} \in U.$$

We shall write

$$u_{\bar{g},\alpha} = \bar{g}a_\alpha \overline{\bar{g}a_\alpha}^{-1}, \text{ if } \bar{g}a_\alpha \overline{\bar{g}a_\alpha}^{-1} \neq 1,$$

and we shall show that *the set of all $u_{\bar{g},\alpha}$ is a system of generators for the subgroup U.* If $u = a_{\alpha_1}^{\varepsilon_1} a_{\alpha_2}^{\varepsilon_2} \dots a_{\alpha_n}^{\varepsilon_n} \in U$, we put $g_k = a_{\alpha_1}^{\varepsilon_1} a_{\alpha_2}^{\varepsilon_2} \dots a_{\alpha_k}^{\varepsilon_k}$, $k \leqq n$. Obviously, $g_0 = 1$, $g_n = u$. Now

$$u = \prod_{k=1}^{n} \bar{g}_{k-1} a_{\alpha_k}^{\varepsilon_k} \bar{g}_k^{-1},$$

because $\bar{g}_0 = \bar{g}_n = 1$. However, if $\varepsilon_k = +1$, then

$$\bar{g}_{k-1} a_{\alpha_k}^{\varepsilon_k} \bar{g}_k^{-1} = \bar{g}_{k-1} a_{\alpha_k} \overline{\bar{g}_{k-1} a_{\alpha_k}}^{-1},$$

which is equal to $u_{\bar{g}_{k-1}, \alpha_k}$ or to the unit element; but if $\varepsilon_k = -1$, then from $g_k = g_{k-1} a_{\alpha_k}^{-1}$ it follows that $g_{k-1} = g_k a_{\alpha_k}$, and therefore

$$\bar{g}_{k-1} a_{\alpha_k}^{\varepsilon_k} \bar{g}_k^{-1} = \overline{\bar{g}_k a_{\alpha_k}} a_{\alpha_k}^{-1} \bar{g}_k^{-1},$$

which is equal to $u_{\bar{g}_k,\,\alpha_k}^{-1}$ or to the unit element. If the element u is expressed in another form in terms of the generators a_α—this new form can be obtained from the previous one by a finite number of elementary transformations consisting of omissions or insertions of two adjacent inverse symbols a_α and a_α^{-1}—and if the above method of representing u by the generators $u_{\bar{g},\,\alpha}$ is applied to the new form, then the reader can immediately verify that the new representation is obtained from the previous one by similar omissions or insertions of adjacent inverse symbols $u_{\bar{g},\,\alpha}$ and $(u_{\bar{g},\,\alpha})^{-1}$. In other words, if U^* is the free group with the free generators $u_{\bar{g},\,\alpha}$,[1] then the method of expressing the element u by the elements $u_{\bar{g},\,\alpha}$ which has been described in the preceding paragraph establishes a correspondence between each element u of U and a well-defined element u^* of U^*. If the symbol $\equiv$ is used to express equality of elements of U^*, then we have[2] for any two elements u_1 and u_2 of U

$$(u_1u_2)^* \equiv u_1^* u_2^*,$$

so that the correspondence $u \to u^*$ is a homomorphic mapping of U into U^*. We shall show that *it is an isomorphic mapping onto the whole of* U^*.

Let us find the element $u_{\bar{g},\,\alpha}^*$. If

$$\bar{g} = a_{\alpha_1}^{\varepsilon_1} \dots a_{\alpha_n}^{\varepsilon_n},$$

$$\overline{g a_\alpha} = a_{\beta_1}^{\eta_1} \dots a_{\beta_m}^{\eta_m},$$

then

$$u_{\bar{g},\,\alpha} = a_{\alpha_1}^{\varepsilon_1} \dots a_{\alpha_n}^{\varepsilon_n} a_\alpha a_{\beta_m}^{-\eta_m} \dots a_{\beta_1}^{-\eta_1} =$$

$$= \prod_{i=1}^{n} \left(\overline{a_{\alpha_1}^{\varepsilon_1} \dots a_{\alpha_{i-1}}^{\varepsilon_{i-1}} a_{\alpha_i}^{\varepsilon_i}} \, \overline{a_{\alpha_1}^{\varepsilon_1} \dots a_{\alpha_i}^{\varepsilon_i}}^{-1} \right) \cdot \left(\bar{g} a_\alpha \overline{\overline{g a_\alpha}}^{-1} \right) \cdot$$

$$\cdot \prod_{j=0}^{m-1} \left(\overline{\bar{g} a_\alpha a_{\beta_m}^{-\eta_m} \dots a_{\beta_{m-j+1}}^{-\eta_{m-j+1}}} \, a_{\beta_{m-j}}^{-\eta_{m-j}} \, \overline{\bar{g} a_\alpha a_{\beta_m}^{-\eta_m} \dots a_{\beta_{m-j}}^{-\eta_{m-j}}}^{-1} \right).$$

If we now make use (for the first time in the whole proof!) of the fact that every segment of a representative is itself the representative of its coset, and if we note that for $0 \leqq j \leqq m-1$

[1] More accurately, if U^* is a free group whose free generators are in one-to-one correspondence with the symbols $u_{\bar{g},\,\alpha}$, regarded as formally distinct.

[2] For the proof it is sufficient to apply the method of constructing u^* to the product u_1u_2 without carrying out any cancellations in the product.

$$\overline{\overline{g}a_\alpha a_{\beta_m}^{-\eta_m} \dots a_{\beta_{m-j}}^{-\eta_{m-j}}} = \overline{u_{\overline{g},\alpha} a_{\beta_1}^{\eta_1} \dots a_{\beta_{m-j-1}}^{\eta_{m-j-1}}} = a_{\beta_1}^{\eta_1} \dots a_{\beta_{m-j-1}}^{\eta_{m-j-1}},$$

then we find without difficulty that in our product all the factors disappear except one, namely $u_{\overline{g},\alpha}$. Thus, we have proved that

$$u^*_{\overline{g},\alpha} \equiv u_{\overline{g},\alpha}.$$

Every generator, and therefore every element, of U^* is the image of an element of U. Moreover, we see that *U is a free group and the set of elements $u_{\overline{g},\alpha}$ is a system of free generators.* This concludes the proof of the Nielsen-Schreier Theorem.

The method just explained of constructing systems of free generators for the subgroups of a free group can be used to establish some new properties of free groups.

I. *The commutator group of a free group of finite rank n, $n > 1$, is a free group of countable rank.*

For let G be a free group with $a_1, a_2, \dots, a_n$ as a system of free generators, and let K be the commutator subgroup of G. Every coset of K contains one and only one element of the form $a_1^{\alpha_1} a_2^{\alpha_2} \dots a_n^{\alpha_n}$ with integer exponents α_i, and the set of these elements form a set of representatives satisfying the requirements set forth in the preceding proof. However, it is easily seen that the element $\overline{g}a_i\overline{g}a_i^{-1}$, where

$$\overline{g} = a_1^{\alpha_1} a_2^{\alpha_2} \dots a_n^{\alpha_n}, \quad \alpha_n = \alpha_{n-1} = \dots = \alpha_{k+1} = 0, \quad \alpha_k \neq 0, \quad k \leqq n,$$

is equal to the unit element if and only if $k \leqq i$. Hence it follows that K has infinite rank.

II. (Schreier [4]). *If U is a subgroup of finite index j in a free group G of finite rank n, then the rank k of U is also finite and*

$$k = 1 + j(n-1).$$

Let $a_1, a_2, \dots, a_n$ be a system of free generators of G, and let the representatives $\overline{g}$ of the right cosets of U be chosen such that every segment of a representative is also the representative of its coset. The total number of products of the form $\overline{g}a_i\overline{g}a_i^{-1}$ is obviously jn; hence it follows that k is finite. We shall now calculate how many of these products are equal to the unit element.

Let P_l be the number of representatives $\overline{g}$ of length l having one of the

elements a_i as their last factor, P_l' the number of representatives of the same length ending with one of the elements a_i^{-1}; we also put $P_0 = 1$, $P_0' = 0$. Now if $\bar{g}a_i\bar{g}\bar{a}_i^{-1} = 1$, that is, $\bar{g}a_i = \bar{g}\bar{a}_i$, and if $\bar{g}$ has length l, then the length of $\bar{g}a_i$ is $l-1$ or $l+1$. In the first case $\bar{g}$ ends with a_i^{-1}. For given l and arbitrary i there are P_l' such cases, because conversely if $\bar{g}$ ends with a_i^{-1}, then $\bar{g}\bar{a}_i$ is a segment of $\bar{g}$ and therefore $\bar{g}a_i\bar{g}\bar{a}_i^{-1} = 1$. In the second case $\bar{g}\bar{a}_i$ is a representative of length $l+1$ with positive last exponent. Conversely, if some representative of length $l+1$ ends with a_i, then it is of the form $\bar{g}a_i$, where $\bar{g}$ is its segment of length l, and then $\bar{g}a_i\bar{g}\bar{a}_i^{-1} = 1$. There are therefore P_{l+1} such cases. The total number of products equal to the unit element, then, is

$$\sum_{l \geqq 0} (P_l' + P_{l+1}),$$

and this sum is equal to $j-1$, because we get j by adding $P_0 = 1$ to the sum. Now

$$k = jn - (j-1) = 1 + j(n-1).$$

This completes the proof.

III. (M. Hall [4]). *Let G be a free group and let*

$$G = A_0 \supset A_1 \supset A_2 \supset \ldots \supset A_k \supset \ldots$$

be a decreasing sequence of subgroups with the following property: For every k, $k \geqq 0$, and every choice of a system of free generators for A_k every element of A_{k+1}, other than 1, has length at least three in these generators. Then the intersection of the sequence of subgroups is E.[d]

Let a system of free generators in G be given. Applying the method described in the above proof of the Nielsen-Schreier theorem, we choose a system of free generators in A_1. Starting from this system of free generators of A_1 we choose free generators for A_2 by the same method, and so on.

Let x be an arbitrary element of A_k, $k \geqq 1$. If its length in the chosen generators of A_{k-1} is n, then its length in the chosen generators of A_k is *not greater than n* (compare with that point in the proof of the Nielsen-Schreier theorem where the element u of the subgroup U is expressed in terms of the $u_{\bar{g},\alpha}$). In our case the length is, however, *strictly less than n*: if

$$x = a_{\alpha_1}^{\varepsilon_1} a_{\alpha_2}^{\varepsilon_2} \ldots a_{\alpha_n}^{\varepsilon_n}$$

is the reduced form of x in the chosen generators of A_{k-1}, and if we have $\overline{a_{\alpha_1}^{\varepsilon_1}} \neq a_{\alpha_1}^{\varepsilon_1}$, then

$$a_{\alpha_1}^{\varepsilon_1} = y\overline{a_{\alpha_1}^{\varepsilon_1}}, \quad y \in A_k,$$

and this implies that the element

$$y = a_{\alpha_1}^{\varepsilon_1} \overline{a_{\alpha_1}^{\varepsilon_1}}^{-1}$$

of A_k is different from 1. Its length in the chosen generators of A_{k-1} is, however, *two*, because the representative $\overline{a_{\alpha_1}^{\varepsilon_1}}$ of the coset $A_k a_{\alpha_1}^{\varepsilon_1}$ has minimal length, that is, length 1. This is in contradiction with the conditions of the theorem. So we see that on transition from A_{k-1} to A_k the length of an element of A_k strictly decreases, and hence no element, other than 1, can lie in all the subgroups A_k.

The following result is a consequence of this last theorem: If ω is the first infinite ordinal number, then *the ω-th derived group of a free group* (see § 14) *is* E. For if x_α are free generators of a free group G and if y is an element of the derived group of G, $y \neq 1$, then in the reduced form of y in terms of the generators x_α the sum of the exponents for every x_α is zero. Hence it follows that the length of y in the generators x_α is not less than four.

The corollary just proved could also be deduced from the following theorem.

MAGNUS' THEOREM. *If G is an arbitrary free group, then the ω-th term of its lower central chain is E.*

This theorem was first proved by Magnus [6] and later by Witt [1], Fuchs-Rabinovič [5], M. Hall [4]. It is also contained in much more general results of Mal'cev [7], which state conditions under which the ω-th term of the lower central series of a free product is E. We shall prove Magnus' theorem by Mal'cev's method.

Let R be an arbitrary associative ring. If we put for $a, b \in R$

$$a \circ b = a + b - ab,$$

we obtain a new operation in R which we shall call the *adjoint multiplication.*[e] This operation is *associative*:

$$a \circ (b \circ c) = a \circ (b + c - bc) = a + (b + c - bc) - a(b + c - bc) =$$
$$= (a + b - ab) + c - (a + b - ab)c = (a \circ b) \circ c.$$

The null element of the ring R obviously plays the rôle of the *unit element* in the adjoint multiplication

$$a \circ 0 = 0 \circ a = a.$$

An element a of R is called a *radical* element if it has an adjoint inverse, that is, an element a' such that

$$a \circ a' = a' \circ a = 0.$$

Clearly

$$(a')' = a.$$

The adjoint product of two radical elements is radical, because

$$(a \circ b)' = b' \circ a'.$$

So we see that the radical elements of a ring R form a group under the adjoint multiplication, which we call the *adjoint group* of the ring R.

Now let $\mathfrak{m}$ be a cardinal number, finite or infinite. We choose a set of symbols e_α, where the index α ranges over a set of cardinal number $\mathfrak{m}$, and we call every expression

$$e_{\alpha_1} e_{\alpha_2} \ldots e_{\alpha_n},$$

a *word* of length n, $n \geqq 1$ if $\alpha_i \neq \alpha_{i+1}$, $i = 1, 2, \ldots, n-1$, so that adjacent "factors" are distinct. We now construct a ring R in the following way. The elements of R shall be formal sums of a finite number of words with non-zero integer coefficients; the representation of the elements of R in the form of such a sum shall be unique up to the order of the summands. Among the elements of R we shall also count the *empty* sum of words which contains no word with non-zero coefficients.

We define the *addition* of two sums of words as the addition of the coefficients of identical words and subsequent omission of those words whose coefficients turn out to be zero. It is clear that this addition is commutative and associative and has a subtraction; in particular, the empty sum of words is the null element.

Let us define the *product of words*. If

$$v_1 = e_{\alpha_1} e_{\alpha_2} \ldots e_{\alpha_n}, \qquad v_2 = e_{\beta_1} e_{\beta_2} \ldots e_{\beta_m},$$

are two words, and if $\alpha_n \neq \beta_1$, then the expression

$$e_{\alpha_1} e_{\alpha_2} \ldots e_{\alpha_n} e_{\beta_1} e_{\beta_2} \ldots e_{\beta_m}$$

is a word which will be regarded as the product $v_1 v_2$; but if $\alpha_n = \beta_1$, then we put $v_1 v_2 = 0$; in particular the square of every word e_α is zero. Note

that if $v_1 v_2 \neq 0$, then the length of $v_1 v_2$ is the sum of the lengths of v_1 and v_2.

Multiplication of two sums of words will now be defined in the following way: Every term of the first sum is multiplied into every term of the second sum (the coefficients are multiplied, and the product of words is taken in the above sense); then similar terms are combined, and the terms whose coefficients turn out to be zero are omitted. This multiplication is obviously not commutative; it is, however, associative, because the multiplication of words is associative, and distributive with respect to addition.

We have therefore constructed a ring R. We denote by G the adjoint group of this ring. Every element e_α is contained in G, for

$$e_\alpha' = -e_\alpha. \tag{1}$$

We show that *the subgroup F generated in G by all the elements e_α is free, and the set of e_α's is a system of free generators of F.*

For

$$e_\alpha \circ e_\alpha = 2e_\alpha,$$

and for every positive integer k and also every negative integer k by (1) the adjoint k-th power of e_α is ke_α. The element e_α therefore generates an infinite cyclic subgroup of G. If we expand the adjoint product

$$k_1 e_{\alpha_1} \circ k_2 e_{\alpha_2} \circ \ldots \circ k_n e_{\alpha_n}, \tag{2}$$

where $\alpha_i \neq \alpha_{i+1}$, $i = 1, 2, \ldots, n-1$ and all the k_i are different from the zero, then we obtain, among others, the term

$$(k_1 k_2 \ldots k_n) e_{\alpha_1} e_{\alpha_2} \ldots e_{\alpha_n}.$$

This is the only term of length n with a non-zero coefficient; it cannot be reduced, and (2) therefore, cannot be equal to zero, that is, to the unit element of G.

Given any non-zero element of R, we shall call the terms of minimal length the *lowest terms* of the element and their length the *height* of the element. To the null element we shall assign infinite height, so that its height exceeds that of any other element of R. It is easy to verify that *the height of a product is greater than or equal to the sum of the heights of the factors.* On the other hand, *the height of a sum is greater than or equal to the smallest height of a summand.* Therefore *the height of a non-zero adjoint*

product of elements of R is greater than or equal to the smallest height of a factor.

Now if a is an element of G, then *a and a' have the same height.* For

$$a + a' - aa' = 0,$$

but the height of the product aa' is strictly greater than the height of either factor, so that the lowest terms of the summands a and a' must annihilate each other.

If a and b are non-zero elements of G, then *the height of their commutator is strictly greater than the height of both a and b.* For if we expand the expression of the commutator and take the definition of the adjoint inverse element into account, then we obtain

$$a' \circ b' \circ a \circ b = -a'b' - ab - a'b - b'a + a'ab + b'ab + \\ + a'b'a + a'b'b - a'b'ab.$$

The height of every term of the sum on the right-hand side is strictly greater than the height of each of the elements a and b, and the same is therefore true of their sum.

We now consider the lower central series of F

$$F = F_0 \supset F_1 \supset F_2 \supset \ldots \supset F_n \supset \ldots, \tag{3}$$

and show that the height of every element of F_n is greater than or equal to $n + 1$. This is true for $F = F_0$. Suppose it has been proved for F_n. If we form the commutator of an element a of F_n with an arbitrary element of F, we obtain an element whose height is strictly greater than the height of a and hence greater than or equal to $n + 2$. This also holds for the adjoint products of such commutators, that is, for every element of F_{n+1}.

It now follows that the intersection of the subgroups (3), that is, the ω-th term of the lower central series of the free group F of rank $\mathfrak{m}$ is E. Since the cardinal number $\mathfrak{m}$ was arbitrary, we have proved Magnus' Theorem.

We mention, without proof, a theorem of Witt [1] which states that *all the factors $F_n/F_{n+1}, n = 0, 1, 2, \ldots$ of the lower central chain of a free group F are free abelian groups.*

Another theorem of the same type as the above theorems of M. Hall and Magnus can be found in a paper by Levi [3]. All these results represent partial advances on the general and not-too-well-defined problem of a survey of all the subgroups of a free group or the problem—to use a terminology

to be introduced in Chapter XI—of a description of the lattice of subgroups of a free group. In any case, a free group is extremely rich in subgroups and even in normal subgroups. This can be seen from various considerations and, for instance, from the following theorem.

If g is an element other than 1 of a free group G, then there exists a normal subgroup of G, of finite index, that does not contain g.

This theorem is contained in the much more general Theorem 7 of the paper by Mal'cev [2]. Later it was proved independently by Iwasawa [2]. The following proof is very simple.

Let x_α (α ranges over a set of indices) be a system of free generators of G. Those generators that occur in the reduced form of g will be denoted by $x_1, x_2, \ldots, x_m$. The element g therefore has a reduced form

$$g = x_{i_1}^{\varepsilon_1} x_{i_2}^{\varepsilon_2} \ldots x_{i_n}^{\varepsilon_n}, \tag{4}$$

where $1 \leqq i_k \leqq m$, $\varepsilon_k = \pm 1$, for $k = 1, 2, \ldots, n$.

We take the symmetric group S_{n+1} of degree $n+1$, permuting the symbols $1, 2, \ldots, n+1$, and choose in it permutations

$$x_1', x_2', \ldots, x_m'. \tag{5}$$

in the following way. With $k = 1, 2, \ldots, n$, we make the following definition: If $\varepsilon_k = +1$, then the permutation x_{i_k}' (this is one of the permutations (5), since $1 \leqq i_k \leqq m$) shall carry k into $k+1$; if $\varepsilon_k = -1$, then x_{i_k}' shall carry $k+1$ into k. None of the permutations (5) of degree $n+1$ is completely determined by this condition, since so far every permutation (5) carries only part of the symbols $1, 2, \ldots, n+1$ into part of the same symbols. This mapping is, however, one to one, because by the irreducibility of the expression (4) none of the permutations (5) can carry an arbitrary symbol k into the two distinct symbols $k-1$ and $k+1$, nor two distinct symbols $k-1$ and $k+1$ into one and the same symbol k. The definition of the mappings (5) can therefore be completed; that is, they can be regarded as permutations of S_{n+1}.

We obtain a homomorphic mapping of G into the finite group S_{n+1} if we map the elements $x_1, x_2, \ldots, x_m$ onto $x_1', x_2', \ldots, x_m'$ respectively, and all the remaining free generators x_α onto the unit element of S_{n+1}. The kernel of this homomorphism is a normal subgroup of finite index in G. The element g lies outside this normal subgroup, because it is mapped onto the permutation

$$g' = x_{i_1}'^{\varepsilon_1} x_{i_2}'^{\varepsilon_2} \dots x_{i_m}'^{\varepsilon_m},$$

which by definition of the permutations (5) carries the symbol 1 into $n+1$, so that it is not the identity permutation. This completes the proof of the theorem.

A paper by M. Hall [2] contains a partial generalization of this theorem.

§ 37. Fully invariant subgroups of free groups. Identical relations

Fully invariant subgroups of free groups are of fundamental interest. This is due, in the first place, to their connection with the so-called *identical relations* in groups.

We know that in every abelian group the equation

$$x_1^{-1} x_2^{-1} x_1 x_2 = 1, \quad \text{or} \quad [x_1, x_2] = 1, \tag{1}$$

is satisfied when arbitrary group elements are substituted for the "variables" x_1 and x_2. Similarly, in every nilpotent group of class 2 (see § 14) we have

$$[[x_1, x_2], x_3] = 1 \tag{2}$$

for arbitrary group elements x_1, x_2, x_3. Lastly, in a finite group of order n the order of every element divides n, and therefore the equation

$$x_1^n = 1 \tag{3}$$

is satisfied "identically."

More generally, let G be a given group. We consider an auxiliary free group W with a countable set of free generators $x_1, x_2, \dots, x_n, \dots$. If w is an element of W, that is, a word in the generators $x_1, x_2, \dots, x_n, \dots$, then the equation

$$w = 1 \tag{4}$$

is called an *identical relation* in G if it is satisfied when arbitrary elements of G are substituted for the x that occur in w.

A group G may, in general, have many identical relations. For example, if (3) is satisfied identically in G, then the relations $x_1^{2n} = 1$, $x_2^n = 1$, $(x_1 x_2 x_3)^n = 1$ and so on, are also satisfied. *The left-hand sides of all identical relations of G form a fully invariant subgroup V_G of W.*

For if the identical relations

$$w_1 = 1,\ w_2 = 1$$

hold in G, then the relations

$$w_1 w_2 = 1 \text{ and } w_1^{-1} = 1$$

obviously also hold, so that the left-hand sides of the identical relations form a subgroup of the free group W. We now consider an arbitrary endomorphism φ of W. It carries every generator x_i into an element $x_i\varphi$, which is a word in the generators $x_1, x_2, \ldots, x_n, \ldots$. If (4) is an arbitrary identical relation of G and

$$w = x_{i_1}^{\alpha_1} x_{i_2}^{\alpha_2} \ldots x_{i_n}^{\alpha_n},$$

then

$$w\varphi = (x_{i_1}\varphi)^{\alpha_1} (x_{i_2}\varphi)^{\alpha_2} \ldots (x_{i_n}\varphi)^{\alpha_n}.$$

On the right-hand side there stands some word in the generators $x_1, x_2, \ldots$. The substitution of arbitrary elements of G for these generators is equivalent to the substitution of the elements in the words $x_{i_k}\varphi, k = 1, 2, \ldots, n$, and the substitution of the values so obtained into the word w. This last substition turns the word w into the unit element, and therefore

$$w\varphi = 1$$

is also an identical relation in G, that is, $w\varphi \in V_G$.

Thus, the identical relation (1) corresponds to the commutator group of W and the relation (2) to the second term W_2 of the lower central chain of W. Lastly, the fully invariant subgroup of W that corresponds to the identical relation (3) is the subgroup generated by the n-th powers of all the elements of W. In the sequel we shall call this subgroup the *n-th power* of W and denote it by W^n. The definition of this fully invariant subgroup carries over to an arbitrary group, as explained in § 14.

In order to give all the identical relations of a group G it is clearly not necessary to write out all the elements of the corresponding subgroup V_G, but it suffices to select elements in this subgroup which generate it as a fully invariant subgroup of W. This choice of elements is, of course, not unique.

If H is an arbitrary fully invariant subgroup of a free group W of countable rank, can we perhaps indicate a group G for which $H = V_G$ holds? An answer to this question, in the affirmative, can be derived from the following considerations.

Let G be a given group. We represent it as a factor group of a normal subgroup N in a free group F with a system of free generators $M=(a_\alpha)$

$$G\simeq F/N$$

and search for the identical relations of G.

Let H be the product of all the fully invariant subgroups of F contained in N; H is itself fully invariant in F. If

$$h=a_{\alpha_1}^{\varepsilon_1}a_{\alpha_2}^{\varepsilon_2}\dots a_{\alpha_n}^{\varepsilon_n}$$

is an arbitrary element of H, then the equation

$$x_{i_1}^{\varepsilon_1}x_{i_2}^{\varepsilon_2}\dots x_{i_n}^{\varepsilon_n}=1, \tag{5}$$

where $i_1, i_2, \dots, i_n$ are natural numbers and $i_k=i_l$ if and only if $\alpha_k=\alpha_l$, is an identical relation in G.

For in order to substitute arbitrary elements of G, that is, arbitrary cosets of N, in (5) it is necessary to substitute in the left-hand side representatives of these cosets, that is, certain words in the generators a_α. This is equivalent, however, to applying to the element h of F an endomorphism, which does not lead outside H nor, consequently, outside N. Equation (5) is thus satisfied for arbitrary elements of G, in other words, *it is an identical relation in* G.

Conversely, if

$$x_{i_1}^{\varepsilon_1}\ x_{i_2}^{\varepsilon_2}\dots x_{i_n}^{\varepsilon_n}=1 \tag{6}$$

is any identical relation of G, then after substituting arbitrary elements of F in its left-hand side we obtain elements that lie in N and, in fact, in H. For, all the elements of N that we obtain when we substitute elements of F in (6) in all possible ways generate a subgroup of N. It is easy to see that it is fully invariant in F and therefore contained in H. In particular, we get a certain element h of H by substituting arbitrary elements of M for the unknowns in (6) so that *the identical relation* (6) *in* G *belongs to those described in the preceding paragraph.*

Hence it follows that $G\simeq F/N$ and F/H have exactly the same identical relations. Note that in virtue of $H\subseteq N$ the first of these groups is isomorphic to a factor group of the second.

The factor groups of the fully invariant subgroups in free groups of arbitrary rank are called *reduced free groups*. We have therefore proved the following theorem.

Every group G is isomorphic to a factor group of a reduced free group having the same identical relations as G itself.

For example, the factor group of a free group with respect to its commutator group, that is, a free abelian group, is reduced. In the case of abelian groups—in other words, groups with the identical relation (1)—we are thus led to a result essentially equivalent to the theorem of § 19 according to which every abelian group is isomorphic to a factor group of a free abelian group.

We now see that every fully invariant subgroup H of a free group W of countable rank can play the rôle of the group V_G for a suitable group G: the factor group W/H will have precisely the elements of H as left-hand side of its identical relations.

Thus, if we wish to classify groups according to their identical relations, along the lines of the classification for the classes of abelian groups and nilpotent groups of class 2, then we would have to enumerate all fully invariant subgroups of a free group W of countable rank. On the other hand, the classification of all reduced free groups is connected with a survey of all fully invariant subgroups of arbitrary free groups. Let us prove some relevant theorems.

Every fully invariant subgroup H of a free group F, if not entirely contained in the commutator group F', is the product of its intersection K with F', $K = H \cap F'$, and of a power F^n of F, $n \geqq 1$. (Levi [3], B. H. Neumann [4].)

Let (a_α) be a system of free generators of F. Taking into account that the factor group F/F' is a free abelian group with the free generators $a_\alpha F'$, we can state that an element h of H can be written, as can every element of F, in the form

$$h = a_{\alpha_1}^{k_1} a_{\alpha_2}^{k_2} \dots a_{\alpha_m}^{k_m} f', \tag{7}$$

where $f' \in F'$, $m \geqq 0$, and where all the subscripts $\alpha_1, \alpha_2, \dots, \alpha_m$ are distinct and all the exponents $k_1, k_2, \dots, k_m$ different from zero. If here $h \notin F'$, then $m > 0$. The endomorphism of F that leaves a_{α_i} in place and carries all other generators a_α into 1 caries h into $a_{\alpha_i}^{k_i}$, since f' goes into 1 under this endomorphism, because in f' the sum of the exponents for every generator is 0. Now H is a fully invariant subgroup, so that

$$a_{\alpha_i}^{k_i} \in H, \; i = 1, 2, \dots, m, \tag{8}$$

and therefore $f' \in H$, that is,

$$f' \in (H \cap F') = K.$$

Let n be the smallest positive exponent with which any generator a_α occurs in H; the existence of such an n follows by what we have just proved from the assumption $H \not\subseteq F'$. But since there exists an endomorphism of F that carries a_α into an arbitrary preassigned element of F and since H is fully invariant, the n-th power of any element of F lies in H, that is, $H \supseteq F^n$. By (8) every exponent $k_1, k_2, \ldots, k_m$ in (7) must be divisible by n, so that

$$a_{\alpha_1}^{k_1} a_{\alpha_2}^{k_2} \ldots a_{\alpha_m}^{k_m} \in F^n.$$

We have thus shown that

$$H = F^n K, \tag{9}$$

and this completes the proof.

The number n introduced in this proof will be denoted by $n(H)$, and if $H \subset F'$ we put $n(H) = \infty$. We shall now prove:

If F is a free group and H a proper fully invariant subgroup, then the factor group of the commutator group in the reduced free group F/H is a direct product of cyclic groups of order $n(H)$; the number of these cyclic direct factors is equal to the rank of F.

For the commutator group of F/H is HF'/H. Now for $H \not\subseteq F'$ we have from (9) and from $K \subseteq F'$ that

$$HF' = F^n F';$$

therefore the factor group of the commutator group in F/H is isomorphic to $F/F^n F'$. But if $H \subseteq F'$, then the factor group of the commutator group in F/H is isomorphic simply to F/F'. In both cases this factor group is abelian and is clearly a direct product of cyclic groups of order n, the number of which is equal to the rank of F. Note that in virtue of the assumption $H \neq F$ the number $n(H)$ is greater than one.

We can now prove the following theorem of Baer [32] which completely reduces the problem of a classification of reduced free groups to a survey of all fully invariant subgroups of all free groups.

Every reduced free group G other than E has a unique representation as a factor group of a fully invariant subgroup of a free group.

Suppose G has two such representations

$$G \simeq F/H \simeq \overline{F}/\overline{H},$$

where F and $\overline{F}$ are free groups and where H and $\overline{H}$ are fully invariant subgroups of F and $\overline{F}$, respectively. By the preceding theorem the factor group

of the commutator group G' of G is a direct product of cyclic groups of one and the same order n. Any two such decompositions of G/G' are isomorphic, as follows from results of § 24 for finite n and from results of § 19 for $n = \infty$. Therefore, again by the preceding theorem, the free groups F and $\overline{F}$ have the same rank and hence are isomorphic.

So we can assume that in a free group F with a system of free generators (a_α) there are two fully invariant subgroups H and K with isomorphic factor groups

$$F/H \simeq F/K. \tag{10}$$

If

$$h = a_{\alpha_1}^{\varepsilon_1} a_{\alpha_2}^{\varepsilon_2} \dots a_{\alpha_n}^{\varepsilon_n}$$

is an arbitrary element of H then, as has been shown at the beginning of the section, the equation

$$x_{i_1}^{\varepsilon_1} x_{i_2}^{\varepsilon_2} \dots x_{i_n}^{\varepsilon_n} = 1$$

(where $i_k = i_l$ if and only if $\alpha_k = \alpha_l$) is an identical relation in F/H. By the isomorphism (10) it is also an identical relation in F/K; therefore the substitution of arbitrary elements of F in its left-hand side leads to an element of K. If, in particular, we substitute for every "unknown" x_{i_k} the element a_{α_l} we obtain h, which is therefore in the subgroup K. Thus $H \subseteq K$. Similarly $K \subseteq H$, and so $H = K$, and this is what we had to prove.

Now we shall indicate the connection between the problem of a survey of all fully invariant subgroups of a free group F of *arbitrary rank* and the corresponding problem for the case of a free group W of *countable rank*. If H is a fully invariant subgroup of F, then in W there corresponds to it a fully invariant subgroup $V_{F/H}$ consisting of the left-hand sides of the identical relations of F/H. If K is another fully invariant subgroup of F, then the subgroups $V_{F/H}$ and $V_{F/K}$ are distinct: if F/H and F/K had the same identical relations then by repeating the final part of the proof of the preceding theorem we would obtain that $H = K$. Moreover, if $H \subset K$, then $V_{F/H} \subset V_{F/K}$, because every identical relation of F/H holds in its homomorphic image F/K. If, conversely, $V_{F/H} \subset V_{F/K}$, then taking an elementary h of H and constructing, as at the beginning of the present section, the corresponding identical relation of F/H and therefore also of F/K, we see that $h \in K$, that is, $H \subset K$. Thus we have proved the following theorem (Baer [32]):

THEOREM: *There exists a one-to-one mapping between the set L_F of all fully invariant subgroups of a free group F of arbitrary rank and the set L_W*

of all fully invariant subgroups of a free group W of countable rank, preserving inclusion in both directions.

If the rank of F is infinite, then this is a mapping of L_F onto the whole of L_W.

For let $M = (x_\alpha)$ be a system of free generators of F. Since M is infinite we can choose a countable subset $M' = (x_1, x_2, \ldots, x_n, \ldots)$. We can now assume that W coincides with the subgroup of F generated by the set M'

Let V be an arbitrary fully invariant subgroup of W and H the fully invariant subgroup of F generated by the set V. We do not go outside H if we take an element of V and arbitrarily replace the elements of M' occurring in its expression by arbitrary elements of M. However, the reader will have no difficulty in verifying that all the elements of H that can be obtained in this way form a fully invariant subgroup of F and therefore exhaust all the elements of H. Thus

$$H \cap W = V,$$

so that the subgroup $V_{F/H}$ of W which corresponds to H in the above sense is, in fact, V.

If the rank r of F is *finite*, then the mapping of L_F into L_W defined above *is not a mapping onto the whole of* L_W. This is clear for $r = 1$ (because W has, for example, an infinite derived chain, while this is not true in an infinite cyclic group) and it can also be proved for other values of r.

A number of other properties of reduced free groups and of fully invariant subgroups of free groups can be found in papers by Levi [3], B. H. Neumann [4], Baer [32], and Mal'cev [9]. We might add that a complete survey of all fully invariant subgroups of the non-cyclic free groups, in other words, a description of the lattice of these subgroups in the sense of Chapter XI, has not yet been obtained.

CHAPTER X

FINITELY GENERATED GROUPS

§ 38. General properties of finitely generated groups

Finitely generated groups, which were first mentioned in § 6, form one of the natural generalizations of finite groups. We have developed an exhaustive theory for finitely generated abelian groups in § 20. In the general case, however, the study of finitely generated groups comes up against great difficulties, much more serious than, for example, the study of finite groups, whose theory is itself far from complete. Let us explain the underlying reasons for these difficulties.

As we have mentioned in § 5, the set of all non-isomorphic finite groups is countable, and from results in § 20 it follows that the set of non-isomorphic finitely generated abelian groups is also countable. In contrast, the set of all finitely generated groups has the cardinal number of the continuum: It cannot have a larger cardinal number, because every finitely generated group is countable; and it cannot have a smaller cardinal number, as a result of the following theorem. (B. H. Neumann [5]).[f]

The set of all non-isomorphic groups with two generators has the cardinal number of the continuum.

In § 9 (Lemma 1) we showed that in the alternating group of degree n, with $n \geqq 3$, the ternary cycles form a system of generators. We now show that *for odd n the elements*

$$a = (12 \ldots n)$$
$$b = (123)$$

also form a system of generators of the alternating group of degree n. This is obvious for $n = 3$; we therefore assume $n \geqq 5$. Note that a is an even permutation, because n is odd.

It is easy to verify that for $3 \leqq i < n$

$$ba^{-1}(1\ 2\ i)ab^2 = (1\ 2\ i+1\ ),$$

so that the subgroup $\{a, b\}$, which contains (123), contains all ternary cycles of the form $(12i)$, $3 \leqq i \leqq n$, and their inverses, $(1i2)$. If $i \neq j$, $i \geqq 3$, $j \geqq 3$, then

$$(12j)\ (12i)\ (1j2) = (1ij),$$

so that $\{a, b\}$ also contains all ternary cycles of the form $(1ij)$. Finally, if the symbols i, j, k, l are distinct from each other and from 1, then

$$(1li)\ (1jk)\ (1il) = (ijk),$$

that is, $\{a, b\}$ contains all ternary cycles of degree n and therefore coincides with the alternating group.

Now let

$$(U)\quad u_1 < u_2 < \ldots < u_n < \ldots$$

be an ascending sequence of odd numbers, $u_1 \geqq 5$, and let G_U' be the direct product product of the finite alternating groups whose degrees occur in U

$$G_U' = A_{u_1} \times A_{u_2} \times \ldots \times A_{u_n} \times \ldots .$$

Every group A_{u_n} is a group of even permutations on $\sigma_{n1}, \sigma_{n2}, \ldots, \sigma_{n,u_n}$, and the cycles $a_n = (\sigma_{n1}, \sigma_{n2}, \ldots, \sigma_{n,u_n})$ and $b_n = (\sigma_{n1}, \sigma_{n2}, \sigma_{n3})$ are generators of this group, as we have shown above. If Σ is the set of all symbols σ_{nk}, $k = 1, 2, \ldots, u_n$, $n = 1, 2, \ldots$, then G_U' is a subgroup of the unrestricted symmetric group of Σ, that is, the group of one-to-one mappings of Σ onto itself.

In the latter group we form the subgroup G_U generated by the elements

$$a = (\sigma_{11}, \sigma_{12}, \ldots, \sigma_{1,u_1})(\sigma_{21}, \sigma_{22}, \ldots, \sigma_{2,u_2}) \ldots (\sigma_{n1}, \sigma_{n2}, \ldots, \sigma_{n,u_n}) \ldots,$$

$$b = (\sigma_{11}, \sigma_{12}, \sigma_{13})(\sigma_{21}, \sigma_{22}, \sigma_{23}) \ldots (\sigma_{n1}, \sigma_{n2}, \sigma_{n3}) \ldots,$$

and show that $G_U \supset G_U'$.

An immediate verification shows that the elements $a_n^{-(u_m-2)} b a_n^{u_m-2}$ and b are permutable when $n > m$. Since in an arbitrary product of powers of a and b the cycles containing the symbols σ_{ni} with one and the same first index n are multiplied together just as in A_{u_n}, we see that the commutator k_m of the elements $a^{-(u_m-2)} b a^{u_m-2}$ and b leaves all the symbols σ_{mi} with $n > m$ in place but affects the symbols σ_{mi} and, possibly, certain σ's with a first index less than m. In other words, k_m is contained in the direct product of A_{u_m} and some of the subgroups A_{u_l}, $l < m$. This also holds for every element conjugate to k_m in G_U: the process of transforming an element x of A_{u_n} by an arbitrary element of G_U carries x into another element of the same subgroup A_{u_n}. Therefore the whole normal subgroup generated in G_U by k_m is contained in the direct product

$$A_{u_1} \times A_{u_2} \times \ldots \times A_{u_m}.$$

The component of this normal subgroup in the direct factor A_{u_m} is a normal subgroup of A_{u_m} other than E, that is, coincides with A_{u_m}, because A_{u_m} is simple. If we assume that $A_{u_1}, \ldots, A_{u_{m-1}}$ are contained in G_U (for $m = 1$ this is obvious), then we obtain that A_{u_m} is also contained in G_U. It follows that all the subgroups A_{u_n} are contained in G_U as normal subgroups.

On the other hand, let H be an arbitrary *finite* normal subgroup of G_U. To every element h of H there corresponds an element of A_{u_n} that effects the same permutation of the symbols $\sigma_{n1}, \sigma_{n2}, \ldots, \sigma_{n,u_n}$, as h. These "components" of the element of H form a normal subgroup of A_{u_n} which must be equal either to A_{u_n} or to E, because A_{u_n} is simple. But since H is finite, from a certain index $n+1$ onwards the second alternative must hold. In other words, the normal subgroup H leaves all the symbols σ_{ki} with $k > n$ unaltered and is, therefore, contained in the direct product

$$A_{u_1} \times A_{u_2} \times \ldots \times A_{u_n},$$

and the component of H in A_{u_n} is the whole of A_{u_n}.

Now let H be isomorphic to an alternating group A_k, $k \geqq 5$. Being simple, H is isomorphic to its component in A_{u_n}, that is, to A_{u_n} itself, so that $k = u_n$. From what we have proved above we deduce that G_U has a finite normal subgroup isomorphic to an alternating group A_k if and only if k is equal to one of the u_n in U.

The set of distinct sequences of type U has the cardinal number of the continuum. If U_1 and U_2 are two such sequences, then it follows from the above that G_{U_1} and G_{U_2} cannot be isomorphic. We therefore obtain a continuous set of non-isomorphic groups with two generators, and this is what we set out to prove.

It follows from this theorem that there exists no "universal" countable group containing subgroups isomorphic to all countable groups; a countable group can clearly contain only a countable set of subgroups with two generators. It is still an open problem whether a group of the cardinal number of the continuum exists such that every group of the cardinal number of the continuum is isomorphic to a subgroup of that group.

In connection with the result obtained above we mention without proof (see Kuroš [9] and also § 49 of the first edition of this book) that the set of all non-isomorphic groups of an arbitrary infinite cardinal number $\mathfrak{m}$ has the cardinal number $2^{\mathfrak{m}}$. Later Kulikov proved that this holds even for abelian groups of cardinal number $\mathfrak{m}$.

We can give yet another reason for the great complexity of the class of all finitely generated groups; we begin with the following lemma, which is of independent interest (see G. Higman, B. H. Neumann and Hanna Neumann [1]).

Lemma 1. *Let A and B be isomorphic subgroups of a group G and let φ be an isomorphic mapping of A onto B. Then G can be embedded in a group H containing an element h such that the transformation of A by h induces the mapping φ,*

$$h^{-1}ah = a\varphi \text{ for all } a \text{ of } A.$$

We consider the free products

$$K = G*\{u\},\ L = G*\{v\},$$

where $\{u\}$ and $\{v\}$ are infinite cyclic groups. From a result in § 34 it follows that the subgroup $U = \{G, u^{-1}Au\}$ of K has a free decomposition and the subgroup $\{G, vBv^{-1}\}$ of L a free decomposition

$$U = G*u^{-1}Au$$
$$V = G*vBv^{-1}.$$

We obtain an isomorphic mapping ψ of U onto V by putting

$$g\psi = g \text{ for all } g \text{ of } G,$$
$$(u^{-1}au)\psi = v(a\varphi)v^{-1}$$

for all a of A.

We can therefore construct the free product H of K and L with an amalgamated subgroup (see § 35) by amalgamating U and V in accordance with the isomorphism ψ. H contains G as a subgroup. On the other hand, since in H

$$u^{-1}au = v(a\varphi)v^{-1} \text{ for all } a \text{ of } A$$

we have

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

so that uv is the required element h.

Lemma 2. *Let A_α be a subgroup of a group G (α ranges over an index set M). Suppose that for every α an isomorphic mapping φ_α of A_α onto a subgroup B_α of G is given. Then G can be embedded in a group H which, for every α, contains an element h_α such that the transformation of A_α by h_α*

induces the mapping φ_α. *Moreover, the elements* h_α, $\alpha \in M$, *can be chosen so that they generate a free subgroup of* H *and are free generators of it.*

We define the group H in the following way: Its generators shall be the generators of G and the symbols h_α, $\alpha \in M$, and its defining relations shall be the defining relations of G together with all the equations

$$h_\alpha^{-1} a_\alpha h_\alpha = a_\alpha \varphi_\alpha, \text{ where } a_\alpha \in A_\alpha, \ \alpha \in M \tag{1}$$

(the elements a_α and $a_\alpha \varphi_\alpha$ are, of course, assumed to be expressed by the generators of G). The elements h_α are then indeed free generators of the subgroup of H that they generate: if we put all the generators of G equal to the unit element, we turn the relations (1) into identities, and therefore no non-trivial relation linking the elements h_α only can follow from them and from the relations of G.

On the other hand, if the generators of G were linked in H by a relation that is not a consequence of the defining relations of G, then this relation could be obtained after adjunction of a finite number of elements h_α. It would then be satisfied *a fortiori* if these elements h_α were adjoined to G in accordance with the basic Lemma 1; but that is not the case. Thus H contains G as subgroup and so satisfies all the requirements of Lemma 2. For what follows we mention that *the generators* h_α *of* H *occur in relation* (1) *only.*

Applying Lemma 2 to the case when $A_\alpha = G$ for all α, and φ_α ranges over all the automorphisms of G, we obtain a group H that plays the same rôle as the holomorph of G.

Our aim is the following theorem, which was expressed as a problem in the first edition of this book and proved in the paper by G. Higman, B. H. Neumann, and Hanna Neumann [1].

Every countable group G *can be embedded isomorphically in a group with two generators.*[1]

Proof. We choose in G a finite or a countable system of generators $g_1, g_2, \ldots$. Further, we set

$$K = G * \{u\}, \tag{2}$$

where $\{u\}$ is an infinite cyclic group. As a system of generators of K we can take the elements u and

$$u_i = u g_i, \ i = 1, 2, \ldots, \tag{3}$$

[1] For finite groups this theorem has, in essence, been proved in § 5, since every finite symmetric group has a system of two generators by § 6, Example 2.

since $g_i = u^{-1}u_i$, $i = 1, 2, \ldots$. The elements u_i are all of infinite order, so that the cyclic groups generated by them are isomorphic. By Lemma 2, K can therefore be embedded in a group L in which there are elements h_i, $i = 1, 2, \ldots$ satisfying the conditions

$$h_i^{-1} u h_i = u_i, \quad i = 1, 2, \ldots; \tag{4}$$

moreover, the elements h_i are free generators of the subgroup H that they generate; they occur only in the defining relations (4) of L, and together with K they generate the whole group. By (4), we can take as generators of L the elements u and h_i, $i = 1, 2, \ldots$.

Now let W be the free group with the generators x, y. We know from § 36 that in the commutator group of W we can find a subgroup with the same (finite or countable) number of free generators $s_1, s_2, \ldots$ as there are elements h_i, $i = 1, 2, \ldots$. We can therefore form the free product Q of L and W with the amalgamated subgroup that arises from the isomorphic subgroups H and S by means of the equations

$$h_i = s_i, \; i = 1, 2, \ldots. \tag{5}$$

In view of (5), Q is generated by u, x, and y.

Let us show that u and x are not linked by any relations in Q. By (2) there exists a homomorphic mapping of K onto an infinite cyclic group $\{\bar{u}\}$ under which u goes into $\bar{u}$ and all the elements of G into the unit element; hence by (3) all the elements u_i, $i = 1, 2, \ldots$ also go into $\bar{u}$. This homomorphism can be extended to a homomorphic mapping of L onto $\{\bar{u}\}$ under which the elements h_i, $i = 1, 2, \ldots$ go into the unit element; for they occur in the relations (4) only, and these relations are not violated by this mapping. On the other hand, there exists a homomorphic mapping of the free group W onto the infinite cyclic group $\{\bar{x}\}$ under which x goes into $\bar{x}$ and y into the unit element; all the elements of the commutator group, in particular all the elements s_i, $i = 1, 2, \ldots$, also go into the unit element under this mapping. We can now define a homomorphic mapping φ of Q onto the free group $\{\bar{u}\} * \{\bar{x}\}$, mapping L onto $\{\bar{u}\}$ and W onto $\{\bar{x}\}$ as above: on the amalgamated subgroups H and S these mappings are compatible, since both these subgroups are mapped into the unit element. The mapping φ carries the elements u, x into free generators $\bar{u}$, $\bar{x}$, respectively, of a free group, and therefore they cannot be linked by any relations in Q.

Thus we have in Q two free subgroups of rank 2, namely $\{x, y\}$ and $\{x, u\}$. By Lemma 1, Q can be embedded in a group R generated by adjoining to Q an element z such that

$$z^{-1}xz = u, \quad z^{-1}yz = x,$$

and hence $zxz^{-1} = y$. It follows that R, generated by the elements u, x, y, z, is in fact a group with two generators x and z. This completes the proof of the theorem.

A number of essentially negative results are known about finitely generated groups. For example, there exist finitely generated groups that are isomorphic to proper factor groups (B. H. Neumann [9], G. Higman [2]). This gives a negative solution to a problem that was known as *Hopf's problem*. This cannot happen in free groups of finite rank, as we shall prove in the following section. It is also known that there exist infinite simple groups with a finite number of generators (G. Higman [3]); this answers a problem that was proposed in the first edition of this book.[g]

Very little is known about the following extremely important problem, the so-called Burnside problem: *Is every finitely generated periodic group finite?*

This problem has not yet been solved even under the restriction that the orders of the elements of the group are bounded. The answer, in the affirmative, is obvious in the case in which the orders of all the elements other than the unit are 2, because such a group is necessarily abelian. Burnside [2] has also found an affirmative answer in the case in which the orders of the elements are 3 and, furthermore, for groups with two generators in which the orders of all the elements are 4 or divisors of 4; the first case is also studied in a paper by Levi and van der Waerden [1]. Further, B. H. Neumann [3] has found the solution for groups in which the orders of the elements do not exceed 3 and, finally, Sanov [1] for groups with an arbitrary finite number of generators in which the order of the elements does not exceed 4. However, even for groups with two generators in which the order of all the elements other than the unit element are 5, the problem remains open. Note that all such groups are factor groups of the reduced free group B_5 with two generators, that is, are obtained by imposing the identical relation $x^5 = 1$ (see § 37). Attempts have been made to give upper estimates for the orders of the finite factor groups of B_5 (Sanov [5]), but they have not yet led to a definite result. Sanov [3] has proved that for an affirmative solution of Burnside's problem in the case of bounded orders, a solution for groups with two generators is sufficient.[h]

We conclude the present section with a proof of the following theorem (M. Hall [4]):

A finitely generated group can have only a finite number of subgroups of given finite index j.

For let G be a group with the generators $a_1, a_2, \ldots, a_n$, and let H be a subgroup of G, of index j. We denote by

$$K_1 = H, K_2, \ldots, K_j \tag{6}$$

the right cosets of H in G. If g is an arbitrary element of G, then the transition from the coset system (6) to the system

$$K_1 g, K_2 g, \ldots, K_j g$$

is a permutation of (6), which we denote by $P(g)$. Thus we obtain a mapping φ,

$$g\varphi = P(g), g \in G \tag{7}$$

of G into the symmetric group S_j of degree j. This is a homomorphic mapping, since

$$P(g_1 g_2) = P(g_1) P(g_2).$$

The homomorphism φ is completely determined by the images of the elements $a_1, a_2, \ldots, a_n$. There consequently exists only a finite number of distinct homomorphisms of G into S_j, namely at most $(j!)^n$. However, the homomorphism φ introduced in (7) determines the subgroup H uniquely, because an element g is contained in H if and only if the permutation $P(g)$ leaves the coset K_1 invariant. A group G with n generators therefore contains not more than $(j!)^n$ subgroups of index j.

§ 39. Gruško's Theorem

We shall now study free decompositions of finitely generated groups; these decompositions are of considerable interest in connection with certain problems of combinatorial topology. All the questions that can be raised here are essentially answered by Gruško's Theorem (Gruško [2]), which will be proved in this and the following section.

Let a group G have a system of generators

$$\overline{g_1}, \overline{g_2}, \ldots, \overline{g_n}, \tag{1}$$

which are assumed to be not necessarily distinct from one another or from the unit element. If an element h of G has in terms of the generators (1) an expression in which $\overline{g_j}$ does not occur, then obviously we again obtain

a system of generators for G if in (1) we replace $\overline{g}_j$ by $h\overline{g}_j$ or by $\overline{g}_j h$. Further, replacing $\overline{g}_j$ in (1) by $\overline{g}_j^{-1}$ also leads to a system of generators. Every system of generators of G that is obtained from (1) by a finite number of transformations of the form indicated will be called *admissible* (with respect to (1)).

Suppose now that G is decomposed into a free product

$$G = A_1 * A_2 * \ldots * A_k. \tag{2}$$

The normal forms of the elements of G, their length, their left halves, middles, and right halves, etc. will be considered in what follows with respect to the free decomposition (2).

We shall call an admissible system of generators *minimal* if the sum of the lengths of its elements or the *length of the system* does not exceed the length of any other admissible system of generators of G (with respect to the original system (1)).

GRUŠKO'S THEOREM: *Every element of an arbitrary minimal system of generators is contained in one of the free factors of the decomposition* (2).

Before we proceed to the proof of this theorem let us indicate a few of its consequences.

The minimal number of generators of a finitely generated group is equal to the sum of the corresponding numbers for all factors of an arbitrary free decomposition of the group.

For if (1) is a system of generators of G with the smallest possible number of elements, if (2) is a given free decomposition of G and

$$g_1, g_2, \ldots, g_n \tag{3}$$

a minimal admissible system of generators relative to (1), then those elements of the system (3) that lie in the free factor A_i, $i = 1, 2, \ldots, k$, form a system of generators of A_i by Gruško's Theorem; clearly A_i cannot have a system of generators with a smaller number of elements.[1]

It follows that *a free decomposition of a group with n generators consists of not more than n factors*, and hence that *every finitely generated group can be decomposed into the free product of a finite number of indecomposable groups.*

Corollaries of another kind also follow from Gruško's Theorem. To every choice of a system of n generators in G there corresponds a homo-

[1] An alternative proof of this result is contained in a paper by B. H. Neumann [8].

morphic mapping of the free group with n free generators onto G. In the case of a free group the transformation of a system of generators considered above give a transition from one system of free generators to another system of free generators. From Gruško's Theorem we can therefore deduce the following theorem, which is essentially equivalent to it.

If a free group S with a finite number of generators is mapped homomorphically onto a group G that is decomposable into the free products of subgroups $A_1, A_2, \ldots, A_k$, then we can choose in S a system of free generators such that each generator is mapped by the homomorphism in question into an element of one of the free factors A_i.

From this it follows that *a free group of rank n cannot have a system of generators consisting of fewer than n elements.* This result could also be obtained immediately by going over to the factor group of the derived group.

Every system of generators of a free group of rank n that consists of n elements is a system of free generators.

For if $a_1, a_2, \ldots, a_n$ is a system of free generators of a free group S, and if $b_1, b_2, \ldots, b_n$ is a system of n generators of S, then by Gruško's Theorem there exists a system of generators $b_1', b_2', \ldots, b_n'$, admissible relative to $b_1, b_2, \ldots, b_n$ and such that every b_i' lies in one subgroup $\{a_j\}$. Since every $\{a_j\}$ must contain at least one of the b_i', we can assume that $b_i' \in \{a_i\}$, because the number of elements in both systems is equal. Now it is easy to see that $b_i' = a_i^{\pm 1}$, that is, $b_1', b_2', \ldots, b_n'$ is a system of free generators of S. The generators $b_1, b_2, \ldots, b_n$ are therefore also free.

This result states, in other words, that *every homomorphic mapping of a free group of finite rank onto itself is isomorphic* or that *a free group of finite rank cannot be isomorphic to one of its proper factor groups.* This theorem was first proved by Magnus [6], using other methods. It can also be deduced from earlier results of Nielsen [3].

We now turn to the proof of Gruško's Theorem.

Proof of Gruško's Theorem. Let

$$g_1, g_2, \ldots, g_n \tag{4}$$

be a minimal admissible system of generators (relative to (1)) of a group G possessing the free decomposition (2). An element g_i of this system of length l, $l > 1$, is called *special* if we can find in (4) elements g_j and $g_{i_1}, g_{i_2}, \ldots, g_{i_s}$ and exponents ε and $\alpha_1, \alpha_2, \ldots, \alpha_s$, equal to ± 1, such that the following conditions are satisfied (here, and in what follows, $l(g)$ is the length of g with respect to the free decomposition (2)):

1) $j \neq i$,
2) $l(g_j) = l$,
3) $l(g_{i_1}) < l, \ldots, l(g_{i_s}) < l$,
4) $l(g_i \cdot \prod_\nu g_{i_\nu}^{\alpha_\nu} \cdot g_j^{\varepsilon}) \leqq l$,
5) $l(\prod_\nu g_{i_\nu}^{\alpha_\nu} \cdot g_j^{\varepsilon}) = l$,
6) $l(\prod_\nu g_{i_\nu}^{\alpha_\nu}) < l$.

Further, let g be an element of G of length l, and let P, Q, and R stand for[1] its left half, middle, and right half (relative to (2)), so that $g = PQR$ where, for even l, $Q = 1$. The element is called *reducible* (relative to the system (4)) if we can find in (4) elements $g_{i_1}, g_{i_2}, \ldots, g_{i_s}$ and exponents $\alpha_1, \ldots, \alpha_s$ such that $l(g_{i_\nu}) < l$, $\nu = 1, 2, \ldots, s$, and

$$g \cdot \prod_\nu g_{i_\nu}^{\alpha_\nu} = PQP^{-1},$$

that is, for even l, $g \cdot \prod_\nu g_{i_\nu}^{\alpha_\nu} = 1$. Otherwise g is called *irreducible*.

Let us assume, for the time being, that the following statement has been proved.

(B) *If* (4) *is a minimal admissible system of generators of* G, *and if among its elements there is one of length greater than* 1, *then* (4) *contains irreducible special elements.*

Let $g_i = PQR$ be one of the elements of shortest length among the irreducible special elements of the minimal admissible system (4). If the elements g_j and $g_{i_1}, g_{i_2}, \ldots, g_{i_s}$ and their exponents have been chosen in accordance with the definition of a special element, then we have by (4) and (5)

$$\bar{g} = \prod_\nu g_{i_\nu}^{\alpha_\nu} \cdot g_j^{\varepsilon} = R^{-1} Q' T,$$

where Q' lies in the same free factor as Q. If $Q = 1$, then $Q' = 1$. We now modify the system (4), replacing g_j by an element g_j' defined as follows:

$$g_j' = g_i \bar{g} = P(QQ')T, \tag{5}$$

[1] These abbreviations will be used in the sequel without special comment.

if $\bar{g}$ is irreducible; but if $\bar{g}$ is reducible, and if in accordance with the definition of a reducible element

$$\bar{g} \cdot \prod_{\mu} g_{j_\mu}^{\beta_\mu} = R^{-1}Q'R, \quad l(g_{j_\mu}) < l, \quad \mu = 1, 2, \ldots, t,$$

then

$$g_j' = g_i \bar{g} \cdot \prod_{\mu} g_{j_\mu}^{\beta_\mu} \cdot g_i^{-1} = P(QQ'Q^{-1})P^{-1}. \tag{6}$$

In both cases g_j can be expressed by g_j' and the remaining elements of (4), so that we obtain another system of generators for G; it is easy to see that it also is admissible and minimal.

We shall now show that, after we replace in this way all the elements of (4) that can play the rôle of g_j in the definition of a special element with respect to the elements g_i under consideration, g_i *ceases to be a special element*. For if there were a new element g_j' with exponent δ, and a product $\prod_{\mu} g_{i_\mu}^{\gamma_\mu}$ satisfying the requirements of the definition of a special element, then we would have

$$\prod_{\mu} g_{i_\mu}^{\gamma_\mu} \cdot g_j'^{\delta} = R^{-1}Q''U, \tag{7}$$

where Q'' lies in the same free factor as Q. However, since the left half of $g_j'^{\delta}$ is equal to P if $\bar{g}$ is irreducible and $\delta = +1$, and also if $\bar{g}$ is reducible and $\delta = \pm 1$, it would follow from the equation

$$\prod_{\mu} g_{i_\mu}^{\gamma_\mu} \cdot P = R^{-1}$$

which holds in this case,[1] that $R \cdot \prod_{\mu} g_{i_\mu}^{\gamma_\mu} = P^{-1}$, in contradiction to the fact that g_i is irreducible; the only possible case remaining is: $\bar{g}$ irreducible and $\delta = -1$. In that case, however, from (5) and (7) it would follow that $\prod_{\mu} g_{i_\mu}^{\gamma_\mu} \cdot T^{-1} = R^{-1}$, that is,

$$R = T\left(\prod_{\mu} g_{i_\mu}^{\gamma_\mu}\right)^{-1}.$$

But then $\bar{g}$ would turn out to be reducible, in contradiction to our assumption.

No new irreducible special elements of length l can appear in our transformations of (4). For an element of length l which was reducible in (4) remains reducible after the replacement of g_j by g_j', since the length of the

[1] Condition (6) of the definition of a special element has to be taken into account.

elements g_{i_ν} that occur in the definition of a reducible element are less than l. Suppose, further, that after we replace g_j by g_j' an element g_m, $m \neq i$, $m \neq j$, $l(g_m) = l$, becomes special. This means that we can choose an exponent ε' for g_j' and a product $\prod_\sigma g_{k_\sigma}^{\delta_\sigma}$ such that for g_m and these elements all the requirements appearing in the definition of a special element are satisfied. It is easy to see, however, that in that case g_m was special even before the change in the system (4): the rôle of g_j was taken by g_i if $\varepsilon' = +1$ and $\bar{g}$ is irreducible, and also if $\varepsilon' = +1$ and $\bar{g}$ is reducible (in these cases the left half of $g_j'^{\varepsilon'}$ coincides with the left half of g_i) and was taken by the original element g_j if $\varepsilon' = -1$ and $\bar{g}$ is reducible.

Suppose, finally, that g_j' itself turns out to be special. If the element $g = \prod_\nu g_{i_\nu}^{\alpha_\nu} \cdot g_j^{\varepsilon}$ was irreducible, so that g_j' is defined by (5), then for $\varepsilon = -1$ it follows from

$$l(g_j'^{-1}) = l[g_j (\prod_\nu g_{i_\nu}^{\alpha_\nu})^{-1} g_i^{-1}] = l$$

that g_j itself was special; only condition 5) of the definition of a special element requires verification; this is very simple and is left to the reader. But if $\varepsilon = +1$, then from the fact that g_j' is special it follows that g_j was also special, since in this case the two elements have the same right halves, and their middles are contained in one and the same free factor. In the case in which $\bar{g}$ is reducible, that is, when g_j' is defined by the formula (6), we have the equation

$$l(g_j') = l(g_i \cdot \prod_\nu g_{i_\nu}^{\alpha_\nu} \cdot g_j^{\varepsilon} \cdot \prod_\mu g_{j_\mu}^{\beta_\mu} \cdot g_i^{-1}) = l,$$

from which we deduce easily that

$$l(g_i \cdot \prod_\nu g_{i_\nu}^{\alpha_\nu} g_j^{\varepsilon}) \leqq l,$$

$$l(g_j^{\varepsilon} \cdot \prod_\mu g_{j_\mu}^{\beta_\mu} \cdot g_i^{-1}) \leqq l.$$

These two equations show that g_j is itself a special element: the first shows it for $\varepsilon = -1$, the second for $\varepsilon = +1$. Conditions 5) and 6) of the definition of a special element are obviously satisfied in both cases.

The transformations of the system (4) considered above therefore decrease the number of irreducible special elements of length l in the system, and after

a finite number of steps we arrive at a system that contains no irreducible special elements of length l at all. The number l was the minimal length of irreducible special elements in (4). We have therefore increased this minimal length,[1] and since our transformations do not diminish the lengths of the elements of the given system of generators, nor their number, after a finite number of such increases we obtain a new minimal admissible system of generators of G in which certain elements, as before, have length greater than 1, and this is in contradiction to the statement (B) that there are no irreducible special elements in the system. Gruško's Theorem will therefore be proved if we can confirm the truth of (B).

§ 40. Gruško's Theorem (conclusion)

We now come to the proof of statement (B).

By assumption the system (4) of the preceding section is a minimal admissible system of generators of G, and the lengths of some of the elements exceed 1. Since (4) is minimal, none of its elements other than the unit element can be expressed by the remaining elements of the system: if $l(g_i) \geqq 1$, and $g_i = \prod_\nu g_{j_\nu}^{\alpha_\nu}$, $j_\nu \neq i$; then the replacement of g_i by

$$g_i' = g_i^{-1} \cdot \prod_\nu g_{j_\nu}^{\alpha_\nu}$$

leads to a new admissible system of generators of length smaller than (4), because $g_i' = 1$.

Every element of an arbitrary free factor $A_1, A_2, \ldots, A_k$ can be expressed in terms of the generators of (4), and in one of the subgroups A_m we can find an element a whose expressions in terms of these generators all involve elements of length greater than 1. For otherwise the elements of length 1 in (4) would be sufficient to express all the elements of G and, among them, the elements of (4) of length greater than 1, and we have just shown this to be impossible. Among the distinct expressions of a by the generators of (4) we select those in which the maximal length of the elements (4) that occur in it is as small as possible, and among them we select those in which the elements with this maximal length occur the least number of times, and among them in turn those expressions in which the elements of length one less than the maximal length occur the least number of times, and so on,

[1] New irreducible special elements, obviously, cannot appear among the elements of length less than l. (*Cf.* the definition of a special element.)

ending up with the elements of length 1.

Let

$$a = g_{j_1}^{\varepsilon_1} g_{j_2}^{\varepsilon_2} \dots g_{j_\omega}^{\varepsilon_\omega}, \quad \varepsilon_i = \pm 1, \quad i = 1, 2, \dots, \omega, \tag{8}$$

be one of these expressions; we have $\omega \geqq 2$, because the expression must involve elements of length greater than 1. We shall use the following notation for the partial products on the right-hand side of (8):

$$[\mu, \nu] = g_{j_\mu}^{\varepsilon_\mu} g_{j_{\mu+1}}^{\varepsilon_{\mu+1}} \dots g_{j_\nu}^{\varepsilon_\nu}, \quad 1 \leqq \mu < \nu \leqq \omega.$$

$l[\mu, \nu]$ is the length of $[\mu, \nu]$, relative to the free decomposition (2).

We shall now prove some lemmas about the right-hand side of (8).

LEMMA I. *There exist indices* μ, ν *with* $1 \leqq \mu < \nu \leqq \omega$ *such that*

1) $l(g_{j_\mu}) = l[\mu, \mu+1] = \dots = l[\mu, \nu-1] > l[\mu, \nu]$,

2) $l(g_{j_\mu}) \geqq l(g_{j_\lambda})$, $\mu < \lambda \leqq \nu$,

3) $l(g_{j_\mu}) \geqq 2$.

For there exists a μ such that[1] $l[1, \mu-1] < l[1, \mu]$, but for all $\lambda \geqq \mu$, $l[1, \lambda] \geqq l[1, \lambda+1]$. Since $l[1, \omega] = l(a) = 1$ for $\mu = \omega$, we would have $l[1, \omega-1] = 0$, that is, $[1, \omega-1] = 1$. However, it would then follow that $a = g_{j_\omega}^{\varepsilon_\omega}$, which is impossible in view of $l(a) = 1$ and the assumptions made about a.

We shall now look for some ν, $\mu < \nu \leqq \omega$, such that

$$l[1, \mu] = l[1, \mu+1] = \dots = l[1, \nu-1] > l[1, \nu].$$

Such an index ν exists if $l[1, \mu] \geqq 2$, since $l[1, \omega] = l(a) = 1$. But if $l[1, \mu] = 1$, then $l[1, \mu-1] = 0$, that is, $[1, \mu-1] = 1$, and in virtue of the assumptions about the right-hand side of (8) we would have $l[1, \lambda] = 1$.

Let $g_{j_\sigma}^{\varepsilon_\sigma}$ be the first factor of (8) whose length exceeds 1. Then from $l[1, \sigma] = 1$ it follows that the replacement of g_{j_σ} in (4) by

$$g'_{j_\sigma} = [1, \sigma] = [1, \sigma-1] \cdot g_{j_\sigma}^{\varepsilon_\sigma}$$

leads to a new admissible system of generators of length shorter than in (4).

[1] In other words, μ is the index of the last factor of (8) which leads, on multiplication by the product of the preceding factor, to an increase in length.

This contradicts the minimal property of (4) and proves the existence of ν.

In what follows we shall use the notation $l(g_{j_\mu}) = l$. Let us prove statements 1) and 2) of Lemma I. From $l[1, \mu-1] < l[1, \mu]$ it follows that in the product $[1, \mu-1] \cdot g_{j_\mu}^{\varepsilon_\mu} = [1, \mu]$ the middle of $g_{j_\mu}^{\varepsilon_\mu}$ remains unaltered or, for even l, its left half is not cancelled completely. Suppose we have already proved for some λ, $\mu < \lambda < \nu$, that $l(g_{j_\sigma}) \leqq l$ for $\mu < \sigma \leqq \lambda$, that $l[\mu, \lambda] = l$ and that in the product $[1, \mu-1]\ [\mu, \lambda]$ the middle of $[\mu, \lambda]$ remains unaltered or, for even l, its left half is not cancelled completely. If $l(g_{j_{\lambda+1}}) > l$ then from $l[1, \lambda] \geqq l[1, \lambda+1]$ it would follow that in the product

$$[1, \lambda+1] = [1, \mu-1]\,[\mu, \lambda] \cdot g_{j_{\lambda+1}}^{\varepsilon_{\lambda+1}}$$

when the cancellations between $[\mu, \lambda]$ and $g_{j_{\lambda+1}}^{\varepsilon_{\lambda+1}}$ are carried out, the whole right half and the middle of $[\mu, \lambda]$ would cancel and, for even l, its left half would be affected by cancellations. Hence it would follow that $l[\mu, \lambda+1] < l(g_{j_{\lambda+1}})$; but since in $[\mu, \lambda+1]$ the element $g_{j_{\lambda+1}}^{\varepsilon_{\lambda+1}}$ is the only factor of length greater than l, we could then diminish the length of the system (4) by replacing $g_{j_{\lambda+1}}$ by the element $g'_{j_{\lambda+1}} = [\mu, \lambda+1]$. Clearly, this again gives an admissible system of generators. Therefore $l(g_{j_{\lambda+1}}) \leqq l$. If now $\lambda + 1 < \nu$, then $l[1, \lambda] = l[1, \lambda+1]$, and so $l[\mu, \lambda+1] = l[\mu, \lambda] = l$, and the left halves of $[\mu, \lambda+1]$ and $[\mu, \lambda]$ coincide. Thus for $\lambda + 1 < \nu$ all the induction hypotheses have been proved. But if $\lambda + 1 = \nu$, then it follows from $l[1, \lambda] > l[1, \nu]$ that the cancellations in the product $[\mu, \lambda] \cdot g_{j_\nu}^{\varepsilon_\nu}$ eliminate the whole left half and middle of $g_{j_\nu}^{\varepsilon_\nu}$, so that $l[\mu, \nu] < l$.

Finally, from $l = 1$ it would now follow that $l[\mu, \nu] = 0$, that is, $[\mu, \nu] = 1$, But this would enable us to replace (8) by a shorter product, and this contradicts our assumptions about (8). Hence $l \geqq 2$, and Lemma I is proved.

We shall now assume that $[\mu, \nu]$ is chosen in accordance with Lemma I. We shall also assume that this product has the smallest number of factors among all those products of the form $[\sigma, \tau]$ and $[\sigma, \tau]^{-1}$, $1 \leqq \sigma < \tau \leqq \omega$ that satisfy all the requirements of Lemma I. Moreover, we can assume that this product $[\mu, \nu] = g_{j_\mu}^{\varepsilon_\mu} g_{j_{\mu+1}}^{\varepsilon_{\mu+1}} \ldots g_{j_\nu}^{\varepsilon_\nu}$ is a product with the smallest total number of factors which can be constructed from the elements of (4)

in keeping with all the requirements of Lemma 1. The length of g_{j_μ} will be denoted by l, as above.

LEMMA II. *Every element g_i of length l that appears in the product $[\mu, \nu]$ at all occurs in it at least twice.*

For if an element g_i, $l(g_i) = l$ occurs in $[\mu, \nu]$ only once, then by $l[\mu, \nu] < l$ the replacement of g_i in (4) by $g_i' = [\mu, \nu]$ leads to a new admissible system of generators, of length smaller than (4).

LEMMA III. *If $\mu \leqq \sigma \leqq \tau \leqq \nu$ and if the product $[\sigma, \tau]$ does not contain a factor of length l, then $l[\sigma, \tau] < l$. But if factors of length l occur in the product and if $\tau < \nu$, then $l[\sigma, \tau] = l$.*

Let us suppose the assertions of the lemma to be already proved for all the partial products of $[\mu, \nu]$ consisting of a smaller number of factors than $[\sigma, \tau]$—they obviously hold for $\sigma = \tau$. Then we have to consider the following cases:

1) $l[\sigma, \tau - 1] < l$, $l(g_{j_\tau}) < l$, $\tau \leqq \nu$. In this case it follows from $l[\mu, \sigma - 1] = l[\mu, \tau - 1] = l$ that in the product

$$[\mu, \tau - 1] = [\mu, \sigma - 1] \cdot [\sigma, \tau - 1] \tag{9}$$

the right half of the second factor remains unaltered. Now from

$$[\mu, \tau] = [\mu, \sigma - 1] \cdot [\sigma, \tau - 1] \cdot g_{j_\tau}^{\varepsilon_\tau} \tag{10}$$

and $l[\mu, \tau] \leqq l$, $l(g_{i_\tau}) < l$ it follows that in the product $[\sigma, \tau - 1] \cdot g_{j_\tau}^{\varepsilon_\tau}$ the cancellations must go so far that either the right half of the first factor or the left half of the second factor is eliminated, while the middle of the corresponding factor will at least undergo an amalgamation. Therefore

$$l[\sigma, \tau] \leqq \max(l[\sigma, \tau - 1], l(g_{j_\tau})) < l.$$

2) $l[\sigma, \tau - 1] = l$, $l(g_{j_\tau}) < l$, $\tau < \nu$. In this case the right half of the second factor of (9) again remains unaltered, and it therefore follows from $l[\mu, \tau] = l$, $l(g_{j_\tau}) < l$ and (10) that the cancellations in the product $[\sigma, \tau - 1] \cdot g_{j_\tau}^{\varepsilon_\tau}$ eliminate the left half of $g_{j_\tau}^{\varepsilon_\tau}$ and that its middle is amalgamated. Therefore $l[\sigma, \tau] = l$.

3) $l[\sigma, \tau - 1] < l$, $l(g_{j_\tau}) = l$, $\tau < \nu$. From (10) and

$$l[\mu, \sigma - 1] = l[\mu, \tau - 1] = l[\mu, \tau] = l \tag{11}$$

it follows, as above, that $l[\sigma, \tau] \leqq l$. However, if the inequality sign holds,

then we could decrease the length of (4), since g_{j_τ} is now the only element of length l in $[\sigma, \tau]$. Therefore $l[\sigma, \tau] = l$.

4) $l[\sigma, \tau - 1] = l$, $l(g_{j_\tau}) = l$, $\tau < \nu$. Again, we have $l[\sigma, \tau] \leqq l$, by (11). Suppose $l[\sigma, \tau] < l$. Since by the induction hypothesis $l[\lambda, \tau] = l$, $\sigma < \lambda < \tau$, we would find in this case that $[\sigma, \tau]^{-1}$ satisfies all the requirements of Lemma I, although it consists of a smaller number of factors that $[\mu, \nu]$, in contradiction to the choice of the latter element. Therefore $l[\sigma, \tau] = l$.

LEMMA IV. $l(g_{j_\nu}) = l$.

For if $l(g_{j_\nu}) < l$, then let $g_{j_\lambda}^{\varepsilon_\lambda}$ be the last factor of length l in $[\mu, \nu]$. Since

$$l[\mu, \lambda] = l[\mu, \lambda - 1] = l(g_{j_\lambda}) = l,$$

the elements $[\mu, \lambda]$ and $g_{j_\lambda}^{\varepsilon_\lambda}$ have identical right halves. It follows, further, from Lemma III under our assumptions that for $\lambda < \sigma \leqq \nu$, $l[\lambda + 1, \sigma] < l$. Therefore for $\sigma < \nu$ it follows easily from $l[\mu, \sigma] = l$ that $l[\lambda, \sigma] = l$ and from $l[\mu, \nu] < l$ that $l[\lambda, \nu] < l$. In other words, the product $[\lambda, \nu]$ satisfies all the requirements of Lemma I, although it contains only one element of length l, in contradiction to Lemma II.

LEMMA V. *The product* $[\mu, \nu]$ *contains at least one factor* $g_{j_\lambda}^{\varepsilon_\lambda}$, $\mu < \lambda < \nu$, *of length* l.

For if $l(g_{j_\lambda}) < l$ for all λ, $\mu < \lambda < \nu$, then by II we have $g_{j_\mu} = g_{j_\nu}$ and by III $l[\mu + 1, \nu - 1] < l$. Therefore, if $g_{j_\mu}^{\varepsilon_\mu} = PQR$, where P is the left half, Q the middle, and R the right half of $g_{j_\mu}^{\varepsilon_\mu}$, then $[\mu, \nu - 1] = PQR'$. If now $\varepsilon_\nu = -\varepsilon_\mu$, that is, $g_{j_\nu}^{\varepsilon_\nu} = R^{-1}Q^{-1}P^{-1}$, then from

$$l[\mu, \nu] = l([\mu, \nu - 1] \cdot g_{j_\nu}^{\varepsilon_\nu}) < l$$

it follows that $R'R^{-1} = 1$, so that $[\mu, \nu] = 1$, and this is impossible by the conditions imposed on the product (8). But if $\varepsilon_\nu = \varepsilon_\mu$, that is, $g_{j_\nu}^{\varepsilon_\nu} = PQR$, then $R'R = 1$, $Q^2 = 1$, and $[\mu, \nu] = PR$. However, since

$$R' = R.\,[\mu + 1, \nu - 1],$$

it follows from $P = R'^{-1}$ that

$$[\mu, \nu] = [\mu + 1, \nu - 1]^{-1}R^{-1} \cdot R = [\mu + 1, \nu - 1]^{-1};$$

in contradiction to the conditions imposed on (8) we could again replace that product by a shorter one.

Lemma V is thus proved.

LEMMA VI. *In the product* $[\mu, \nu]$ *there occurs at least one irreducible element* g_{j_λ}, *of length* l, *with* $\mu < \lambda < \nu$.

We begin with some preliminary remarks. From the definition of a reducible element it follows immediately that if g is reducible and $g_i^{\varepsilon_i}$ is such that $l(g_i^{\varepsilon_i}) < l(g)$ and $l(g g_i^{\varepsilon_i}) = l(g)$, then the product $g g_i^{\varepsilon_i}$ is also reducible; the same is true of $g_i^{\varepsilon_i} g$ provided $l(g_i^{\varepsilon_i} g) = l(g)$. Furthermore, if g_1 and g_2 are reducible and $l(g_1) = l(g_2) = l(g_1 g_2)$, then $g_1 g_2$ is also reducible. For let $g_1 = PQR$; then $g_2 = R^{-1} Q' S$ and $g_1 g_2 = P(QQ')S$, where Q and Q' lie in the same free factor and for odd length $QQ' \neq 1$. If now, by definition of a reducible element,

$$g_1 \cdot \prod_k g_{i_k}^{\varepsilon_k} = PQP^{-1}, \quad g_2 \cdot \prod_l g_{j_l}^{\delta_l} = R^{-1} Q' R,$$

then

$$g_1 g_2 \cdot \prod_l g_{j_l}^{\delta_l} \cdot \prod_k g_{i_k}^{\varepsilon_k} = P(QQ')P^{-1},$$

that is, $g_1 g_2$ is also reducible. Finally, it is easy to see that from the reducibility of g there follows that of g^{-1}, and vice versa.

We now turn to the proof of the lemma. It is clearly true for even l, because if there were a reducible element of even length in (4), then the system would not be minimal. Let l be odd. From Lemma V there follows the existence of a factor $g_{j_\lambda}^{\varepsilon_\lambda}$ of length l in $[\mu, \nu]$ with $\mu < \lambda < \nu$. If all such factors were reducible, then the above remarks and Lemma III show that the product $[\mu + 1, \nu - 1]$ would also be reducible. Moreover, again by Lemma III, $l[\mu + 1, \nu - 1] = l$. Let $[\mu + 1, \nu - 1] = PQR$, and

$$[\mu + 1, \nu - 1] \cdot \prod_k g_{i_k}^{\alpha_k} = PQP^{-1}.$$

Then $g_{j_\mu}^{\varepsilon_\mu} = SQ_1 P^{-1}$, $g_{j_\nu}^{\varepsilon_\nu} = R^{-1} Q_2 T$, and in view of $l[\mu, \nu] < l$ we must have $Q_1 Q Q_2 = 1$ and $[\mu, \nu] = ST$. If the elements $g_{j_\mu}^{\varepsilon_\mu}$ and $g_{j_\nu}^{\varepsilon_\nu}$ are also reducible, let

$$g_{j_\mu}^{\varepsilon_\mu} \cdot \prod_m g_{x_m}^{\beta_m} = SQ_1 S^{-1}, \qquad g_{j_\nu}^{\varepsilon_\nu} \cdot \prod_n g_{y_n}^{\gamma_n} = R^{-1} Q_2 R.$$

Now

$$R \cdot \prod_k g_{i_k}^{\alpha_k} = P^{-1}, \qquad P^{-1} \cdot \prod_m g_{x_m}^{\beta_m} = S^{-1}, \qquad T \cdot \prod_n g_{y_n}^{\gamma_n} = R.$$

Hence

$$[\mu, \nu] = S \cdot T = (\prod_m g_{x_m}^{\beta_m})^{-1} \cdot PR\,(\prod_n g_{y_n}^{\gamma_n})^{-1} =$$

$$= (\prod_m g_{x_m}^{\beta_m})^{-1} (\prod_k g_{t_k}^{\alpha_k})^{-1} (\prod_n g_{y_n}^{\gamma_n})^{-1},$$

that is to say, the product $[\mu, \nu]$ can be expressed by elements of (4) of length smaller than l. But this contradicts the conditions imposed on (8).

If now at least one of the elements $g_{j_\mu}^{\varepsilon_\mu}$, $g_{j_\nu}^{\varepsilon_\nu}$ is irreducible, then by Lemma II $g_{j_\mu} = g_{j_\nu}$. If $\varepsilon_\mu = \varepsilon_\nu$, then $S = R^{-1}$, $P^{-1} = T$, hence

$$[\mu, \nu] = ST = R^{-1}P^{-1} = \prod_k g_{t_k}^{\alpha_k}.$$

But if $\varepsilon_\mu = -\varepsilon_\nu$, then $S = T^{-1}$, hence $[\mu, \nu] = ST = 1$. In both cases we again arrive at a contradiction to the conditions imposed on (8). This proves Lemma VI.

LEMMA VII. *Every irreducible element g_{j_λ} of length l, $\mu < \lambda < \nu$, is special.*

If $\varepsilon_\lambda = +1$, then we take the element $g_{j_\sigma}^{\varepsilon_\sigma}$ that stands nearest to g_{j_λ} on the right among all elements of length l in $[\mu, \nu]$, $\sigma \leqq \nu$. Now we shall convince ourselves, by recourse to $[\lambda, \sigma]$ that g_{j_λ} satisfies all the requirements in the definition of a reducible element. For conditions 2) and 3) follow from the choice of the element $g_{j_\sigma}^{\varepsilon_\sigma}$, conditions 4), 5), and 6) from Lemma III for $\sigma < \nu$. For $\sigma = \nu$ they are also easily seen to be satisfied.

It remains to show that condition 1) holds. Let $j_\sigma = j_\lambda$. If $\varepsilon_\sigma = +1$ and $g_{j_\lambda} = PQR$, then we also have $g_{j_\sigma}^{\varepsilon_\sigma} = PQR$, hence

$$g_{j_\lambda} \cdot \prod_{\alpha=\lambda+1}^{\sigma-1} g_{j_\alpha}^{\varepsilon_\alpha} \cdot g_{j_\sigma}^{\varepsilon_\sigma} = PQR \cdot \prod_{\alpha=\lambda+1}^{\sigma-1} g_{j_\alpha}^{\varepsilon_\alpha} \cdot PQR.$$

Since $l[\lambda, \sigma] \leqq l$ and $l[\lambda, \sigma - 1] = l$, it follows that

$$R \cdot \prod_{\alpha=\lambda+1}^{\sigma-1} g_{j_\alpha}^{\varepsilon_\alpha} = P^{-1}$$

and this contradicts the irreducibility of $g_{j\lambda}$. But if $\varepsilon_\sigma = -1$, that is, $g_{j_\sigma}^{\varepsilon_\sigma} = R^{-1}Q^{-1}P^{-1}$, then

$$g_{j_\lambda} \cdot \prod_{\alpha=\lambda+1}^{\sigma-1} g_{j_\alpha}^{\varepsilon_\alpha} \cdot g_{j_\sigma}^{\varepsilon_\sigma} = PQR \cdot \prod_{\alpha=\lambda+1}^{\sigma-1} g_{j_\alpha}^{\varepsilon_\alpha} \cdot R^{-1}Q^{-1}P^{-1}.$$

In view of $l[\lambda, \sigma] \leqq l$ and $l[\lambda, \sigma - 1] = l$ this implies that $\prod_{\alpha=\lambda+1}^{\sigma-1} g_{j_\alpha}^{\varepsilon_\alpha} = 1$, and hence $[\lambda, \sigma] = 1$, in contradiction to the conditions imposed on (8). This proves that g_{j_λ} is a special element.

Finally, if $\varepsilon_\lambda = -1$, then we take in $[\mu, \nu]$ the element of length l standing nearest on the left to $g_{j_\lambda}^{\varepsilon_\lambda}$ and proceed with a similar argument. This proves Lemma VII.

The proof of the statement (B) and with it the proof of Gruško's theorem is now complete.

§ 41. Groups with a finite number of defining relations

If a group G is given in some system of generators by a finite system of defining relations, then only a finite number of the generators occur in these relations, and G is therefore the free product of a free group and of a finitely generated group with a finite number of defining relations. We can therefore confine ourselves to the study of finitely generated groups.

Groups with a finite number of generators and defining relations—we shall call them *finitely presented groups—form a much narrower class of groups than that of all groups with a finite number of generators*; we have seen in § 38 that the latter form a set with the cardinal number of the continuum, whereas simple set-theoretical considerations show that the set of all finitely generated and finitely related groups is only countable.

To the class of finitely presented groups belong all *finite* groups, for they can be given by their Cayley tables (see § 18).

We wish to prove a few theorems which follow immediately from the definition, given above, of finitely presented groups and which show that this class of groups is, in fact, well defined. We begin by indicating, without reference to the finiteness of the number of generators and defining relations, certain types of transformations of a system of generators and defining relations, that is, certain methods of transition from a given system of generators and defining relations to another system of generators and defining relations of the same group.

THEOREM. *Let a group G be given by a system of generators $\mathfrak{M}$ consisting of the symbols $a_\alpha, a_\beta, \ldots$ and a system of defining relations linking these generators. Then the same group can be given by the system of generators $\overline{\mathfrak{M}}$ consisting of the set $\mathfrak{M}$ and a new symbol b, provided that a relation of the form*

$$bw(a) = 1$$

is added to the defining relations, where $w(a)$ is any given word in the symbols a_α, a_β, ...

We first prove the following lemma.

LEMMA. *Let W be the free group with a system of free generators $\mathfrak{M}$. If b is an element of $\mathfrak{M}$, $\mathfrak{M}'$ the set of all elements of $\mathfrak{M}$ except b, and B the normal subgroup of W generated by b, then the factor group W/B is isomorphic to the free group with $\mathfrak{M}'$ as a system of free generators.*

For the subgroup W' of W generated by $\mathfrak{M}'$ is a free group with $\mathfrak{M}'$ as a system of free generators. On the other hand, every word that occurs in B has the following property: If all the powers of the symbol b in it are deleted and then all necessary cancellations are carried out, then the empty word results. This statement is clear for words that are conjugate to b. For arbitrary elements of B it follows from the remark that if w_1 and w_2 are words of W that are transformed into the empty word by deletion of powers of b and subsequent cancellations, then $w_1 w_2$ has the same property. It follows that the intersection $B \cap W' = E$, so that by the isomorphism theorem

$$W/B \simeq W'/E \simeq W'.$$

We now turn to the proof of the theorem. If W is the free group with $\mathfrak{M}$ as a system of free generators, then $G \simeq W/H$, where H is the normal subgroup generated by the left-hand sides of the defining relations. Let $\overline{W}$ be the free group with $\overline{\mathfrak{M}}$ as a system of free generators—we then have $\overline{W} \supset W$—and let $\overline{H}$ be the normal subgroup of $\overline{W}$ generated by the elements that occur in H and by $c = bw(a)$. We have to show that

$$\overline{W}/\overline{H} \simeq W/H.$$

Let us assume first that $w(a)$ is the empty word, so that $c = b$. If B is is the normal subgroup of $\overline{W}$ generated by b, then by the lemma,

$$\overline{W}/B \simeq W.$$

By the theorem on the correspondence between the subgroups of a group and the subgroups of a factor group of the group (§ 10), the normal subgroup H corresponds to a normal subgroup $\overline{H}'$ of $\overline{W}$ and

$$\overline{W}/\overline{H}' \simeq W/H.$$

But $\overline{H}'$ actually coincides with $\overline{H}$: it contains H as well as b, that is,

$\overline{H'} \supseteq \overline{H}$, while on the other hand every element of $\overline{H'}$ has the form hb' with $h \in H$, $b' \in B$, so that $\overline{H'} \subseteq \overline{H}$.

The case of an arbitrary word $w(a)$ will reduce to the case just considered if we can show that the set $\mathfrak{M}$ and the element $c = b \cdot w(a)$ together form a new system of free generators for $\overline{W}$. For this purpose it is sufficient to prove that the elements $a_\alpha, a_\beta, \ldots$ are not linked with c by any relations; for it is clear that these elements together generate the whole group $\overline{W}$.

Suppose, then, that we have in $\overline{W}$ an equation

$$w_1(a)\, c^{\delta_1} w_2(a)\, c^{\delta_2} \ldots w_k(a)\, c^{\delta_k} = 1,$$

where $w_1(a), w_2(a), \ldots, w_k(a)$ are non-empty words in the elements $a_\alpha, a_\beta, \ldots$, and $\delta_1, \delta_2, \ldots, \delta_k$ are non-zero integers. After we replace every c in this equation by $bw(a)$ and carry out all the cancellations, the left-hand side must become the empty word, because otherwise we would obtain a relation linking the symbols of $\mathfrak{M}$ in $\overline{W}$. Now all factors b and b^{-1} actually remain uncancelled, since for $i = 2, 3, \ldots, k$

$$c^{-1} w_i(a)\, c = w^{-1}(a)\, b^{-1} w_i(a)\, bw(a),$$

$$c w_i(a)\, c^{-1} = bw(a)\, w_i(a)\, w^{-1}(a)\, b^{-1},$$

so that in both cases b and b^{-1} are separated by a non-empty word. This completes the proof.

By a *transformation of type A* we shall mean a transformation of a system of generators and defining relations of the type described in the theorem just proved and also its inverse transformation, which consists in the omission of an element b from the system of generators, provided the element occurs in only one defining relation of the form $bw(a) = 1$, where $w(a)$ is a word in the remaining generators; this relation is also to be omitted from the system of defining relations.

On the other hand, if a group is given by some generators and some defining relations, then any other relation between the generators is a *consequence* of the given defining relations, that is to say, its left-hand side is contained in the normal subgroup of the free group generated by the left-hand sides of the defining relations; this relation can therefore be added to the system of defining relations. Conversely, we can omit from the system of defining relations every relation that is a consequence of the remaining defining relations. Transformations of this kind shall be called *transformations of type B*.

The transformations of type B enable us to give an easy proof of the following stronger form of von Dyck's Theorem (see § 18). *If two groups G and G' are given by certain defining relations in one and the same system of generators and if every defining relation of G is a consequence of the defining relations of G', then G' is isomorphic to a factor group of G.* For G' can in this case be defined by the totality of the given defining relations of G and G', and it only remains to apply von Dyck's Theorem.

We explain, finally, *transformations of type B'.* Let G be a group given by the generators a_α, a_β, ..., and b, and by a system of defining relations one of which has the form

$$bw(a) = 1,$$

where b also occurs in other defining relations. We take one of these relations

$$\overline{w}(a; b) = 1 \tag{1}$$

(the left-hand side is a word in a_α, a_β, ..., and b) and replace one of the factors b occurring in it by $w^{-1}(a)$ (or b^{-1} by $w(a)$) and carry out the necessary cancellations. We obtain a new relation

$$\overline{w}'(a; b) = 1 \tag{2}$$

and we replace relation (1) in our system of defining relations by this relation.

The transformations of type B' can be obtained by a simple application of transformations of the type B. If, for example,

$$\overline{w}(a;\ b) = \overline{w}_1(a;\ b)\, b\, \overline{w}_2(a;\ b),$$

where w has been written in a form that exhibits the factor b that is to be replaced, then

$$\overline{w}'(a;\ b) = \overline{w}_1(a;\ b)\,(bw(a))^{-1}\,\overline{w}_1^{-1}(a;\ b)\,\overline{w}(a;\ b),$$

so that (2) is a consequence of the given defining relations and can therefore, by B, be added to the system of defining relations. But if we now solve the last equation with respect to $\overline{w}(a; b)$, then we find that (1) is a consequence of the remaining relations and can therefore be omitted.

These types of transformations of the defining relations enable us to prove a few important theorems on finitely presented groups.

If a group G is given by a finite system of generators linked by a finite

number of defining relations, then in any other finite system of generators the group can also be given by a finite system of defining relations.

Let G be given by the generators $a_1, \ldots, a_k$ and the defining relations $w_1(a) = 1, \ldots, w_s(a) = 1$. Let $b_1, \ldots, b_l$ be another finite system of generators for G. Every b_i can be expressed as a power product of elements of the first system. For every i we choose one of the possible expressions

$$b_i = f_i(a) \qquad i = 1, 2, \ldots, l.$$

The group G can now be given (transformations of type A) by the generators $a_1, \ldots, a_k, b_1, \ldots, b_l$ and the defining relations

$$\left.\begin{aligned} w_1(a) = 1, \ldots, w_s(a) = 1, \\ b_1 = f_1(a), \ldots, b_l = f_l(a). \end{aligned}\right\} \tag{3}$$

Further, we express every a_j by $b_1, \ldots, b_l$,

$$a_j = \varphi_j(b), \qquad j = 1, 2, \ldots, k,$$

and add to the defining relations (3) the relations

$$a_1 = \varphi_1(b), \ldots, a_k = \varphi_k(b), \tag{4}$$

which must be consequences of the relations (3) (transformations of type B). By means of the relations (4) we now replace the elements $a_1, \ldots, a_k$ in (3) by their expressions in terms of $b_1, \ldots, b_l$ (transformations of type B'). We obtain $s + l$ relations linking the elements $b_1, \ldots, b_l$. These relations, together with (4), give a system of defining relations for G in the generators $a_1, \ldots, a_k$ and $b_1, \ldots, b_l$. Finally, by applying transformations of type A we omit the generators $a_1, \ldots, a_k$ and the relations (4).

If a group G is given by a finite number of defining relations in a finite system of generators, then we can select from an arbitrary system of defining relations linking any other finite system of generators a finite subsystem that is also sufficient to give the group.

On account of the above theorem we can confine ourselves to the following case: G is given in terms of the generators $a_1, a_2, \ldots, a_k$ by a finite system of defining relations

$$w_1(a) = 1, \ldots, w_s(a) = 1,$$

as well as by an infinite system of defining relations

$$\overline{w}_1(a) = 1, \overline{w}_2(a) = 1, \ldots.$$

In the corresponding free group the words $w_1(a), \ldots, w_s(a)$ generate the same normal subgroup as the words

$$\overline{w}_1(a), \overline{w}_2(a), \ldots \tag{5}$$

However, every element $w_i(a)$, $i = 1, 2, \ldots, s$ can be expressed as a product of a finite number of elements conjugate to elements of the sequence (5). Thus, a finite number of elements in (5) already suffice to generate the whole normal subgroup H. Finally, the following theorem holds (Tietze [1]).

If a finitely presented group G is given in two ways by a finite system of generators, then we can go from one to the other by a finite number of transformations of types A and B.

For let G be given, on the one hand, by the generators $a_1, \ldots, a_k$ linked by the defining relations

$$w_1(a) = 1, \ldots, w_s(a) = 1 \tag{6}$$

and on the other by the generators $b_1, \ldots, b_l$ with the relations

$$w_1'(b) = 1, \ldots, w_t'(b) = 1. \tag{7}$$

Since every b_i must be expressible by the first system, let $b_i = f_i(a)$, $i = 1, 2, \ldots, l$; similarly, $a_j = \varphi_j(b)$, $j = 1, 2, \ldots, k$. By applying transformations of type A we can now give G by the generators $a_1, \ldots, a_k$, $b_1, \ldots, b_l$ and the defining relations (6) and

$$b_1 = f_1(a), \ldots, b_l = f_l(a),$$

and then, by performing transformations of type B, adjoin the relations (7) and the relations

$$a_1 = \varphi_1(b), \ldots, a_k = \varphi_k(b).$$

In a completely analogous way we could have arrived at the same system of generators and relations starting from the second presentation of G. The proof of the theorem is now completed by the remark that transformations inverse to those of type A and B belong to the same types.

For groups with a finite number of generators and defining relations it is natural to raise certain problems of an algorithmic character (see Dehn [1]). The most important among them is the *word problem* (or *identity problem*): An arbitrary group is given by a finite number of generators and relations

and an algorithm is required which will allow us to decide in a finite number of steps whether a given word in these generators is equal to the unit element, or else to prove that such an algorithm cannot exist. This problem can also be formulated, of course, as the problem of finding an algorithm to decide whether a given element of a free group W is contained in the normal subgroup generated in W by some other given elements.[1]

The word problem has so far been solved successfully for some classes of groups more special than that of all groups with a finite number of generators and defining relations. For example, for free groups (even without the assumption about the finite number of generators) a solution of the word problem follows from the fact that every element has a unique irreducible representation. Furthermore, it is easy to see that the word problem can be solved for a free product if a solution is known for each factor. For groups with a single defining relation the word problem has been solved by Magnus [3]. A new rather general approach to the word problem is contained in papers by Tartakowskiĭ [1-6].[1]

Equally difficult is the *conjugacy problem*, or *transformation problem*, that is, the problem of finding an algorithm to decide in a finitely presented group whether two given words are conjugate. For free groups this problem has an affirmative solution: If w is a word in the free generators of a free group W, then we "bend the word into a circle," that is, we write down its end in front of its beginning and carry out all the cancellations. In this way we obtain the "cyclic" word corresponding to w; in a cyclic word all the elements are of equal standing: there is no first nor last. Now two words in a free group W are obviously conjugate if and only if one and the same cyclic word corresponds to them both.[1]

Finally, there is the *isomorphism problem*, that is, the problem of finding an algorithm to decide whether two finitely presented groups are isomorphic. This problem has not even been solved yet in the case in which one of the given groups is the trivial group, nor in the case in which each of the two groups is given by a single defining relation. A similar isomorphism problem arises for finite groups when they are given by their Cayley tables.

Groups with a single defining relation form a class of groups that in a certain sense is closest to free groups. Their study has been carried some-

[1] Quite recently Novikov [1-3] has proved that the word problem and the transformation problem for finitely presented groups are algorithmically unsolvable.[1] [*Trans.*]

what further than that of groups with an arbitrary finite number of relations; but, for example, the subgroup problem for groups with a single defining relation is far from exhausted. The fundamental result here is the following *Freedom Theorem* (Magnus [1]).

If a group G is given by the generators $a_1, a_2, \ldots, a_n$ and one relation $f(a_1, a_2, \ldots, a_n) = 1$, and if further the element a_n occurs in this relation and cannot be removed from it by transformations, then the subgroup $\{a_1, \ldots, a_{n-1}\}$ is free, and $a_1, \ldots, a_{n-1}$ are free generators of the subgroup.

We shall not prove this theorem[1] but we mention that it has the consequence that two elements of a free group W generate the same normal subgroup of W if and only if they are conjugate. This once more points to the great wealth of normal subgroups in a free group, on which we have already commented in § 36.

In a paper by Whitehead [2] an algorithm is given to decide whether a given group with one defining relation is isomorphic to a free group.

[1] See also Reidemeister [3].

CHAPTER XI

DIRECT PRODUCTS. LATTICES

§ 42. Preliminary remarks

The definition and the simplest properties of the direct product of groups have been dealt with in § 17. The aim of the present chapter is the exposition of deeper results in the theory of direct products.

We know from the theory of abelian groups (see §§ 25 and 26) that there exist groups that are direct products but cannot be decomposed into the direct product of indecomposable groups. This leads us to inquire for conditions under which such a decomposition is possible. A partial answer is given by the following theorem.

THEOREM. *If all the decreasing chains of direct factors of a group G break off, then G cannot be decomposed into the direct product of an infinite set of subgroups, and every direct decomposition of G with a finite number of factors can be refined to a decomposition in which all the factors are indecomposable.*

For if G has direct decompositions with an infinite set of factors, then there exist decompositions in which the set of factors is countable; let

$$G = A_1 \times A_2 \times \ldots \times A_n \times \ldots$$

be one of them. If

$$B_k = A_k \times A_{k+1} \times \ldots,$$

then

$$G = B_1 \supset B_2 \supset \ldots \supset B_k \supset \ldots$$

is an infinite decreasing sequence of direct factors of G. This proves the first half of the theorem.

Let

$$G = H_1 \times H_2 \times \ldots \times H_k$$

be a direct decomposition of G that cannot be refined to a decomposition with indecomposable factors. It follows then that at least one of the direct factors, say H_1, is decomposable but cannot be decomposed into the direct product of indecomposable factors. We take a direct decomposition of H_1,

$H_1 = H_{11} \times H_{12}$. At least one of the subgroups H_{11}, H_{12}, which are clearly direct factors of G, must itself be decomposable but without a decomposition into indecomposable factors. Continuing this process we arrive at an infinite decreasing chain of direct factors of G.

In the formulation of this theorem the assumption that decreasing chains of direct factors of G break off can be replaced by the condition that *increasing chains of direct factors break off*. For if an indefinitely decreasing sequence of direct factors of a group G is given,

$$G \supset H_1 \supset H_2 \supset \ldots \supset H_n \supset \ldots,$$

then by VII′ (§ 17) $H_n = H_{n+1} \times F_n$, $n = 1, 2, \ldots$. We therefore arrive at an increasing sequence

$$F_1 \subset (F_1 \times F_2) \subset \ldots \subset (F_1 \times F_2 \times \ldots \times F_n) \subset \ldots$$

consisting of direct factors of G. Therefore, when the increasing chains of direct factors break off then the decreasing chains of direct factors also break off, and the above theorem follows.

COROLLARY. *Every group in which the descending or ascending normal chains break off—in particular, every group with principal series—decomposes into the direct product of a finite number of indecomposable factors.*

In § 17 we have given a number of examples of indecomposable groups. We know further, from § 35, that every group that is decomposable into a free product cannot be decomposed into a direct product. This result shows, in particular, that there exists no group, other than E, which would be a direct factor in every group containing it as a subgroup. The following theorem is therefore of interest, because it throws new light on complete groups (see § 13).

THEOREM. *Every complete group is a direct factor in any group in which it is contained as a normal subgroup.*

Proof. Let G be a group containing a complete group A as a normal subgroup. We denote the centralizer of A in G by B. As we have shown at the end of § 11, it is a normal subgroup of G. The intersection of A and B is E, because A is a group without center, so that A and B form a direct product in G. But this direct product must be the whole of G: if g is an arbitrary element of G, then the transformation of A by this element induces an automorphism of the complete group A which must be an inner automorphism, that is, must be generated by the transformation by an element

a of A. It follows that the element $b = a^{-1}g$ is permutable with every element of A, in other words, that it belongs to B, so that

$$g = ab \in A \times B$$

and $G = A \times B$.

It can be shown (see Baer [33]) that only complete groups have the property discussed in this theorem.

In what follows we shall be interested in two fundamental problems of the theory of direct products of groups. First of all, there is the problem of *conditions under which any two direct decompositions of a group have a common refinement*; such a group admits not more than one direct decomposition with indecomposable factors. Even the finite abelian groups show that the case in which a group has a unique direct decomposition with indecomposable factors is very rare. In the non-commutative case, however, it occurs more often; we shall show below that all groups without center and all groups that coincide with their derived groups have this property.

Even more important is the problem of *conditions under which any two direct decompositions of a group have isomorphic refinements* so that any two direct decompositions with indecomposable factors turn out to be isomorphic, provided that the group admits such decompositions at all. We know that many important types of abelian groups have this property. But on the other hand, as we have shown in § 28, there exist primary abelian groups with direct decompositions that do not have isomorphic refinements. Corresponding examples for the case of abelian operator groups that are decomposable into direct products of a finite number of indecomposable groups have been given by Krull [3], and Kuroš [16] has constructed an *example of a group without operators that has two non-isomorphic direct decompositions, each consisting of two indecomposable factors.* This example will now be given.

We consider a group A with generators a_1 and a_2 and one defining relation

$$a_1^2 = a_2^2.$$

It is (see § 35) the free product of two infinite cyclic groups with the amalgamated subgroup $\{a\}$, where

$$a = a_1^2 = a_2^2.$$

From results of § 35 it follows that the center of A is $\{a\}$ and that A does not contain elements of finite order other than 1. A is therefore not decomposable into a direct product: if such a decomposition existed, then the center $\{a\}$ would have to be contained entirely in one of the direct

factors, and the component of each element a_1, a_2 in the other factor could not be of order more than two.

We also consider a group B with generators b_1 and b_2 and one defining relation

$$b_1^3 = b_2^3.$$

As above, B has as its center the subgroup $\{b\}$, where

$$b = b_1^3 = b_2^3,$$

it contains no element of finite order other than 1 and, finally, it is not decomposable into a direct product.

The required group G is the direct product of A and B:

$$G = A \times B. \tag{1}$$

In order to construct a second direct decomposition of G not isomorphic with (1), we put

$$c = a^3b^{-2}, \quad d = a^{-1}b,$$
$$c_1 = aa_1b^{-1}, \quad c_2 = aa_2b^{-1}, \quad c_3 = ab^{-1}b_1, \quad c_4 = ab^{-1}b_2. \tag{2}$$

Let

$$C = \{c_1, c_2, c_3, c_4\}, \quad D = \{d\}.$$

Since (2) implies the equations

$$c_1d = a_1, \quad c_2d = a_2, \quad c_3d = b_1, \quad c_4d = b_2,$$

we have

$$G = \{C, D\}.$$

Furthermore, C and D are elementwise permutable, since D is part of the center of G.

We now find the intersection of C and D. From (2) it follows that

$$c_1^2 = c_2^2 = c_3^3 = c_4^3 = c$$

and that each of the elements c_1, c_2 is permutable with both c_3 and c_4. Since c belongs to the center of the group, it follows that every element x of C can be written as a product of a power of c with a word of length l_1, $l_1 \geqq 0$, in which first powers of c_1 and c_2 alternate and with a word of length l_2, $l_2 \geqq 0$, in which first or second powers of c_3 and c_4 alternate. If we replace the elements c_1, c_2, c_3, c_4 in this expression by their expressions

in (2), we obtain x as a product of an element of the center with a word of length l_1 in which first powers of a_1 and a_2 alternate and with a word of length l_2 in which first or second powers of b_1 and b_2 alternate. The element x therefore belongs to the center of G only if $l_1 = l_2 = 0$, that is, if x is a power of c. It follows that

$$C \cap D = \{c\} \cap D = E.$$

This shows that there exists a direct decomposition

$$G = C \times D, \tag{3}$$

which is clearly not isomorphic to (1). Both factors of (3) are indecomposable: for D this is obvious, and for C it can be proved in the same way as for A above; we have to take into account that the center of C is $\{c\}$, which follows from what has been proved in the preceding paragraph.

The existence of examples such as the one just considered naturally leads to a search for classes of groups as wide as possible for which we can assert the isomorphism of any two direct decompositions with indecomposable factors or, more generally, the existence of isomorphic refinements for arbitrary direct decompositions. For arbitrary finite groups this was proved by Remak [1], who filled a gap in a previous proof by Wedderburn [1], and again by Schmidt [1, 2]. Later Krull [1] proved the corresponding theorem for groups with an arbitrary operator domain and Schmidt [4] for groups with a principal series, also with an arbitrary operator domain. This Krull-Schmidt theorem has been the starting point of numerous investigations. Various generalizations of this theorem and also results leading in other directions can be found in papers by Kuroš [1, 13, 16], Fitting [2], Kořinek [1], Golovin [1], Livšic [2], Baer [37, 38], Azumaya [1], Kulikov [3].

It has been shown, further, that it is appropriate to develop the theory of direct decompositions within the framework of the theory of modular lattices (Dedekind structures). The extension of the Krull-Schmidt Theorem to modular lattices has been given by Ore [2]. Further results in this direction are contained in the above-mentioned papers by Kuroš [13, 16], and also in papers by Graev [3], Baer [39], and Livšic [3]. In § 47 we shall prove one theorem from the paper by Kuroš [16] from which the Krull-Schmidt Theorem follows. Aiming at the greatest possible clarity we shall use mixed lattice-theoretical and group-theoretical methods. The

extension of this theorem to the theory of lattices can be found in the paper by Livsič [3].

Central isomorphism. Two subgroups A and B of a group G are called *centrally isomorphic* if they are isomorphic and if an isomorphism φ (an operator isomorphism if the groups under consideration are operator groups) can be established between them such that for every element a of A the element ab^{-1}, where $b = a\varphi$, lies in the center of G. Note that in this case

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

Two direct decompositions of a group G are called *centrally isomorphic* if their factors can be put into a one-to-one correspondence for which the corresponding factors are centrally isomorphic. As a rule an isomorphism of direct decompositions of a group turns out to be a central isomorphism.

In the sequel we shall use the following lemma.

LEMMA. *If* $G = A_1 \times B = A_2 \times B$, *then* A_1 *and* A_2 *are centrally isomorphic.*

For A_1 and A_2 are isomorphic, because they are isomorphic, by VIII, § 17, to the factor group G/B. In this isomorphism corresponding elements a_1 and a_2 of A_2 and A_1 are contained in the same cosets of B, so that there exists an element b of B such that $a_1 = a_2 b$. The element b is permutable with every element of A_2. On the other hand, an arbitrary element of B is permutable with both a_1 and a_2, so that it must be permutable with b as well. Therefore b lies in the center of G.

This lemma allows us to apply the following device to establish a central isomorphism of direct decompositions. Suppose two direct decompositions of a group G are given:

$$G = \prod_{\alpha} A_\alpha = \prod_{\alpha} B_\alpha, \tag{4}$$

such that a one-to-one correspondence between their factors has already been established. Suppose, further, that every factor A_α of the first decomposition can be *substituted* for the corresponding factor B_α in the second decomposition; this means that for every α we have the direct decomposition

$$G = A_\alpha \times \prod_{\beta \neq \alpha} B_\beta.$$

In that case it follows from the lemma that the direct decompositions (4) are centrally isomorphic. A study of several variants of the concept of *substitu-*

tion in the theory of direct decompositions can be found in a paper by Baer [37].

§ 43. Lattices

The concept of a subgroup plays an exceptionally important rôle in every part of group theory. This is especially true of the theories of composition series and of direct products: in the definition of the fundamental concepts (direct product, principal series) and also to a certain degree in the formulation of the fundamental theorems, there occur not the elements of the group with their multiplication but rather the subgroups (or normal subgroups) with set-theoretical inclusion and with the operation of intersection and union. It therefore seems appropriate to select as objects of an independent study certain axiomatically defined formations similar to the set of all subgroups or all normal subgroups of a group. Formations of such a kind, so-called lattices (or structures), occur in many distinct branches of mathematics, and their theory has already been worked out fairly well (see the book by Birkhoff [5]). In this and in the following sections we shall investigate only certain basic definitions and elementary properties of lattices that will later be applied to the theory of direct decompositions.

A set S is called *partially ordered* if for some pairs of its elements a, b a relation $a \leqq b$ is defined (in words: "a is contained in b," "a precedes b," "a is less than or equal to b") satisfying the following conditions:

1) $a \leqq a$;

2) $a \leqq b$ and $b \leqq a$ implies $a = b$; that is, the elements a and b coincide;

3) $a \leqq b$ and $b \leqq c$ implies $a \leqq c$ (transitivity).

The symbol $a < b$ shall mean that $a \leqq b$ but $a \neq b$. The symbols $a \geqq b$ ("a contains b," "a follows b," "a is greater than or equal to b") and $a > b$ are equivalent to $b \leqq a$ and $b < a$, respectively.

A partially ordered set L is called a *lattice* (or a *structure*) if it satisfies the following two conditions:

I. For every pair of elements a, b of L there exists an element $c = ab$ in L, the *product* of a and b, such that

$$c \leqq a, \; c \leqq b,$$

and if there is an element c' that also has the properties $c' \leqq a$, $c' \leqq b$, then $c' \leqq c$.

II. For every pair of elements a, b of L there exists an element $d = a + b$ in L, the the *sum* of a and b, such that

$$d \geqq a, \; d \geqq b,$$

and if there is an element d' that also has the properties $d' \geqq a$, $d' \geqq b$, then $d' \geqq d$.[1]

This definition, which is based on the set-theoretical concept of order, can be replaced by the following entirely algebraic definition.

A set L is called a *lattice* if there are two algebraic operations, multiplication and addition, defined in L which assign to every pair of elements a, b of L a product ab and a sum $a + b$, subject to the following rules: (i) these operations are commutative and associative

$$ab = ba, \qquad a + b = b + a, \tag{1}$$

$$a(bc) = (ab)c, \qquad a + (b + c) = (a + b) + c, \tag{2}$$

(ii) for every a of L they satisfy the condition

$$aa = a, \qquad a + a = a, \tag{3}$$

and (iii) they are linked by the conditions:

$$\text{if } ab = a, \text{ then } a + b = b, \text{ and vice versa.} \tag{4}$$

Let us prove the *equivalence of these two definitions*. The product and the sum introduced in the first definition are unique: if, for example, in Axiom I the rôle of the element c can also be taken by $\bar{c}$, then $c \leqq \bar{c}$, $\bar{c} \leqq c$, so that $\bar{c} = c$. We are, therefore, dealing here with algebraic operations (in the sense of § 1). Conditions (1) and (3) are obviously satisfied by these operations. We verify (2), say, for multiplication, as follows: By I,

$$a(bc) \leqq a,$$
$$a(bc) \leqq bc \leqq b,$$
$$a(bc) \leqq bc \leqq c,$$

and again by I,

$$a(bc) \leqq ab$$
$$a(bc) \leqq (ab)c.$$

[1] Other names for the two lattice operations, and other notations, are in frequent use: other names for the product are *intersection* or *meet* or *greatest lower bound* of a and b, denoted by $a \cap b$; the corresponding names for the sum are *union* or *join* or *least upper bound*, denoted by $a \cup b$. [*Trans.*]

Similarly, $(ab)c \leqq a(bc)$, so that $a(bc) = (ab)c$.

Finally we prove (4). From $ab = a$ it follows by I that $a \leqq b$, that is, $b \geqq a$, and since by 1) we also have $b \geqq b$, we see by II that $b \geqq a + b$. On the other hand, also by II, $b \leqq a + b$. Therefore, by 2), $a + b = b$. The converse is also true.

The second definition can therefore be deduced from the first. We now show that the first can be deduced from the second. If in a set L operations are defined with properties (1)-(4), then we put $a \leqq b$ if the equations $ab = a$ and $a + b = b$, which are equivalent by (4), hold for a and b. Thus a partial ordering is introduced into the set L. For it follows from (3) that $a \leqq a$. Further, if the relations $a \leqq b$ and $b \leqq a$ hold simultaneously, then $ab = a$, $ba = b$; but since by (1) $ab = ba$, we have $a = b$. Finally, if $a \leqq b$, $b \leqq c$, that is, $ab = a$, $bc = b$, then by (2)

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

so that $a \leqq c$.

We now prove Axiom I. From

$$(ab)a = a(ba) = a(ab) = (aa)b = ab$$

it follows that $ab \leqq a$. Similarly, $ab \leqq b$. If now an arbitrary element c' is taken in L satisfying the conditions $c' \leqq a$, $c' \leqq b$, that is, $c'a = c'$, $c'b = c'$, then

$$c'(ab) = (c'a)b = c'b = c',$$

so that $c' \leqq ab$. The element ab is therefore the product of a and b in the sense of Axiom I. Similarly, we show that the element $a + b$ is the sum of a and b in the sense of Axiom II.

An example of a lattice, fundamental for the theory of groups, is the set of all subgroups of a group G. *In the set of subgroups the rôle of the order relation is played by their set-theoretical inclusion, the intersection of two subgroups is their product in the sense of lattice theory, and the union of two subgroups (that is, the subgroup generated by them) is their sum.*

The set of all normal subgroups of a group also forms a lattice with respect to these operations and, more generally, so does the set of all subgroups of a given group that are admissible for a certain operator domain.

A subset L' of a lattice L is called a *sublattice* of L if it is a lattice with respect to the operations defined in L, that is, if it contains the product and the sum of any two of its elements. For example, the lattice of normal subgroups is a sublattice of the lattice of all subgroups of a given group, because

the intersection and the union of normal subgroups are themselves normal subgroups. We must emphasize that in the definition of a sublattice we have used the operations defined in the lattice and not the partial ordering: a subset of a lattice L which is a lattice with respect to the partial ordering that exists in L does not always satisfy the above definition of a sublattice.

Among the elements of a lattice L there may be one that is contained in every other element of the lattice. This element (which is unique if it exists) is denoted by the symbol 0 and is called the *null* element (or *least* element) of the lattice; obviously it satisfies

$$a \cdot 0 = 0, \qquad a + 0 = a$$

for all a of L.

The lattice L may also have an element containing every other element. This element is denoted by the symbol 1 and is called the *unit* element (or *greatest* element) of the lattice; it satisfies, for all a of L, the conditions

$$a \cdot 1 = a, \qquad a + 1 = 1.$$

In the lattice of all subgroups of a group G the rôle of the null element is played by the unit subgroup E and that of the unit element by G itself.

Two lattices L and L' are called *isomorphic* if a one-to-one correspondence can be established between their elements such that the sum and the product of any two elements of L goes over into the sum and the product of their images in L'. We can also say, by using the connection between the lattice operations and the partial order, that a lattice isomorphism is a one-to-one correspondence preserving the order relations in the two lattices.

To every group G there corresponds uniquely the lattice $L(G)$ consisting of all its subgroups. The problem naturally arises whether the group G is determined by giving the lattice $L(G)$, in other words, whether a lattice isomorphism between $L(G)$ and $L(G')$ implies a group isomorphism between G and G'. It is easy to see that in the general case the answer is in the negative: all cyclic groups of distinct prime orders have the same subgroup lattice, although they are not isomorphic. Nevertheless for certain types of groups it can be shown that if a group G of this type has a subgroup lattice $L(G)$ isomorphic to the subgroup lattice $L(G')$ of some group G', then G and G' are, in fact, necessarily isomorphic; in other words, a group G of the given type is determined by the lattice of its subgroups.

A number of theorems of this kind can be found in a paper by Baer [20]. For example, every abelian group of rank not less than 2 is determined by

its subgroup lattice. Extending this result, Petropavlovskaya [1] has proved that every non-periodic abelian group is determined by the lattice of its subsystems; here a *subsystem* of a group is a subset that is closed under multiplication. We also mention an interesting theorem of Sadovskiĭ [3] according to which every group that is decomposable into a free product is determined by its subgroup lattice.[k]

Complete lattices. In speaking of the lattice of subgroups or the lattice of normal subgroups of a group we make use of the existence of an intersection and a union for only a *finite* number of subgroups or normal subgroups. However, intersection and union are, in fact, uniquely determined for an *arbitrary* set of subgroups or of normal subgroups. The totality of all the subgroups of a group and that of all the normal subgroups of a group or, more generally, of all the admissible subgroups for a given operator domain belong, then, to certain formations called complete lattices.

A partially ordered set L is called a *complete lattice* if for an arbitrary set of elements a_α of L (α ranges over an index set M) there exist elements c and d in L with the following properties:

1) $c \leqq a_\alpha$ for all α in M; and if there is an element c' that also satisfies the condition $c' \leqq a_\alpha$ for all α in M, then $c' \leqq c$.

2) $d \geqq a_\alpha$ for all α in M; and if there is an element d' that also satisfies the condition $d' \geqq a_\alpha$ for all α in M, then $d' \geqq d$.

The uniquely defined elements c and d are called the *product* and the *sum*, respectively, of the elements a_α, $\alpha \in M$, and are denoted by

$$c = \prod_{\alpha \in M} a_\alpha, \quad d = \sum_{\alpha \in M} a_\alpha.$$

It is clear that every complete lattice is a lattice, so that we shall use the previous notation for finite products and sums.

The definition of a complete lattice can also be given in the following form.

A set L is called a *complete lattice* if for an arbitrary subset of L a product and a sum are uniquely defined satisfying conditions (4) in the definition of a lattice and if, in addition, the following conditions are satisfied, which contain conditions (1), (2), and (3) in the definition of a lattice as special cases: If elements a_α, $\alpha \in M$, are given in L, and if the index set M is represented in an arbitrary way as the union of subsets M_β, $\beta \in N$, then

$$\prod_{\beta \in N} \left(\prod_{\alpha \in M_\beta} a_\alpha \right) = \prod_{\alpha \in M} a_\alpha, \tag{5}$$

$$\sum_{\beta \in N} \left(\sum_{\alpha \in M_\beta} a_\alpha \right) = \sum_{\alpha \in M} a_\alpha. \tag{6}$$

The first definition of a complete lattice implies the second.

For we know that condition (4) is a consequence of the first definition. It remains to prove equations (5) and (6). We shall prove one of them, say the first.

Let

$$\prod_{\alpha \in M} a_\alpha = c, \quad \prod_{\alpha \in M_\beta} a_\alpha = c_\beta, \quad \prod_{\beta \in N} c_\beta = \bar{c}.$$

Then $c \leqq a_\alpha$, $\alpha \in M_\beta$, that is, $c \leqq c_\beta$, and therefore $c \leqq \bar{c}$. On the other hand, for every $\alpha \in M$ there is a $\beta \in N$ such that $\alpha \in M_\beta$, and therefore $c_\beta \leqq a_\alpha$. Hence it follows that

$$\bar{c} \leqq c_\beta \leqq a_\alpha, \qquad \alpha \in M,$$

that is, $\bar{c} \leqq c$. We thus have arrived at the equation $c = \bar{c}$; that is, we have proved (5).

The second definition of a complete lattice implies the first.

For, as we know, it follows from the second definition that L is a lattice and that $a \leqq b$ if and only if $ab = a$ and therefore $a + b = b$. Let a_α, $\alpha \in M$, be an arbitrary set of elements of L, and let

$$\prod_{\alpha \in M} a_\alpha = c.$$

Then, by (5), we have for an arbitrary α_0 of M

$$a_{\alpha_0} c = a_{\alpha_0} \cdot \prod_{\alpha \in M} a_\alpha = \prod_{\alpha \in M} a_\alpha = c,$$

that is, $c \leqq a_\alpha$ for all α in M. On the other hand, if an element c' has the property that $c' \leqq a_\alpha$ for all α in M, so that $c' a_\alpha = c'$, then again by (5)

$$c' c = c' \prod_{\alpha \in M} a_\alpha = \prod_{\sigma \in M} (c' a_\alpha) = \prod_{\alpha \in M} c' = c',$$

and hence $c' \leqq c$. The analogous result can be obtained for the sum of the elements a_α, $\alpha \in M$.

Every complete lattice has a null and a unit element.

They are the product and the sum, respectively, of all the elements of the lattice.

§ 44. Modular and complete modular lattices

The link between the lattice operations of multiplication and addition that is expressed by Axiom (4) of the definition is a very weak one. In many cases it is expedient to impose further restrictions to make this link closer. The most obvious restriction would, of course, be the distributive law

$$(a + b)c = ac + bc.$$

Lattices in which this law holds for any three elements are called *distributive lattices* and they arise in a natural way in many branches of mathematics. For the theory of groups, however, the restriction to distributive lattices would be unnecessarily strong. For as Ore [6] has shown (see also § 50 of the first edition of this book) a group has a distributive lattice of subgroups if and only if it is either cyclic or the union of an ascending sequence of cyclic groups.

Of considerable interest for the theory of groups are the *modular lattices* (or *Dedekind structures*), which form a much wider class than that of the distributive lattices. A modular lattice differs from a distributive lattice in that the distributive law

$$(a + b)c = ac + bc$$

is postulated only under the condition that one of the summands in the parenthesis, say a, is contained in c, so that $ac = a$. In other words, a lattice L is called *modular* if it satisfies the condition

(D) If $a \leqq c$, then $(a + b)c = a + bc$,

The definition of a modular lattice can be put into many other equivalent forms. The following definition is often convenient: *A lattice L is modular if and only if the following condition holds*

(D′) If a, b, c, are elements of L with $a \leqq b$, and if

$$ac = bc \quad \text{and} \quad a + c = b + c,$$

then $a = b$.

Let us prove the *equivalence of conditions* (D) *and* (D′). Suppose that (D) is satisfied and that a, b, c are elements of L with $a \leqq b$, $ac = bc$, $a + c = b + c$. Then

$$(a + c)b = (b + c)b = b.$$

On the other hand, we have by (D)

$$(a+c)b=a+cb=a+ac=a,$$

and hence $a=b$.

Suppose now that (D′) is satisfied and that a, b, c, are elements of L with $a\leqq c$. We introduce the notation:

$$\bar{a}=a+bc,\ \bar{b}=(a+b)c,\ \bar{c}=b.$$

Since $a+bc\leqq a+b$ and $a+bc\leqq c$, we have $\bar{a}\leqq\bar{b}$. Further, from $a+bc\leqq c$ it follows that $(a+bc)b\leqq bc$, and since $a+bc\geqq bc$, $b\geqq bc$, we have $(a+bc)b\geqq bc$ and $\bar{a}\bar{c}=bc$. However, in view of $a+b\geqq b$ we have

$$\bar{b}\bar{c}=(a+b)cb=bc,$$

that is, $\bar{a}\bar{c}=\bar{b}\bar{c}$. Because of $bc\leqq b$ we have, finally,

$$\bar{a}+\bar{c}=a+bc+b=a+b.$$

From $(a+b)c\geqq a$ it now follows that

$$(a+b)c+b\geqq a+b,$$

and since $(a+b)c\leqq a+b$, $b\leqq a+b$, we have $(a+b)c+b\leqq a+b$, that is, $\bar{b}+\bar{c}=a+b$, and hence $\bar{a}+\bar{c}=\bar{b}+\bar{c}$. Condition (D′) for the elements $\bar{a}$, $\bar{b}$, $\bar{c}$ now gives $\bar{a}=\bar{b}$, that is, $a+bc=(a+b)c$.

The significance of modular lattices for the theory of groups is based on the following theorem.

The lattice of all normal subgroups of an arbitrary group is modular.

For the proof we use condition (D′). Let A, B, C be normal subgroups of a group G and let $A\subseteq B$, $A\cap C=B\cap C$, $\{A, C\}=\{B, C\}$. Since $B\subseteq\{A, C\}$, every element b of B has the form $b=ac$, where $a\in A$, $c\in C$. Hence $c=a^{-1}b$, that is, $c\in B$, and so $c\in(B\cap C)=(A\cap C)$, that is, $c\in A$. It follows that $b\in A$, that is, $B=A$.

Since every sublattice of a modular lattice is obviously modular, it follows from the theorem just proved that the lattice of admissible subgroups of a group G, for an arbitrary operator domain containing all the inner automorphisms, is also modular. The lattice of all subgroups of a group is, in general, not modular: the reader can easily verify that the subgroup lattice of the alternating group of degree 4 provides a counter-example. However, there do exist groups with a modular subgroup lattice, although not all the subgroups of the group are normal—for example, the symmetric group of

degree 3. Groups with a modular subgroup lattice are studied in papers by Iwasawa [1, 3], Jones [1] and Zappa [3].[1]

In the following, we shall use yet another form of the definition of a modular lattice.

(D″) If

$$x_1,\ x_2,\ \ldots,\ x_n,\quad y_1,\ y_2,\ \ldots,\ y_n,\quad n \geqq 1$$

are elements of a lattice L, and if

$$x_i \leqq y_j \text{ for } i \neq j,\ i, j = 1, 2, \ldots, n,$$

then

$$(x_1 + x_2 + \ldots + x_n) y_1 y_2 \ \ldots\ y_n = x_1 y_1 + x_2 y_2 + \ldots + x_n y_n.$$

For condition (D) is a special case of (D″): putting $n = 2$, $y_1 = x_1 + x_2$ in (D″), we get

$$(x_1 + x_2) y_2 = x_1 + x_2 y_2 \quad \text{for } x_1 \leqq y_2.$$

Conversely, if (D) holds and if $x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n$ are subject to the conditions $x_i \leqq y_j$ for $i \neq j$, then applying (D) several times we obtain

$$\begin{aligned}(x_1 + x_2 + \ldots + x_n) y_1 y_2 \ \ldots\ y_n &= \\ = (x_1 y_1 + x_2 + \ldots + x_n) y_2 \ \ldots\ y_n &= \\ = (x_1 y_1 + x_2 y_2 + x_3 + \ldots + x_n) y_3 \ \ldots\ y_n &= \ldots \\ \ldots &= x_1 y_1 + x_2 y_2 + \ldots + x_n y_n.\end{aligned}$$

Normal and principal series. Let L be a lattice with a null and a unit element. An ordered finite system of elements

$$0 = a_0 < a_1 < a_2 < \ \ldots\ < a_{k-1} < a_k = 1 \tag{1}$$

is called a *normal series of* L of *length* k. A normal series

$$0 = b_0 < b_1 < b_2 < \ \ldots\ < b_{l-1} < b_l = 1 \tag{2}$$

is called a *refinement* of (1) if every a_i of (1) is equal to some b_j of (2).

For modular lattices the following theorem holds.

Any two normal series of a modular lattice have refinements of equal length.

For let (1) and (2) be arbitrary normal series of a modular lattice L.

We put

$$a_{ij} = a_i + a_{i+1}b_j, \quad i = 0, 1, \ldots, k-1, \quad j = 0, 1, \ldots, l;$$

$$b_{ji} = b_j + b_{j+1}a_i, \quad j = 0, 1, \ldots, l-1, \quad i = 0, 1, \ldots, k.$$

Since

$$a_{i0} = a_i, \quad a_{il} = a_{i+1}$$

and

$$a_{ij} \leqq a_{i,\,j+1}, \; j = 0, 1, \ldots, l-1,$$

the elements a_{ij} form a normal series, possibly with repetitions, which is a refinement of (1). Similarly, the elements b_{ji} form a refinement of (2). These two new series have the same length kl; it therefore remains to show that they have the same number of repetitions.

Suppose, then, that

$$a_{ij} = a_{i,\,j+1}. \tag{3}$$

By applying in succession the definition of $a_{i,\,j+1}$, the equation (3), the inequality $a_{ij} \leqq a_{i+1}$, the definition of a_{ij}, and finally, condition (D) together with the inequality $a_{i+1}b_j < b_{j+1}$, we obtain the following chain of equations:

$$a_{i+1}b_{j+1} = a_{i,\,j+1}(a_{i+1}b_{j+1}) = a_{ij}(a_{i+1}b_{j+1}) =$$
$$= a_{ij}b_{j+1} = (a_i + a_{i+1}b_j)\,b_{j+1} = a_ib_{j+1} + a_{i+1}b_j.$$

This result, together with the definitions of b_{ji} and $b_{j,\,i+1}$ and the obvious inequality $a_{i+1}b_j \leqq b_j$ leads to the equations

$$b_{ji} = b_j + b_{j+1}a_i = b_j + b_{j+1}a_i + a_{i+1}b_j = b_j + a_{i+1}b_{j+1} = b_{j,\,i+1}.$$

Thus we have shown that the repetitions in the refinements of the normal series (1) and (2) which we have constructed are in one-to-one correspondence, so that they can be omitted simultaneously. This completes the proof of the theorem.

A *principal series* of a lattice is a normal series that cannot be refined without repetitions. Just as in § 16, we deduce from the theorem the following results.

If a modular lattice has principal series, than any two of its principal series are of equal length.

If a modular lattice has principal series, then every normal series can be refined to a principal series.

Hence it follows that *every sublattice of a modular lattice with principal series itself has principal series.*

Finally, *a modular lattice has principal series if and only if all of its ascending and descending chains of elements break off.*

The definition of a modular lattice (condition (D')) shows that every non-modular lattice contains a sublattice consisting of five elements with two principal series of different length, namely two and three. We can therefore characterize modular lattices in a new way:

A lattice is modular if and only if in every sublattice having principal series all principal series have the same length.

The theorem on normal series of a lattice that we have proved above could be sharpened so that the whole group-theoretical theorem on the isomorphism of principal series follows from it (see Ore [1], and also § 51 of the first edition of this book). A number of investigations are concerned with the problem of extending the Jordan-Hölder Theorem on composition series of groups to the theory of (not necessarily modular) lattices. We mention the relevant papers by Ore [5], Kuroš [1], and also a group of papers by Uzkov [1], Kořinek [4], and Livšic [1].

Complete modular lattices. The concept of a modular lattice can also be used when complete lattices are investigated. For the development of the theory of direct decompositions it is convenient, however, to impose on a complete lattice the following somewhat stronger restriction (see Kuroš [13]): A complete lattice L is called *complete modular* if for arbitrary systems of elements x_α and y_α (α ranges over an index set M) satisfying the conditions

$$x_\alpha \leqq y_\beta \text{ for } \alpha \neq \beta,\ \alpha, \beta \in M$$

the following equation holds

$$(\overline{\mathrm{D}}) \qquad \Big(\sum_{\alpha \in M} x_\alpha\Big) \cdot \prod_{\alpha \in M} y_\alpha = \sum_{\alpha \in M} x_\alpha y_\alpha.$$

Every complete modular lattice is modular, since (D'') follows from the definition of complete modular lattices. The converse, however, does not hold: there exist complete lattices that are modular, and even distributive, but not complete modular in the above sense.

The value of this class of lattices for the theory of groups arises from the following theorem.

The lattice of admissible normal subgroups of a group with an arbitrary operator domain is complete modular.

For let X_α and Y_α (α ranges over an index set M) be systems of normal subgroups of a group G, and let

$$X_\alpha \subseteqq Y_\beta \text{ for } \alpha \neq \beta,\ \alpha, \beta \in M. \tag{4}$$

If an element lies in the product of all the X_α, then it can be written in the form

$$a = x_{\alpha_1} x_{\alpha_2} \dots x_{\alpha_n}, \quad n \geqq 1, \quad x_{\alpha_i} \in X_{\alpha_i}, \tag{5}$$

where all the subscripts $\alpha_1, \alpha_2, \dots, \alpha_n$ are distinct. If a is also contained in the intersection of all the Y_α, then it occurs, in particular, in Y_{α_i}. All the factors of the product (5) except x_{α_i} also occur in Y_{α_i}, by (4), so that $x_{\alpha_i} \in Y_{\alpha_i}$, that is, $x_{\alpha_i} \in (X_{\alpha_i} \cap Y_{\alpha_i})$. Thus we have proved that a is contained in the product of all intersections $X_\alpha \cap Y_\alpha$, in other words, that the left-hand side of the equation (D) is contained in the right-hand side. The opposite inclusion, however, holds in an arbitrary complete lattice because of the conditions $x_\alpha \leqq y_\beta$ for $\alpha \neq \beta$.

§ 45. Direct sums in complete modular lattices

One of the definitions of a direct decomposition of a group, which we have studied in § 17, uses only products and intersections of normal subgroups. This enables us to carry over the concept of a direct product to arbitrary complete modular lattices.

Let an element a of a complete modular lattice L be the sum of elements a_α, where α ranges over an index set M,

$$a = \sum_{\alpha \in M} a_\alpha.$$

We introduce the notation

$$\bar{a}_\alpha = \sum_{\beta \in M,\ \beta \neq \alpha} a_\beta.$$

The element a is the *direct sum* of the elements a_α, $\alpha \in M$, if we have for every α of M

$$a_\alpha \bar{a}_\alpha = 0.$$

To express the decomposition of a into a direct sum we shall use the following symbolism:

$$a = \dot{\sum_{\alpha \in M}} a_\alpha$$

or, in the case of a finite number of summands,

$$a = a_1 \dot{+} a_2 \dot{+} \ldots \dot{+} a_n.$$

The element $\overline{a}_\alpha$ is called the *complement* of a_α in the direct decomposition.

It is clear that *direct decompositions of a group are equivalent to direct decompositions of the unit element of the lattice of normal subgroups of the group.*

Later on we shall make use of the following properties of direct sums in complete modular lattices.

I. *If*

$$a = \dot{\sum_{\alpha}} a_\alpha \tag{1}$$

and if all or some of the direct summands are themselves decomposed into direct sums

$$a_\alpha = \dot{\sum_{\beta}} a_{\alpha\beta}, \tag{2}$$

then

$$a = \dot{\sum_{\alpha,\beta}} a_{\alpha\beta}.$$

For a is the sum of all elements $a_{\alpha\beta}$ (compare with the second definition of a complete lattice in § 43). On the other hand, when we fix the subscripts α and β and use, successively, the inequality $a_{\alpha\beta} \leqq a_\alpha$, the modular nature of the lattice, and the fact that the decompositions (1) and (2) are direct, then we obtain

$$a_{\alpha\beta}\left(\sum_{\gamma \neq \alpha} a_\gamma + \sum_{\delta \neq \beta} a_{\alpha\delta}\right) = a_{\alpha\beta} a_\alpha \left(\sum_{\gamma \neq \alpha} a_\gamma + \sum_{\delta \neq \beta} a_{\alpha\delta}\right) =$$

$$= a_{\alpha\beta}\left(a_\alpha \sum_{\gamma \neq \alpha} a_\gamma + \sum_{\delta \neq \beta} a_{\alpha\delta}\right) = a_{\alpha\beta} \sum_{\delta \neq \beta} a_{\alpha\delta} = 0.$$

II. *If*

$$a = \dot{\sum_{\alpha \in M}} a_\alpha,$$

and if N is a proper subset of M and

$$b = \sum_{\alpha \in N} a_\alpha, \qquad c = \sum_{\alpha \in M-N} a_\alpha,$$

then $bc = 0$.

For by using the inequality $a_\alpha \leqq \bar{a}_\beta$ for $\alpha \neq \beta$ and then the definition of a complete modular lattice (that is, equation $(\overline{D})$), we obtain

$$bc = \sum_{\alpha \in N} a_\alpha \cdot \sum_{\alpha \in M-N} a_\alpha \leqq \sum_{\alpha \in N} a_\alpha \cdot \prod_{\alpha \in N} \bar{a}_\alpha = \sum_{\alpha \in N} a_\alpha \bar{a}_\alpha = 0.$$

III. *If*

$$a = \dot{\sum_{\alpha \in M}} a_\alpha$$

and if M is split into disjoint subsets M_β and

$$\sum_{\alpha \in M_\beta} a_\alpha = b_\beta,$$

then

$$a = \dot{\sum} b_\beta.$$

For a is the sum of the elements b_β, by the definition of a complete lattice. Moreover, by property II we obtain

$$b_\beta \cdot \sum_{\gamma \neq \beta} b_\gamma = \sum_{\alpha \in M_\beta} a_\alpha \cdot \sum_{\alpha \in M - M_\beta} a_\alpha = 0.$$

IV. *If*

$$a = \dot{\sum}_\iota$$

and if for every α an element c_α is chosen with

$$0 \leqq c_\alpha \leqq a_\alpha,$$

then the sum c of all the elements c_α is direct. This sum differs from a if at least one c_α differs from the corresponding a_α.

For

$$c_\alpha \cdot \sum_{\beta \neq \alpha} c_\beta \leqq a_\alpha \cdot \sum_{\beta \neq \alpha} a_\beta = 0.$$

If $c = a$, then we use the fact that the lattice is modular and obtain for every β:

$$a_\beta = a_\beta a = a_\beta \sum_\alpha c_\alpha = c_\beta + a_\beta \sum_{\alpha \neq \beta} c_\alpha \leqq c_\beta + a_\beta \sum_{\alpha \neq \beta} a_\alpha = c_\beta.$$

V. *If*

$$a = a_1 \dot{+} a_2$$

and

$$a_1 \leqq b \leqq a,$$

then

$$b = a_1 \dot{+} ba_2.$$

For by the use of (D) we obtain

$$b = ba = b(a_1 + a_2) = a_1 + ba_2.$$

But

$$a_1 \cdot ba_2 \leqq a_1 a_2 = 0.$$

Components. Let

$$1 = \dot{\sum_{\alpha \in M}} a_\alpha \tag{3}$$

be a decomposition of the unit element in a complete modular lattice L. If b is an arbitrary element of the lattice, then we call the element

$$b\varphi_\alpha = a_\alpha(b + \overline{a}_\alpha) \tag{4}$$

the *component* of b in the direct summand a_α of (3), where a_α, as above, is the supplement of a_α in (3).

If a direct decomposition of a group G is given,

$$G = \dot{\prod_\alpha} A_\alpha, \tag{5}$$

and if B is a normal subgroup of G, then $B\varphi_\alpha$ *coincides with the component of* B *in the direct factor* A_α *of* (5) in the sense of § 17.

For an element b of B has a representation

$$b = a_\alpha \overline{a}_\alpha, \qquad a_\alpha \subset A_\alpha, \qquad \overline{a}_\alpha \subset \overline{A}_\alpha,$$

and hence

$$a_\alpha = b\overline{a}_\alpha^{-1},$$

that is, the component a_α of b lies in A_α and in $B\overline{A}_\alpha$.

Conversely, if x is an arbitrary element of $A_\alpha \cap B\overline{A}_\alpha$, then it has a representation of the form

$$x = b\overline{a}_\alpha$$

and is therefore the component of b in A_α.

The mapping of G into itself that associates every element with its component in A_α is obviously an endomorphism of G (an operator endomorphism if G is a group with operators). These endomorphisms, for all α, are called the *endomorphisms of the direct decomposition of G under consideration.*[1] With this in view we can also call the mappings φ_α, $\alpha \in M$, of the lattice L in the general case the *endomorphisms of the direct decomposition* (3). These mappings are monotonic: if $b \leqq c$, then $b\varphi_\alpha \leqq c\varphi_\alpha$.

The direct decomposition (3) implies

$$1 = a_\alpha \dot{+} \bar{a}_\alpha$$

The component of b in the direct summand $\bar{a}_\alpha$ of this decomposition is

$$b\bar{\varphi}_\alpha = \bar{a}_\alpha(b + a_\alpha).$$

The mapping $\bar{\varphi}_\alpha$ is called the *complement* of the endomorphism φ_α in the direct decomposition (3).

We mention some properties of the mappings φ_α. From (4) there follows immediately:

VI. *For every b in L we have*

$$b\varphi_\alpha \leqq a_\alpha.$$

If $b \geqq a_\alpha$, then

$$b\varphi_\alpha = a_\alpha.$$

VII. *If $b \leqq a_\alpha$, then*

$$b\varphi_\alpha = b.$$

For we obtain from (D):

$$b\varphi_\alpha = a_\alpha(b + \bar{a}_\alpha) = b + a_\alpha\bar{a}_\alpha = b.$$

VIII. $b\varphi_\alpha = 0$ *if and only if* $b \leqq \bar{a}_\alpha$.

For let $b\varphi_\alpha = 0$. Since $b + \bar{a}_\alpha \geqq \bar{a}_\alpha$, we have by V

$$b + \bar{a}_\alpha = (b + \bar{a}_\alpha)\, a_\alpha + \bar{a}_\alpha, \tag{6}$$

and hence by (D)

$$0 = b\varphi_\alpha = a_\alpha(b + \bar{a}_\alpha) = a_\alpha[(b + \bar{a}_\alpha)\, a_\alpha + \bar{a}_\alpha] =$$
$$= (b + \bar{a}_\alpha)\, a_\alpha + a_\alpha\bar{a}_\alpha = (b + \bar{a}_\alpha)\, a_\alpha.$$

[1] Another, more suggestive, name is *projection endomorphisms* of the direct decomposition of G. [*Trans.*]

Equation (6) now turns into

$$b + \bar{a}_\alpha = \bar{a}_\alpha,$$

so that $b \leqq \bar{a}_\alpha$. The converse follows from (4).

From VII and VIII we deduce

IX. *For all b of L and all indices α,*

$$b\bar{\varphi}_\alpha \varphi_\alpha = b\varphi_\alpha \bar{\varphi}_\alpha = 0,$$

where $\bar{\varphi}_\alpha$ is the complement of φ_α in (3).

X. *Every element b is contained in the sum of all its components in all summands a_α of* (3).

For since $a_\alpha \leqq b + \bar{a}_\beta$ for $\alpha \neq \beta$, we obtain by the use of $(\bar{\mathrm{D}})$ and (3)

$$\sum_\alpha b\varphi_\alpha = \sum_\alpha a_\alpha (b + \bar{a}_\alpha) = \sum_\alpha a_\alpha \cdot \prod_\alpha (b + \bar{a}_\alpha) = \prod_\alpha (b + \bar{a}_\alpha) \geqq b.$$

XI. *The component of a sum is equal to the sum of the components, that is to say, if*

$$b = \sum_\beta b_\beta,$$

then

$$b\varphi_\alpha = \sum_\beta b_\beta \varphi_\alpha.$$

For $b_\beta \leqq b$ implies $b_\beta \varphi_\alpha \leqq b\varphi_\alpha$, and therefore

$$\sum_\beta b_\beta \varphi_\alpha \leqq b\varphi_\alpha.$$

But by X and VI

$$b = \sum_\beta b_\beta \leqq \sum_\beta b_\beta \varphi_\alpha + \bar{a}_\alpha,$$

and so, by applying (4), (D), and VI, we obtain

$$b\varphi_\alpha \leqq \left(\sum_\beta b_\beta \varphi_\alpha + \bar{a}_\alpha\right)\varphi_\alpha = a_\alpha \left(\sum_\beta b_\beta \varphi_\alpha + \bar{a}_\alpha\right) = \sum_\beta b_\beta \varphi_\alpha + a_\alpha \bar{a}_\alpha = \sum_\beta b_\beta \varphi_\alpha.$$

XII. *Let N be a subset of the index set M in* (3) *and*

$$a = \sum_{\alpha \in N} a_\alpha, \qquad \bar{a} = \sum_{\alpha \in M - N} a_\alpha,$$

so that, by III, *we have*

$$1 = a \dot{+} \bar{a}. \tag{7}$$

If b is an element of L and $b\psi$ is its component in the summand a of (7), *then*

$$b\psi \leqq \sum_{\alpha \in N} b\varphi_\alpha.$$

For since

$$b + \bar{a} \leqq b + \bar{a}_\alpha$$

for all α in N, and therefore

$$b + \bar{a} \leqq \prod_{\alpha \in N} (b + \bar{a}_\alpha),$$

we have, by $(\bar{\mathrm{D}})$,

$$b\psi = a(b + \bar{a}) \leqq \sum_{\alpha \in N} a_\alpha \cdot \prod_{\alpha \in N} (b + \bar{a}_\alpha) = \sum_{\alpha \in N} a_\alpha (b + \bar{a}_\alpha) = \sum_{\alpha \in N} b\varphi_\alpha.$$

XIII. *If $b\varphi_\alpha = c$, then for every element c', $c' \leqq c$, there exists an element b', $b' \leqq b$ such that $b'\varphi_\alpha = c'$.*

For we can put

$$b' = b(c' + \bar{a}_\alpha).$$

Then the condition $b' \leqq b$ is satisfied. But by applying (D), (4), and the equation $c\bar{a}_\alpha = 0$ (which follows from $c = b\varphi_\alpha \leqq a_\alpha$), we obtain

$$\begin{aligned} b'\varphi_\alpha &= a_\alpha(b' + \bar{a}_\alpha) = a_\alpha[b(c' + \bar{a}_\alpha) + \bar{a}_\alpha] = \\ &= a_\alpha[(b + \bar{a}_\alpha)(c' + \bar{a}_\alpha)] = c(c' + \bar{a}_\alpha) = c' + c\bar{a}_\alpha = c'. \end{aligned}$$

Properties I-XIII of direct decompositions and their endomorphisms will be used in the rest of this chapter and will be denoted simply by the roman numerals I-XIII.

Existence of a common refinement. Suppose that in a complete modular lattice L two direct decompositions of the unit element are given:

$$1 = \sum_\alpha{}^{\cdot} a_\alpha = \sum_\beta{}^{\cdot} b_\beta. \tag{8}$$

We denote the endomorphisms of these decompositions by φ_α and θ_β, respectively, and write $\bar{\varphi}_\alpha$ for the complement of φ_α.

THEOREM (Kuroš [13]). *The direct decompositions* (8) *have a common*

refinement if and only if for all α *and* β *the mapping* $\bar{\varphi}_\alpha\theta_\beta\varphi_\alpha$ *carries the unit element (and hence every element of the lattice) into the null element, that is,*

$$1\bar{\varphi}_\alpha\theta_\beta\varphi_\alpha = 0\,. \tag{9}$$

Proof. Suppose the decompositions (8) have a common refinement

$$1 = \dot{\sum_\gamma} c_\gamma.$$

Every c_γ is contained in some product $a_\alpha b_\beta$, so that the sum of all the products (for all α and β) is the unit element. Moreover, this sum is direct:

$$\sum_{\alpha,\beta} a_\alpha b_\beta = \sum_\alpha \left(\sum_\beta a_\alpha b_\beta\right),$$

but every sum on the right-hand side is direct, by IV, so that it remains to use I. Thus,

$$1 = \dot{\sum_{\alpha,\beta}} a_\alpha b_\beta. \tag{10}$$

Hence

$$a_\alpha = \dot{\sum_\beta} a_\alpha b_\beta, \qquad b_\beta = \dot{\sum_\alpha} a_\alpha b_\beta. \tag{11}$$

Let us now find the element $1\bar{\varphi}_\alpha\theta_\beta\varphi_\alpha$. By VI and (11)

$$1\bar{\varphi}_\alpha = \bar{a}_\alpha = \sum_{\gamma\neq\alpha}\sum_\beta a_\gamma b_\beta.$$

Hence, applying XI, VII, and VIII, we obtain

$$1\bar{\varphi}_\alpha\theta_\beta = \bar{a}_\alpha\theta_\beta = \sum_{\gamma\neq\alpha} a_\gamma b_\beta \leqq \bar{a}_\alpha,$$

and therefore (9) holds, again by VIII.

Suppose now, conversely, that (9) is satisfied for all α and β. By (8), VI, and IX,

$$a_\alpha = \sum_\beta b_\beta\varphi_\alpha.$$

Let us show, by using (9), that this sum is direct. By XI and (D)

$$b_\beta\varphi_\alpha \cdot \sum_{\gamma\neq\beta} b_\gamma\varphi_\alpha = b_\beta\varphi_\alpha \cdot \bar{b}_\beta\varphi_\alpha = a_\alpha(b_\beta + \bar{a}_\alpha)\cdot a_\alpha(\bar{b}_\beta + \bar{a}_\alpha) =$$

$$= a_\alpha(b_\beta + \bar{a}_\alpha)(\bar{b}_\beta + \bar{a}_\alpha) = a_\alpha[b_\beta(\bar{b}_\beta + \bar{a}_\alpha) + \bar{a}_\alpha] = \bar{a}_\alpha\theta_\beta\varphi_\alpha = 1\bar{\varphi}_\alpha\theta_\beta\varphi_\alpha = 0.$$

Thus

$$a_\alpha = \dot{\sum_\beta} b_\beta \varphi_\alpha,$$

so that, by I, we arrive at the direct decomposition

$$1 = \dot{\sum_{\alpha,\beta}} b_\beta \varphi_\alpha, \tag{12}$$

which is a refinement of the first decomposition (8).

Re-writing (12) in the form

$$1 = \dot{\sum_\beta} (\dot{\sum_\alpha} b_\beta \varphi_\alpha)$$

and taking into account that by X,

$$b_\beta \leqq \dot{\sum_\alpha} b_\beta \varphi_\alpha,$$

we find from (8) and IV that for all β

$$b_\beta = \dot{\sum_\alpha} b_\beta \varphi_\alpha.$$

Thus (12) is also a refinement of the second decomposition (8). This completes the proof of the theorem.

Let us apply the theorem to groups. Suppose that two direct decompositions of a group G with an arbitrary operator domain are given:

$$G = \prod_\alpha A_\alpha = \prod_\beta B_\beta. \tag{13}$$

We denote by φ_α, θ_β, and $\overline{\varphi}_\alpha$, the mappings that carry every element of G into its component in A_α, B_β, and $\overline{A}_\alpha = \prod_{\gamma \neq \alpha} A_\gamma$, respectively.

Therefore the mapping $\overline{\varphi}_\alpha \theta_\beta \varphi_\alpha$ is also an operator endomorphism. We shall show that *it carries every element of G into the center of G and therefore maps the whole of G onto an admissible subgroup of the center.* We know from § 17 that components of permutable elements of a group are themselves permutable; therefore, *if two permutable elements are given, then a component of one is permutable with the other.* Let g be an arbitrary element of G. Then $g\overline{\varphi}_\alpha$ lies in $\bar{A}_\alpha$ and is therefore permutable with every element of A_α. It follows that its component in a direct factor B_β of the

second decomposition (13), that is, the element $g\overline{\varphi_\alpha}\theta_\beta$, is also permutable with every element of A_α. Finally, this is also true for $g\overline{\varphi_\alpha}\theta_\beta\varphi_\alpha$, and since this element lies in A_α, it must belong to the center of A_α, that is, to the center of G.

The *admissible center* of an operator group G is defined as the union of all admissible subgroups of the center. We know from § 14 that the center of a group is not always admissible, so that the admissible center may turn out to be smaller than the center itself. From the above theorem we obtain the following result (Fitting [3], Kuroš [5]).

Suppose that a group G with an arbitrary operator domain is such that the mapping onto the unit element is the only operator homomorphism of G (or, what comes to the same thing, of the factor group of its derived group) into its admissible center.[1] *Then any two direct decompositions of G have a common refinement.*

In particular, *any two direct decompositions of a group have a common refinement if it is a group without center (or, in the case of an operator group, at least without admissible center) or if it coincides with its derived group.*

§ 46. Further lemmas

Suppose that in a complete modular lattice L two direct decompositions of the unit element into two summands are given:

$$1 = a_1 \dot{+} a_2 = b_1 \dot{+} b_2. \tag{1}$$

We denote the endomorphisms of these decompositions by φ_1, φ_2 and θ_1, θ_2, respectively, and shall prove a number of lemmas that will be used in the following section for the proof of the fundamental theorem.

LEMMA 1. *For all x of L,*

$$x\theta_1\varphi_1\theta_2 = x\theta_1\varphi_2\theta_2.$$

The equations obtained by interchanging the rôles of θ_1 and θ_2 and of θ and φ, also hold.

For we have by $x\theta_1 \leqq b_1$ and (D)

[1] We shall come across groups with these properties in § 47. We call them F-groups.

$$x\theta_1\varphi_1\theta_2 = b_2[a_1(x\theta_1 + a_2) + b_1] = b_2[x\theta_1 + a_1(x\theta_1 + a_2) + b_1] =$$
$$= b_2[(x\theta_1 + a_1)(x\theta_1 + a_2) + b_1].$$

But in this expression a_1 and a_2 occur symmetrically.

LEMMA 2. *If* $x \leqq a_1$ *then*

$$x\theta_1\varphi_1\theta_2\varphi_1 = x\theta_2\varphi_1\theta_1\varphi_1;$$

in other words, as far as elements contained in a_1 *are concerned,* $\theta_1\varphi_1$ *and* $\theta_2\varphi_1$ *are permutable.*

For by applying Lemma 1 several times, and by the equation $x = x\varphi_1$, which follows from VII, we obtain

$$x\theta_1\varphi_1\theta_2\varphi_1 = x\varphi_1\theta_1\varphi_1\theta_2\varphi_1 = x\varphi_1\theta_1\varphi_2\theta_2\varphi_1 =$$
$$= x\varphi_1\theta_2\varphi_2\theta_1\varphi_1 = x\varphi_1\theta_2\varphi_1\theta_1\varphi_1 = x\theta_2\varphi_1\theta_1\varphi_1.$$

The elements $n_{1j}^{(k)}$ $(j = 1, 2)$ **and** $n_1^{(k)}$, $k = 1, 2, \ldots$ We consider the direct summand a_1 of the first decomposition (1). Let $n_{11}^{(k)}$, $k = 1, 2, \ldots$, be the sum of all the elements x contained in a_1 for which $x(\theta_2\varphi_1)^k = 0$; here $(\theta_2\varphi_1)^k$ denotes the k-th power of the mapping $\theta_2\varphi_1$. Similarly, we denote by $n_{12}^{(k)}$, $k = 1, 2, \ldots$, the sum of all the elements x, $x \leqq a_1$, for which $x(\theta_1\varphi_1)^k = 0$. By XI

$$n_{11}^{(k)}(\theta_2\varphi_1)^k = 0, \quad n_{12}^{(k)}(\theta_1\varphi_1)^k = 0. \tag{2}$$

Clearly,

$$n_{1j}^{(1)} \leqq n_{1j}^{(2)} \leqq \ldots \leqq n_{1j}^{(k)} \leqq \ldots, \quad j = 1, 2. \tag{3}$$

Further, let $n_1^{(k)}$ be the sum of all the elements x, $x \leqq a_1$, for which $x(\theta_1\varphi_1\theta_2\varphi_1)^k = 0$. Again

$$n_1^{(k)}(\theta_1\varphi_1\theta_2\varphi_1)^k = 0, \tag{4}$$

$$n_1^{(1)} \leqq n_1^{(2)} \leqq \ldots \leqq n_1^{(k)} \leqq \ldots, \tag{5}$$

LEMMA 3. $n_{1j}^{(k)} \leqq n_1^{(k)}$, $j = 1, 2$, $k = 1, 2, \ldots$.

Let $j = 1$, say. Applying Lemma 2 and the first equation (2) we obtain

$$n_{11}^{(k)}(\theta_1\varphi_1\theta_2\varphi_1)^k = n_{11}^{(k)}(\theta_2\varphi_1)^k(\theta_1\varphi_1)^k = 0(\theta_1\varphi_1)^k = 0,$$

and hence

$$n_{11}^{(k)} \leqq n_1^{(k)}.$$

LEMMA 4. *If* $x \leqq a_1$, *then for* $k = 1, 2, \ldots$ *we have the following inequality*:

$$x \leqq x(\theta_1\varphi_1)^k + x(\theta_1\varphi_1)^{k-1}(\theta_2\varphi_1) + x(\theta_1\varphi_1)^{k-2}(\theta_2\varphi_1)^2 + \ldots + x(\theta_2\varphi_1)^k. \quad (6)$$

For by X

$$x \leqq x\theta_1 + x\theta_2,$$

and therefore, by XI,

$$x = x\varphi_1 \leqq (x\theta_1 + x\theta_2)\varphi_1 = x\theta_1\varphi_1 + x\theta_2\varphi_1,$$

which proves (6) for $k = 1$. Suppose the inequality already proved for a given k. Then we replace every summand on the right-hand side of (6) by the sum of its images under the mappings $\theta_1\varphi_1$ and $\theta_2\varphi_1$; as we have seen, this can only strengthen the inequality. Now we apply Lemma 2 and combine like summands. This proves (6) for $k + 1$.

LEMMA 5. $n_1^{(k)} \leqq n_{11}^{(k)} + n_{12}^{(k)}$, $k = 1, 2, \ldots$.

By Lemma 4,

$$n_1^1 \leqq n_1^1\theta_1\varphi_1 + n_1^1\theta_2\varphi_1.$$

However, from (4) and Lemma 2 it follows that

$$(n_1^1\theta_1\varphi_1)\,\theta_2\varphi_1 = 0, \quad (n_1^{(1)}\theta_2\varphi_1)\,\theta_1\varphi_1 = 0,$$

so that

$$n_1^1\theta_1\varphi_1 \leqq n_{11}^1, \quad n_1^1\theta_2\varphi_1 \leqq n_{12}^1.$$

This proves the lemma for $k = 1$. Suppose it already proved for $k - 1$. We apply Lemma 4 to $n_1^{(k)}$ in place of x. From (4) it follows that

$$[n_1^{(k)}(\theta_1\varphi_1)^k](\theta_2\varphi_1)^k = 0,$$

that is, $n_1^{(k)}(\theta_1\varphi_1)^k \leqq n_{11}^{(k)}$, and similarly, $n_1^{(k)}(\theta_2\varphi_1)^k \leqq n_{12}^{(k)}$.

The remaining terms on the right-hand side of (6) are all mapped into the null element even under $(\theta_1\varphi_1\theta_2\varphi_1)^{k-1}$, that is, they are contained in $n_1^{(k-1)}$; therefore, by the induction hypothesis, they are in $n_{11}^{(k-1)} + n_{12}^{(k-1)}$ and finally, by (3), in $n_{11}^{(k)} + n_{12}^{(k)}$.

LEMMA 6. $n_{11}^{(k)} \cdot n_{12}^{(l)} = 0$, $k, l = 1, 2, \ldots$

Let

$$x \leqq n_{11}^{(k)} \cdot n_{12}^{(l)},$$

that is

$$x(\theta_2\varphi_1)^k = x(\theta_1\varphi_1)^l = 0.$$

If $k = l = 1$, then from $x \leqq x\theta_1\varphi_1 + x\theta_2\varphi_1$ and $x\theta_1\varphi_1 = x\theta_2\varphi_1 = 0$ it follows that $x = 0$. We now argue by induction over the sum $k + 1$. If, for example, $k > 1$, then from

$$x(\theta_2\varphi_1)(\theta_2\varphi_1)^{k-1} = 0$$

and

$$x(\theta_2\varphi_1)(\theta_1\varphi_1)^l = x(\theta_1\varphi_1)^l(\theta_2\varphi_1) = 0$$

it follows that $x(\theta_2\varphi_1) = 0$; from this and $x(\theta_1\varphi_1)^l = 0$ we deduce that $x = 0$ because $1 + l < k + l$.

From Lemmas 3, 5, and 6 we get

LEMMA 7. $n_1^{(k)} = n_{11}^{(k)} + n_{12}^{(k)}$, $k = 1, 2, \ldots$.

Let $n_{21}^{(k)}$, $n_{22}^{(k)}$, $n_2^{(k)}$ be the elements that play the same rôle for a_2 as $n_{11}^{(k)}$, $n_{12}^{(k)}$, $n_1^{(k)}$ do for a_1; also let $m_{j1}^{(k)}$, $m_{j2}^{(k)}$, $m_j^{(k)}$ $j = 1, 2$, play the corresponding rôles in the direct summand b_j in the second decomposition (1). Lemmas analogous to the above hold for all these elements.

LEMMA 8. $n_1^{(k)} + n_2^{(k)} = m_1^{(k)} + m_2^{(k)}$, $k = 1, 2, \ldots$.

For by applying Lemma 1 several times and by using the equation $m_1^{(k)}(\varphi_1\theta_1\varphi_2\theta_1)^k = 0$, we find that

$$(m_1^{(k)}\varphi_1)(\theta_1\varphi_1\theta_2\varphi_1)^k =$$

$$= (m_1^{(k)}\varphi_1)(\theta_1\varphi_2\theta_2\varphi_1)^k = (m_1^{(k)}\varphi_1)(\theta_1\varphi_2\theta_1\varphi_1)^k = m_1^{(k)}(\varphi_1\theta_1\varphi_2\theta_1)^k\varphi_1 = 0.$$

This proves that $m_1^{(k)}\varphi_1 \leqq n_1^{(k)}$, since $m_1^{(k)}\varphi_1 \leqq a_1$. Similarly, $m_1^{(k)}\varphi_2 \leqq n_2^{(k)}$. Hence, from $m_1^{(k)} \leqq m_1^{(k)}\varphi_1 + m_1^{(k)}\varphi_2$ it follows that

$$m_1^{(k)} \leqq n_1^{(k)} + n_2^{(k)}.$$

The same inequality holds for $m_2^{(k)}$ instead of $m_1^{(k)}$. But by a similar argument

$$n_i^{(k)} \leqq m_1^{(k)} + m_2^{(k)}, \quad i = 1, 2.$$

LEMMA 9. $n_{11}^{(k)}\theta_1 \leqq m_{11}^{(k)}$, $k = 1, 2, \ldots$.

For by using VII, Lemma 1 and equation (2) we find

$$n_{11}^{(k)}\theta_1(\varphi_2\theta_1)^k = n_{11}^{(k)}\varphi_1\theta_1(\varphi_2\theta_1)^k = n_{11}^{(k)}\varphi_1\theta_2(\varphi_2\theta_1)^k =$$

$$= \ldots = n_{11}^{(k)}\varphi_1(\theta_2\varphi_1)^k\theta_1 = n_{11}^{(k)}(\theta_2\varphi_1)^k\theta_1 = 0,$$

but since $n_{11}^{(k)}\theta_1 \leqq b_1$, we have $n_{11}^{(k)}\theta_1 \leqq m_{11}^{(k)}$.

LEMMA 10. $n_{11}^{(k)}(m_{12}^{(k)} + m_2^{(k)}) = 0,\ k = 1, 2, \ldots.$

Denote the left-hand side of this equation by x. Then by Lemma 9

$$x\theta_1 \leqq n_{11}^{(k)}\theta_1 \leqq m_{11}^{(k)}.$$

On the other hand, by XI and VII,

$$x\theta_1 \leqq (m_{12}^{(k)} + m_2^{(k)})\,\theta_1 = m_{12}^{(k)}\theta_1 = m_{12}^{(k)},$$

since $m_2^{(k)}\theta_1 \leqq b_2\theta_1 = 0$. So by reference to Lemma 6, we obtain

$$x\theta_1 \leqq m_{11}^{(k)} \cdot m_{12}^{(k)} = 0.$$

Hence $x\theta_1\varphi_1 = 0$, and since $x \leqq n_{11}^{(k)} \leqq a_1$, we have $x \leqq n_{12}'$. Therefore, again by Lemma 6,

$$x \leqq n_{11}^{(k)} \cdot n_{12}' = 0.$$

LEMMA 11. $m_{11}^{(k)} \leqq n_{11}^{(k)} + m_{22}^{(k)},\ k = 1, 2, \ldots.$

First of all, let $k = 1$. Since $m_{11}'\varphi_2\theta_1 = 0$, we have, by VIII, $m_{11}'\varphi_2 \leqq b_2$, and therefore, because of

$$(m_{11}'\varphi_2)\,(\varphi_1\theta_2) = m_{11}'\,(\varphi_2\varphi_1)\,\theta_2 = 0$$

(see IX), we have

$$m_{11}'\varphi_2 \leqq m_{22}'.$$

Furthermore, by Lemma 9, with the rôles of the first and second decompositions in (1) interchanged,

$$m_{11}'\varphi_1 \leqq n_{11}'.$$

Thus

$$m_{11}' \leqq m_{11}'\varphi_1 + m_{11}'\varphi_2 \leqq n_{11}' + m_{22}'.$$

Suppose the lemma already proved for $k - 1$. We know that $m_{11}^{(k)} \leqq m_{11}^{(k)}\varphi_1 + m_{11}^{(k)}\varphi_2$, and that, by Lemma 9,

$$m_{11}^{(k)}\varphi_1 \leqq n_{11}^{(k)}.$$

Furthermore

$$m_{11}^{(k)}\varphi_2 \leqq m_{11}^{(k)}\varphi_2\theta_1 + m_{11}^{(k)}\varphi_2\theta_2.$$

Since $m_{11}^{(k)}\varphi_2\theta_1 \leqq b_1$ and

$$(m_{11}^{(k)}\varphi_2\theta_1)\,(\varphi_2\theta_1)^{k-1} = m_{11}^{(k)}\,(\varphi_2\theta_1)^k = 0,$$

we have

$$m_{11}^{(k)}\varphi_2\theta_1 \leqq m_{11}^{(k-1)},$$

and so, by the induction hypothesis,

$$m_{11}^{(k)}\varphi_2\theta_1 \leqq n_{11}^{(k-1)} + m_{22}^{(k-1)} \leqq n_{11}^{(k)} + m_{22}^{(k)}.$$

Finally,

$$m_{11}^{(k)}\varphi_2\theta_2 \leqq b_2$$

and by Lemma 1,

$$(m_{11}^{(k)}\varphi_2\theta_2)(\varphi_1\theta_2)^k = m_{11}^{(k)}(\varphi_2\theta_1)(\varphi_1\theta_2)^k = \ldots =$$
$$= m_{11}^{(k)}(\varphi_2\theta_1)^k(\varphi_1\theta_2) = 0,$$

so that $m_{11}^{(k)}\varphi_2\theta_2 \leqq m_{22}^{(k)}$. This proves the lemma.

We shall say that an element c of a lattice L *has a principal series* if the sublattice L_c consisting of the elements between 0 and c,

$$0 \leqq x \leqq c$$

has a principal series.

We know that this is equivalent to the fact that all ascending and descending chains of elements in L_c break off.

We shall now make the following assumption, which will remain in force until the end of this section.

(A) *Every mapping* $\varphi_i\theta_1\varphi_i\theta_2\varphi_i$, $i = 1, 2$, *and* $\theta_j\varphi_1\theta_j\varphi_2\theta_j$, $j = 1, 2$, *carries the unit element into an element having a principal series.*

We introduce the notation

$$\varphi_1\theta_1\varphi_1\theta_2\varphi_1 = \eta.$$

LEMMA 12. *The elements* 1, 1η, $1\eta^2$, ..., $1\eta^k$, ... *form a descending sequence*

$$1 \geqq 1\eta \geqq 1\eta^2 \geqq \ldots \geqq 1\eta^k \geqq \cdots. \tag{7}$$

There exists a k_0 *such that*

$$1\eta^{k_0} = 1\eta^{k_0+1} = \ldots, \tag{8}$$

Writing

$$\bar{a}_1 = 1\eta^{k_0},$$

we deduce from $x \leqq \bar{a}_1$, $x\eta = 0$ *that* $x = 0$.

(7) follows from the monotonic character of the mapping η, and the existence of an exponent k_0 with property (8) follows from (A). Let us

prove the third statement of the lemma. Let $0 < x \leqq \bar{a}_1$ and $x\eta = 0$. Since by (8)

$$\bar{a}_1\eta = \bar{a}_1,$$

we have $\bar{a}_1 \neq 0$, because $0 < x$. By repeated application of XIII, there exists an element y, $y \leqq \bar{a}_1$, such that

$$y\eta = x.$$

Since by XI,

$$(x + y)\eta = x\eta + y\eta = y\eta = x,$$

we can assume strict inequality: $y > x$. Continuing this process, we construct in $\bar{a}_1$, and hence in 1η, an infinite ascending sequence of elements, in contradiction to (A).

LEMMA 13. $n_1^{(k_0)} = n_1^{(k_0+1)} = \ldots$.

For every natural number l we have

$$n_1^{(k_0+l)}\eta^{k_0} \leqq 1\eta^{k_0} = \bar{a}_1.$$

But

$$n_1^{(k_0+l)}\eta^{k_0+l} = (n_1^{(k_0+l)}\eta^{k_0})\,\eta^l = 0.$$

Therefore by the preceding lemma

$$n_1^{(k_0+l)}\eta^{k_0} = 0,$$

that is, $n_1^{(k_0+l)} \leqq n_1^{k_0}$. Hence the lemma follows from (5).

LEMMA 14. $n_{1j}^{(k_0)} = n_{1j}^{(k_0+1)} = \ldots$, $j = 1, 2$.

This follows from (3), Lemmas 7 and 13, and IV.

We denote the sums of the ascending sequences (5) and (3) by n_1 and n_{1j}, $j = 1, 2$, respectively. The elements that play the same rôles for a_2 will be denoted by n_2 and n_{2j}, $j = 1, 2$, and for b_i, $i = 1, 2$, by m_i and m_{ij}, $j = 1, 2$. Lemmas 13 and 14 allow us to deduce the following results from Lemmas 7 and 8:

$$n_i = n_{i1} \dot{+} n_{i2}, \qquad m_i = m_{i1} \dot{+} m_{i2}, \qquad i = 1, 2, \tag{9}$$

$$n_1 + n_2 = m_1 + m_2. \tag{10}$$

We denote the element on the left-hand (or right-hand) side of (10) by v. Since

$$n_1 n_2 \leqq a_1 a_2 = 0$$

and similarly

$$m_1 m_2 = 0,$$

we have two direct decompositions of v

$$v = n_1 \dot{+} n_2 = m_1 \dot{+} m_2. \tag{11}$$

By the use of (9) we arrive at two refinements:

$$v = n_{11} \dot{+} n_{12} \dot{+} n_{21} \dot{+} n_{22} = m_{11} \dot{+} m_{12} \dot{+} m_{21} \dot{+} m_{22}. \tag{12}$$

Let us study these new decompositions.

LEMMA 15. *In* (12) *the elements* n_{11} *and* m_{11}, *also* n_{12} *and* m_{21}, n_{21} *and* m_{12}, n_{22} *and* m_{22} *can be substituted for one another.*

For by Lemmas 13 and 14 it follows from Lemmas 10 and 11 that

$$n_{11}(m_{12} + m_2) = 0,$$

$$m_{11} \leqq n_{11} + m_{22},$$

so that, taking account of (12) and (9),

$$v = n_{11} \dot{+} m_{12} \dot{+} m_{21} \dot{+} m_{22};$$

the element n_{11} can therefore be substituted for m_{11} in the second decomposition (12). By a similar argument we also have

$$v = m_{11} \dot{+} n_{12} \dot{+} n_{21} \dot{+} n_{22}.$$

Furthermore, it is easy to verify that, for example, the elements n_{12} and m_{21} stand in the same relation to each other as n_{11} and m_{11}. Thus the lemma follows.

LEMMA 16. $n_1 \bar{a}_1 = 0$.

Since, by Lemma 13, $n_1 = n_1^{(k_0)}$, we have

$$(n_1 \bar{a}_1)\, \eta^{k_0} = 0.$$

The lemma now follows from the last statement of Lemma 12.

LEMMA 17. $\bar{a}_1(m_1 + b_2) = 0$, *and* $\bar{a}_1(m_2 + b_1) = 0$.

We use the notation

$$\bar{a}_1(m_1 + b_2) = x.$$

By Lemma 13 there exists a k_0 such that $m_1 = m_1^{(k_0)}$. Then

$$x(\theta_1\varphi_1\theta_2\varphi_1)^{k_0+1} \leqq (m_1^{(k_0)} + b_2)(\theta_1\varphi_1\theta_2\varphi_1)^{k_0+1} =$$
$$= m_1^{(k_0)}(\theta_1\varphi_1\theta_2\varphi_1)^{k_0+1} + b_2(\theta_1\varphi_1\theta_2\varphi_1)^{k_0+1}.$$

The second term on the right-hand side is the null element, because $b_2\theta_1 = 0$. Moreover, by Lemma 1 we have $m_1^{(k_0)}\theta_1 = m_1^{(k_0)}$, and by the definition of $m_1^{(k_0)}$

$$m_1^{(k_0)}(\theta_1\varphi_1\theta_2\varphi_1)^{k_0+1} = m_1^{(k_0)}(\theta_1\varphi_2\theta_1\varphi_1)^{k_0+1} =$$
$$= m_1^{(k_0)}(\varphi_2\theta_1\varphi_1\theta_1)^{k_0}\varphi_2\theta_1\varphi_1 = 0.$$

Thus, $x(\theta_1\varphi_1\theta_2\varphi_1)^{k_0+1} = 0$, and since $x \leqq a_1$, $x \leqq n_1$. On the other hand, we know that $x \leqq \bar{a}_1$. Therefore, by the preceding lemma,

$$x \leqq n_1\bar{a}_1 = 0.$$

The second part of the lemma is proved in the same way, because

$$a_1(\theta_1\varphi_1\theta_2\varphi_1)^{k_0+1} = a_1(\theta_2\varphi_1\theta_1\varphi_1)^{k_0+1}.$$

Finally, we make two further assumptions:

(B)
$$a_i = n_i + \bar{a}_i, \quad i = 1, 2,$$
$$b_j = m_j + \bar{b}_j, \quad j = 1, 2.$$

(C)
$$\bar{b}_1 \leqq \bar{a}_i + b_2, \quad \bar{b}_2 \leqq \bar{a}_i + b_1, \quad i = 1, 2,$$
$$\bar{a}_1 \leqq \bar{b}_j + a_2, \quad \bar{a}_2 \leqq \bar{b}_j + a_1, \quad j = 1, 2.$$

Assumption (B) together with Lemma 16 and the analogous lemmas for the other terms of (1) lead to the following direct decompositions:

$$a_i = n_i \dot{+} \bar{a}_i, \quad i = 1, 2,$$
$$b_j = m_j \dot{+} \bar{b}_j, \quad j = 1, 2.$$

From this and from (9) we obtain the following refinements of the original direct decompositions (1):

$$1 = n_{11} \dot{+} n_{12} \dot{+} \bar{a}_1 \dot{+} n_{21} \dot{+} n_{22} \dot{+} \bar{a}_2 =$$
$$= m_{11} \dot{+} m_{12} \dot{+} \bar{b}_1 \dot{+} m_{21} \dot{+} m_{22} \dot{+} \bar{b}_2. \quad (13)$$

LEMMA 18. *The terms in the direct decompositions* (13) *can be put into*

a one-to-one correspondence such that corresponding terms can be substituted for each other.

This has been proved in Lemma 15 for the terms that occur in the direct decompositions (12) of v. In the above general case it remains true because the decompositions (13) are refinements of the direct decompositions

$$1 = v \dotplus \bar{a}_1 \dotplus \bar{a}_2 = v \dotplus \bar{b}_1 \dotplus \bar{b}_2.$$

But (C) and Lemma 17 show that each direct summand $\bar{b}_1$, $\bar{b}_2$ of the second decomposition (13) can be substituted for every summand $\bar{a}_1$, $\bar{a}_2$ of the first decomposition, and vice versa.

§ 47. The fundamental theorem

Our aim is to prove the following theorem (Kuroš [16]).

Let G be a group with an arbitrary operator domain having the following properties: Every admissible subgroup of the admissible center of G onto which G (or the factor group of its derived group) can be mapped operator homomorphically has a principal series quâ operator group. Then any two direct decompositions of G have centrally isomorphic refinements.

To begin with, we consider direct decompositions with two factors each. In this case the assertion of the theorem follows immediately from Lemma 18 of the preceding section. We need only show that the lattice of normal subgroups of G satisfies assumptions (A), (B), and (C).

Suppose, then, that two decompositions are given

$$G = A_1 \times A_2 = B_1 \times B_2. \tag{1}$$

We denote the endomorphisms of these decompositions by φ_1, φ_2 and θ_1, θ_2, respectively.

Assumption (A). As we know from § 45, the mapping $\theta_1\varphi_1\theta_2$ is an operator endomorphism carrying G into the admissible center. This is true, *a fortiori*, for the mapping $\varphi_1\theta_1\varphi_1\theta_2$. On the other hand, the endomorphism φ_1 maps a subgroup of the center onto a subgroup of the center, because the components of center elements belong to the center. Thus $G\varphi_1\theta_1\varphi_1\theta_2\varphi_1$, as well as $G\varphi_2\theta_1\varphi_2\theta_2\varphi_2$ and $G\theta_j\varphi_1\theta_j\varphi_2\theta_j$, $j = 1, 2$, are admissible subgroups of the center, and (A) follows from the condition of the theorem.

Assumption (B). Instead of n_1 and $\bar{a}_1$ we shall now write N_1 and $\bar{A}_1$. We have to show that

$$A_1 = \{N_1, \bar{A}_1\}.$$

If a_1 is an arbitrary element of A_1, then by Lemma 12

$$a_1\eta^{k_0} \in \bar{A}_1.$$

However $\bar{A}_1\eta^{k_0} = \bar{A}_1$, that is, there exists an element a_1 in A_1 such that

$$\bar{a}_1\eta^{k_0} = a_1\eta^{k_0}.$$

Hence

$$(\bar{a}_1^{-1}a_1)\eta^{k_0} = 1,$$

and by Lemma 13, $\bar{a}_1^{-1}\, a_1 \in N_1$, so that $a_1 \in \{N_1, \bar{A}_1\}$.

Assumption (C). Instead of $\bar{b}_1$ we shall write $\bar{B}_1$. We have to show that

$$\bar{B}_1 \subseteq \{\bar{A}_1, B_2\}. \tag{2}$$

Let x be an element of $\bar{B}_1$. Since

$$\bar{B}_1(\varphi_1\theta_1\varphi_2\theta_1) = \bar{B}_1,$$

there exists an element y in $\bar{B}_1$ such that

$$y\varphi_1\theta_1\varphi_2\theta_1 = x.$$

Let k_0' be the number that plays the same rôle for $\bar{B}_1$ as k_0 does for A_1 in Lemma 12; we denote the larger of the two numbers by k. Then there exists an element b_1 in $\bar{B}_1$ such that

$$b_1(\varphi_1\theta_1\varphi_2\theta_1)^k = y. \tag{3}$$

Expressing the corresponding elements in turn by their components in the first and second decomposition (1) we obtain:

$$y\varphi_1 = y\varphi_1\theta_1 \cdot y\varphi_1\theta_2 = y\varphi_1\theta_1\varphi_1 \cdot y\varphi_1\theta_1\varphi_2 \cdot y\varphi_1\theta_2 =$$
$$= y\varphi_1\theta_1\varphi_1 \cdot y\varphi_1\theta_1\varphi_2\theta_1 \cdot y\varphi_1\theta_1\varphi_2\theta_2 \cdot y\varphi_1\theta_2.$$

Hence

$$x = y\varphi_1\theta_1\varphi_2\theta_1 = (y\varphi_1\theta_1\varphi_1)^{-1} \cdot y\varphi_1 \cdot (y\varphi_1\theta_2)^{-1}(y\varphi_1\theta_1\varphi_2\theta_2)^{-1}. \tag{4}$$

The last two factors on the right-hand side of (4) obviously belong to B_2. Let us show that the first two factors, which belong to A_1, are contained

in $\overline{A}_1$. For this purpose we have to strengthen somewhat Lemmas 1 and 2 of the preceding section, because we must apply them to elements of the group and not merely to subgroups.

LEMMA 1'. *For every element x of G*

$$x\theta_1\varphi_1\theta_2 = x^{-1}\theta_1\varphi_2\theta_2.$$

For since

$$x\theta_1 = x\theta_1\varphi_1 \cdot x\theta_1\varphi_2,$$

we have

$$x\theta_1\varphi_1\theta_2 \cdot x\theta_1\varphi_2\theta_2 = (x\theta_1\varphi_1 \cdot x\theta_1\varphi_2)\,\theta_2 = x\theta_1\theta_2 = 1.$$

LEMMA 2'. *If the element x is contained in the subgroup A_1, then*

$$x\theta_1\varphi_1\theta_2\varphi_1 = x\theta_2\varphi_1\theta_1\varphi_1.$$

The proof is the same as that of Lemma 2 except that in the course of the proof Lemma 1' has to be applied four times.

We now return to equation (4). By applying (3) and Lemmas 1' and 2', we obtain

$$y\varphi_1 = b_1\,(\varphi_1\theta_1\varphi_2\theta_1)^k\varphi_1 = (b_1\varphi_1)\,(\theta_1\varphi_2\theta_1\varphi_1)^k = (b_1\varphi_1)\,(\theta_1\varphi_1\theta_2\varphi_1)^k \subset \overline{A}_1;$$

$$y\varphi_1\theta_1\varphi_1 = b_1\,(\varphi_1\theta_1\varphi_2\theta_1)^k\,\varphi_1\theta_1\varphi_1 = (b\varphi_1)\,(\theta_1\varphi_2\theta_1\varphi_1)^k\,\theta_1\varphi_1 =$$

$$= (b\varphi_1)\,(\theta_1\varphi_1\theta_2\varphi_1)^k\theta_1\varphi_1 = (b\varphi_1\theta_1\varphi_1)\,(\theta_2\varphi_1\theta_1\varphi_1)^k \subset \overline{A}_1.$$

This proves (2). The other part of assumption (C) is proved similarly.

Let us now consider two direct decompositions of a group G with an arbitrary *finite* number of factors:

$$G = A_1 \times A_2 \times \ldots \times A_k = B_1 \times B_2 \times \ldots \times B_l; \qquad (5)$$

by induction over $k + l$ we shall prove the existence of centrally isomorphic refinements of (5) in which *every A_i, $i = 1, 2, \ldots, k$ is decomposed into the product of l factors, and every B_j, $j = 1, 2, \ldots, l$ into the product of k factors (some of these may be E); a centrally isomorphic correspondence between these factors can be established such that no two factors occurring in the decomposition of an arbitrary A_i are linked with factors of the decomposition of one and the same B_j.*

This is true for $k + l = 4$: it is obvious for $k = 1$, $l = 3$ and for $k = 3$, $l = 1$; for $k = l = 2$ it follows from what has been proved above. For in any case the decompositions (13) of the preceding section can be

turned into centrally isomorphic refinements of (1) satisfying the conditions set down above by combining, for example, $\overline{A}_1$ with N_{11}, $\overline{A}_2$ with N_{22}, $\overline{B}_1$ with M_{11}, and $\overline{B}_2$ with M_{22}.

Let $k + l > 4$, and let us assume that our assertion is already proved for every group satisfying the conditions of the theorem and for all pairs of its direct decompositions with fewer than $k + l$, but otherwise arbitrarily many direct factors. If, for example, $k > 2$, we introduce the notation

$$A^*_{k-1} = A_{k-1} \times A_k. \tag{6}$$

Then the direct decompositions

$$G = A_1 \times A_2 \times \ldots \times A^*_{k-1} = B_1 \times B_2 \times \ldots \times B_l$$

have, by hypothesis, centrally isomorphic refinements:

$$\begin{aligned} G = &(A_{11} \times \ldots \times A_{1l}) \times (A_{21} \times \ldots \times A_{2l}) \times \ldots \times \\ &\times (A^*_{k-1,\,1} \times \ldots \times A^*_{k-1,\,l}) = \\ = &(B_{11} \times \ldots \times B_{1,\,k-1}) \times (B_{21} \times \ldots \times B_{2,\,k-1}) \times \ldots \times \\ &\times (B_{l1} \times \ldots \times B_{l,\,k-1}). \end{aligned}$$

Since A^*_{k-1}, as a direct factor of G, also satisfies the conditions of our theorem and $2 + l < k + l$, the two direct decompositions of A^*_{k-1}, namely (6) and

$$A^*_{k-1} = A^*_{k-1,\,1} \times \ldots \times A^*_{k-1,\,l},$$

have centrally isomorphic refinements

$$\begin{aligned} A^*_{k-1} &= (A_{k-1,\,1} \times \ldots \times A_{k-1,\,l}) \times (A_{k1} \times \ldots \times A_{kl}) = \\ &= (A^*_{k-1,\,1,\,1} \times A^*_{k-1,\,1,\,2}) \times \ldots \times (A^*_{k-1,\,l,\,1} \times A^*_{k-1,\,l,\,2}). \end{aligned}$$

If $A^*_{k-1,\,j} \cong B_{j,\,k-1}$, $j = 1, 2, \ldots, l$, and if this central isomorphism links the direct decomposition $A^*_{k-1,\,j} = A^*_{k-1,\,j,\,1} \times A^*_{k-1,\,j,\,2}$ with $B_{j,\,k-1} = B_{j,\,k-1,\,1} \times B_{j,\,k-1,\,2}$, then obviously the direct decompositions

$$\begin{aligned} G = &(A_{11} \times \ldots \times A_{1l}) \times (A_{21} \times \ldots \times A_{2l}) \times \ldots \\ &\ldots \times (A_{k-1,\,1} \times \ldots \times A_{k-1,\,l}) \times (A_{k1} \times \ldots \times A_{kl}) = \\ = &(B_{11} \times \ldots \times B_{1,\,k-1,\,1} \times B_{1,\,k-1,\,2}) \times \\ &\times (B_{21} \times \ldots \times B_{2,\,k-1,\,1} \times B_{2,\,k-1,\,2}) \times \ldots \\ &\ldots \times (B_{l1} \times \ldots \times B_{l,\,k-1,\,1} \times B_{l,\,k-1,\,2}) \end{aligned}$$

are the required centrally isomorphic refinements of (5).

To complete the proof it remains to consider the case of direct decompositions of G with an infinite number of factors. Making use of the concept of an F-group introduced at the end of § 45 and of the theorem on F-groups proved there, we shall first prove the two following lemmas. In the first of these, the restrictions of the fundamental theorem need not be imposed.

LEMMA 19. *Let*

$$G = \dot{\prod_{\alpha}} A_\alpha \times \dot{\prod_{\gamma}} C_\gamma = \dot{\prod_{\beta}} B_\beta \times \dot{\prod_{\delta}} D_\delta \tag{7}$$

be two direct decompositions of a group G with an arbitrary operator domain. If the subgroups

$$C = \dot{\prod_{\gamma}} C_\gamma, \quad D = \dot{\prod_{\delta}} D_\delta$$

are F-groups and if the direct decompositions

$$G = \dot{\prod_{\alpha}} A_\alpha \times C = \dot{\prod_{\beta}} B_\beta \times D \tag{8}$$

have centrally isomorphic refinements, then the given direct decompositions (7) also have centrally isomorphic refinements.

For by assumption the direct decompositions (8) have centrally isomorphic refinements

$$G = \dot{\prod_{\alpha'}} A'_{\alpha'} \times \dot{\prod_{\varepsilon}} C'_\varepsilon = \dot{\prod_{\beta'}} B'_{\beta'} \times \dot{\prod_{\eta}} D'_\eta , \tag{9}$$

where

$$\dot{\prod_{\varepsilon}} C'_\varepsilon = C, \quad \dot{\prod_{\eta}} D'_\eta = D.$$

Since C is an F-group, its direct decompositions

$$C = \dot{\prod_{\gamma}} C_\gamma = \dot{\prod} C'_\varepsilon$$

have, by what has been proved in § 45, a common refinement

$$C = \dot{\prod} C''_\sigma .$$

Substituting this refinement of the decomposition $\prod_{\sigma} C'_{\sigma}$ into the first decomposition (9) and decomposing the centrally isomorphic factors in the second decomposition (9) correspondingly, we come to two new centrally isomorphic decompositions of G:

$$G = \prod_{\alpha'} A'_{\alpha'} \times \prod_{\sigma} C''_{\sigma} = \prod_{\beta''} B''_{\beta''} \times \prod_{\xi} D''_{\xi}, \tag{10}$$

where

$$\prod_{\xi} D''_{\xi} = D.$$

The direct decompositions

$$D = \prod_{\delta} D_{\delta} = \prod_{\xi} D''_{\xi}$$

of the F-group D have a common refinement. Substituting this for $\prod_{\xi} D''_{\xi}$ in the second decomposition (10) correspondingly, we obtain the required centrally isomorphic refinement of the given direct decompositions (7).

LEMMA 20. *If a group G satisfies the conditions of the fundamental theorem, then from any direct decomposition of G a finite number of direct factors can be omitted such that the product of the remaining factors is an F-group.*

Let an arbitrary direct decomposition of G be given. We shall show that it contains only a *finite* number of factors such that the factor groups of the derived group of an *infinite* number of direct factors of the given decomposition could be mapped homomorphically in a non-trivial way into the admissible center of each. Indeed, if this were not so, then we could find a *countable* system of direct factors for which the factor groups of the derived group could be mapped non-trivially into the admissible centers of *distinct* direct factors. Contrary to the conditions of the theorem this however leads to the existence of a homomorphic mapping of the factor group of the derived group of the whole group G onto a subgroup of its admissible center which is the direct product of a countable set of subgroups and therefore cannot have a principal series.

From the given direct decomposition we omit the (finite number of) factors we have spoken of in the preceding paragraph. We show that now we can find altogether only a finite number of factors whose factor groups of the derived group allow a non-trivial isomorphic mapping into the admissible center of any one of the remaining factors. For suppose there were infinitely many such factors: since only a finite number of the factor

groups in question can now be mapped non-trivially into the admissible center of every remaining factor, we could again find a countable system of direct factors for which the factor groups of the derived groups could be mapped non-trivially into the admissible centers of distinct direct factors, again in contradiction to the conditions of the theorem. If we omit these factors also, then the product of the remaining factors is now easily seen to be an F-group.

Lemmas 19 and 20 reduce the general case of the fundamental theorem to the case of decompositions with a finite number of direct factors considered above. The proof of the theorem is thus complete.

The conditions of the fundamental theorem are satisfied if the admissible center of a group or the factor group of its derived group have principal series.

Hence we obtain the Krull-Schmidt Theorem.

KRULL-SCHMIDT THEOREM. *If a group with an arbitrary operator domain has principal series, then any two direct decompositions of the group with indecomposable factors are centrally isomorphic.*

A direct proof of the Krull-Schmidt Theorem can be found in § 27 of the first edition of this book.[m]

CHAPTER XII

EXTENSIONS OF GROUPS

§ 48. Factor systems

According to the definition in § 10, a group G is called an *extension of a group A by a group B* if A is a normal subgroup of G and the factor group G/A is isomorphic to B. For a given A and B there always exist extensions of A by means of B—for example, the direct product of A and B. However, (see § 10) the group G is, in general, not uniquely determined by A and B; it therefore becomes desirable to give a complete survey of all distinct extensions of a given group A by a given group B. Certain problems within the theory of groups and also in the application of group theory to the theory of fields and to combinatorial topology combine to make such a survey necessary.

The classification of the extensions of a group A by a group B is usually carried to within equivalence. Two extensions G and H of A by B are here called *equivalent* if there exists an isomorphism between G and H that on A coincides with the identity automorphism and that maps onto each other the cosets of A corresponding to the same element of B. It is clear that two extensions G and H may turn out to be isomorphic even if they are not equivalent (see Gol'fand [1]).

A first approach to the extension problem was made by Schreier [2, 3]; his theory will be expounded in the present section. Later Baer [4] carried the theory somewhat further, using other methods; in particular, he reduced the survey of the extensions of a group A by a group B essentially to the case in which A is abelian. Finally, in this latter case significant progress has been made during the last few years by the use of the so-called cohomology groups. These group-theoretical constructions, which had been used before in combinatorial topology, were built into the framework of the general theory of groups in independent papers by Eilenberg and MacLane [4, 5] and Faddeev [1].

We shall now present the original theory of Schreier. Let G be an extension of its normal subgroup A by B; the elements of A will be denoted by Latin letters, $a, b, c, \ldots$, the elements of B by Greek letters, $\alpha, \beta, \gamma, \ldots$. In every coset gA of A in G we choose an element as representative and denote it by g_α, where α is the element of B associated with the coset gA in

the isomorphism between G/A and B. The product of the representatives g_α and g_β, again by the isomorphism between G/A and B, lies in the coset of A with representative $g_{\alpha\beta}$ (where the subscript is the product of α and β in B); in other words, there is an element $m_{\alpha,\beta}$ in A such that

$$g_\alpha g_\beta = g_{\alpha\beta} m_{\alpha,\beta}.$$

In particular, taking for α and β the unit element ε of B, we obtain

$$g_\varepsilon g_\varepsilon = g_\varepsilon m_{\varepsilon,\varepsilon},$$

Hence $g_\varepsilon = m_{\varepsilon,\varepsilon}$.

The transformation of A by g_α induces an automorphism in A. We denote the image of an element a of A under this automorphism by a^α;

$$g_\alpha^{-1} a g_\alpha = a^\alpha.$$

Correspondingly, the element $b^{-1}ab$, $b \in A$, will be denoted by a^b. Then

$$(a^\alpha)^\beta = (a^{\alpha\beta})^{m_{\alpha,\beta}}. \tag{1}$$

Further, from the associative law for multiplication in G it follows that

$$g_\alpha g_\beta g_\gamma = g_\alpha (g_{\beta\gamma} m_{\beta,\gamma}) = g_{\alpha\beta\gamma} m_{\alpha,\beta\gamma} m_{\beta,\gamma} = (g_{\alpha\beta} m_{\alpha,\beta}) g_\gamma =$$
$$= g_{\alpha\beta} (g_\gamma m_{\alpha,\beta}^\gamma) = g_{\alpha\beta\gamma} m_{\alpha\beta,\gamma} m_{\alpha,\beta}^\gamma,$$

so that

$$m_{\alpha,\beta\gamma} m_{\beta,\gamma} = m_{\alpha\beta,\gamma} m_{\alpha,\beta}^\gamma. \tag{2}$$

We note, finally, that if $g_\alpha a$ and $g_\beta b$ are two arbitrary elements of G, then they are multiplied in the following way:

$$g_\alpha a \cdot g_\beta b = g_{\alpha\beta} (m_{\alpha,\beta} a^\beta b). \tag{3}$$

So far we have started from a given extension of A by B and have established a correspondence between this extension and a system of elements $m_{\alpha,\beta}$, a so-called *factor system*, and a system of automorphisms $a \to a^\alpha$. Conversely, let us assume now that in a group a system of elements $m_{\alpha,\beta}$ is chosen, where α and β range independently over all the elements of a group B, and that every element α of B is associated with some automorphism $a \to a^\alpha$ of A for which conditions (1) and (2) are satisfied. We shall show that there exists an extension G of A by B for which the given elements $m_{\alpha,\beta}$ and the given automorphisms correspond to this extension in the above sense.

The elements of G will be symbols $g_\alpha a$, where a is an arbitrary element of A and where the symbols g_α correspond one to one to the elements α of B. We define multiplication in G by formula (3) and show that G is a group. The associative law of this multiplication follows easily from its definition and conditions (1) and (2). In fact,

$$(g_\alpha a \cdot g_\beta b) \cdot g_\gamma c = (g_{\alpha\beta} m_{\alpha,\beta} a^\beta b)\, g_\gamma c = g_{\alpha\beta\gamma} m_{\alpha\beta,\gamma} (m_{\alpha,\beta} a^\beta b)^\gamma c =$$
$$= g_{\alpha\beta\gamma} m_{\alpha\beta,\gamma} m_{\alpha,\beta}^\gamma (a^\beta)^\gamma b^\gamma c = g_{\alpha\beta\gamma} m_{\alpha\beta,\gamma} m_{\alpha,\beta}^\gamma (a^{\beta\gamma})^{m_{\beta,\gamma}} b^\gamma c,$$
$$g_\alpha a \cdot (g_\beta b \cdot g_\gamma c) = g_\alpha a \cdot (g_{\beta\gamma} m_{\beta,\gamma} b^\gamma c) =$$
$$= g_{\alpha\beta\gamma} m_{\alpha,\beta\gamma} a^{\beta\gamma} m_{\beta,\gamma} b^\gamma c = g_{\alpha\beta\gamma} m_{\alpha,\beta\gamma} m_{\beta,\gamma} (a^{\beta\gamma})^{m_{\beta,\gamma}} b^\gamma c.$$

and the right-hand sides of the two equations are equal by (2).

We now note that from (1) with $\alpha = \beta = \varepsilon$ it follows that

$$(a^\varepsilon)^\varepsilon = (a^\varepsilon)^{m_{\varepsilon,\varepsilon}},$$

and since a^ε ranges over the whole group A as a does, we have

$$a^\varepsilon = a^{m_{\varepsilon,\varepsilon}}. \tag{4}$$

Further, from (2) it follows for $\beta = \gamma = \varepsilon$ that

$$m_{\alpha,\varepsilon} m_{\varepsilon,\varepsilon} = m_{\alpha,\varepsilon} m_{\alpha,\varepsilon}^\varepsilon,$$

and hence by (4)

$$m_{\varepsilon,\varepsilon} = m_{\alpha,\varepsilon}^- = m_{\alpha,\varepsilon}^{\cdots\varepsilon},$$

and since $m_{\varepsilon,\varepsilon}$ does not change when it is transformed by itself, we obtain

$$m_{\alpha,\varepsilon} = m_{\varepsilon,\varepsilon}. \tag{5}$$

Finally, from (2) it follows for $\alpha = \beta = \varepsilon$ that

$$m_{\varepsilon,\gamma} m_{\varepsilon,\gamma} = m_{\varepsilon,\gamma} m_{\varepsilon,\varepsilon}^\gamma,$$

and hence that

$$m_{\varepsilon,\gamma} = m_{\varepsilon,\varepsilon}^\gamma. \tag{6}$$

If $g_\alpha a$ is an arbitrary element of G, then by (4) and (5)

$$g_\alpha a \cdot g_\varepsilon m_{\varepsilon,\varepsilon}^{-1} = g_\alpha m_{\alpha,\varepsilon} a^\varepsilon m_{\varepsilon,\varepsilon}^{-1} = g_\alpha m_{\varepsilon,\varepsilon} a^{m_{\varepsilon,\varepsilon}} m_{\varepsilon,\varepsilon}^{-1} = g_\alpha a,$$

so that $g_\varepsilon m_{\varepsilon,\varepsilon}^{-1}$ is a right unit element of G. Furthermore,

$$g_a a \cdot g_{a^{-1}} (a^{a^{-1}})^{-1} m_{a,a^{-1}}^{-1} m_{\varepsilon,\varepsilon}^{-1} = g_\varepsilon m_{\varepsilon,\varepsilon}^{-1},$$

so that every element of G has a right inverse. This proves that G is a group.

Let us show that G is the required extension of A by B. If we associate with every element a of A the element

$$\bar{a} = g_\varepsilon m_{\varepsilon,\varepsilon}^{-1} a$$

of G, then by (4) and (6)

$$\bar{a} \cdot \bar{b} = g_\varepsilon m_{\varepsilon,\varepsilon}^{-1} a \cdot g_\varepsilon m_{\varepsilon,\varepsilon}^{-1} b = g_\varepsilon m_{\varepsilon,\varepsilon}^{-1} ab = \overline{ab},$$

and from $\bar{a} = g_\varepsilon m_{\varepsilon,\varepsilon}^{-1}$ (that is, for the unit element of G) it follows that $a = 1$. Thus, the elements $\bar{a}$ form a subgroup $\bar{A}$ of G, isomorphic to A. Further, if we use the notation $\bar{g}_\alpha = g_\alpha \cdot 1$, then, by (5),

$$\bar{g}_\alpha \bar{a} = g_\alpha 1 \cdot g_\varepsilon m_{\varepsilon,\varepsilon}^{-1} a = g_\alpha m_{\alpha,\varepsilon} m_{\varepsilon,\varepsilon}^{-1} a = g_\alpha a. \tag{7}$$

It follows that the elements $\bar{g}_\alpha$ lie in distinct left cosets of $\bar{A}$: for

$$\bar{g}_\beta = \bar{g}_\alpha \bar{a}, \quad \beta \neq \alpha,$$

would imply

$$g_\beta 1 = g_\alpha a,$$

and this is clearly impossible because $\beta \neq \alpha$. On the other hand, (7) shows that every left coset of $\bar{A}$ contains one of the elements $\bar{g}_\alpha$. From (6) and (7) we deduce

$$\bar{a}\bar{g}_\alpha = g_\varepsilon m_{\varepsilon,\varepsilon}^{-1} a \cdot g_\alpha 1 = g_\alpha m_{\varepsilon,\alpha} (m_{\varepsilon,\varepsilon}^{-1})^\alpha a^\alpha = g_\alpha a^\alpha = \bar{g}_\alpha \bar{a}^\alpha,$$

and hence

$$\bar{g}_\alpha^{-1} \bar{a} \bar{g}_\alpha = \bar{a}^\alpha \in \bar{A},$$

that is, $\bar{A}$ is a normal subgroup of G, and the transformation by $\bar{g}_\alpha$ induces an automorphism in A that coincides with the original automorphism $a \to a^\alpha$ of A. Finally, the equation

$$\bar{g}_\alpha \cdot \bar{g}_\beta = g_\alpha 1 \cdot g_\beta 1 = g_{\alpha\beta} m_{\alpha,\beta} = \bar{g}_{\alpha\beta} \bar{m}_{\alpha,\beta}$$

shows that the factor group $G/\bar{A}$ is isomorphic to B, in other words, that G is an extension of $\bar{A}$ by B and that the factor system of this extension coincides with the given elements $m_{\alpha,\beta}$, provided that the chosen representatives of the left cosets of $\bar{A}$ are precisely the elements $\bar{g}_\alpha$.

Finally, if we compare the construction of G just explained with the one given earlier for a definite factor system and if, in particular, we take (3)

into account, then we find that every extension of A by B to which the factor system $m_{\alpha,\beta}$ and the automorphisms $a \to a^{\alpha}$ correspond is equivalent to the extension G constructed above.

We have, then, the following result.

Every system of elements $m_{\alpha,\beta}$ and of automorphisms $a \to a^{\alpha}$ of A, $\alpha, \beta \in B$, for which conditions (1) *and* (2) *are satisfied corresponds to an extension of A by B, which is uniquely determined up to equivalence. Conversely, every extension of A by B can be given by such a system of elements and automorphisms.*

This correspondence between extensions on the one hand and factor systems on the other is, however, not one to one, since the choice of the representatives g_{α} of the cosets of A in the extension G was completely arbitrary. If G is an extension of A by B and if this extension is given by the factor system $m_{\alpha,\beta}$ and the automorphisms φ_{α} for the choice of representatives g_{α}, while another choice of representatives $g'_{\alpha} = g_{\alpha}c_{\alpha}$, $c_{\alpha} \in A$, leads to the factor system $m_{\alpha,\beta}'$ and the automorphisms φ'_{α}, then each φ_{α}' is obtained from φ_{α} by multiplying on the right by the inner automorphism induced in A by c_{α}. Furthermore, from

$$g'_{\alpha} \cdot g'_{\beta} = g_{\alpha}c_{\alpha} \cdot g_{\beta}c_{\beta} = g_{\alpha\beta}m_{\alpha,\beta}c_{\alpha}^{\beta}c_{\beta} = g'_{\alpha\beta}c_{\alpha\beta}^{-1}m_{\alpha,\beta}c_{\alpha}^{\beta}c_{\beta}$$

it follows that

$$m'_{\alpha,\beta} = c_{\alpha\beta}^{-1}m_{\alpha,\beta}c_{\alpha}^{\beta}c_{\beta}. \tag{8}$$

Conversely, if two extensions G and G' are given and if we can find elements c_{α} in A, $\alpha \varepsilon B$, such that the factor systems and automorphisms which give the two extensions are linked in the way just described, then it is easy to verify that the correspondence carrying the element $g_{\alpha}a$ of G into the element $g'_{\alpha}c_{\alpha}^{-1}a$ of G' is an isomorphism that establishes the equivalence of G and G'. If we note, finally, that the factor systems and automorphisms do not change when $c_{\alpha} = 1$ for all α, then we obtain the following result.

Two extensions G and G' of a group A by means of a group B given by the factor systems $m_{\alpha,\beta}$ and $m'_{\alpha,\beta}$ and the automorphisms φ_{α} and φ_{α}', respectively, are equivalent if and only if every element α of can be associated with an element c_{α} of A in such a way that (i) *every automorphism φ_{α}' is obtained by multiplying the automorphism φ_{α} on the right by the inner automorphism of A induced by c_{α} and* (ii) *the factors are linked by the relations* (8).

This theory cannot be considered as complete. The description of the distinct extensions of a given group A by a given group B is here reduced to

the search for certain systems of elements and of automorphisms of A which are subject to rather complicated conditions and which, in general, do not simplify very much the survey of the totality of all non-equivalent extensions. In the following sections we shall describe methods by which we can come much closer to such a survey; here we shall conduct some preliminary investigations.

Let us denote by $\mathfrak{A}$ the factor group of the subgroup of inner automorphisms in the group of all automorphisms of A; the elements of $\mathfrak{A}$ are denoted by $\mathfrak{a}$ with subscripts and are called *automorphism classes* of A. If now G is an extension of A by B and if the element α of B corresponds to the coset $g_\alpha A$ of G, then the automorphisms of A induced by transforming A by various elements of $g_\alpha A$ are obtained from one another by multiplication by inner automorphisms; that is, they belong to the same automorphism class. Thus, to every element α of B there corresponds an element $\mathfrak{a}_\alpha$ of $\mathfrak{A}$ and from $g_\alpha A \cdot g_\beta A = g_{\alpha\beta} A$ and the definition of multiplication of automorphisms it follows that

$$\mathfrak{a}_\alpha \cdot \mathfrak{a}_\beta = \mathfrak{a}_{\alpha\beta}.$$

In other words, to the extension G there corresponds a well-defined homomorphic mapping of B into $\mathfrak{A}$ which will be called the *homomorphism associated with this extension.*

Suppose now that two *equivalent* extensions of A by B are given. From the link established above between the automorphisms $a \to a_\alpha$ of A corresponding to equivalent extensions, it follows that *the same homomorphism of B into $\mathfrak{A}$ is associated with both extensions.* In the following classification we may therefore confine ourselves to those non-equivalent extensions of A by B that have a given associated homomorphism of B into $\mathfrak{A}$; of course, it is also necessary to establish which of the homomorphisms of B into $\mathfrak{A}$ can be associated with arbitrary extensions of A by B and which cannot.

§ 49. Extensions of abelian groups. Cohomology groups

In this section we shall study the extensions of an abelian group A by an arbitrary group B. As we have shown above, we can confine our classification to extensions with a *given* associated homomorphism of B into $\mathfrak{A}$. In our case, $\mathfrak{A}$ coincides with the group of automorphisms of A, so that we can regard B as a *group of operators* for the abelian group A. This means

that products $a\alpha$, $a \in A$, $\alpha \in B$, are so defined that $a\alpha \in A$ and that the following conditions are satisfied:

1) $(ab)\alpha = a\alpha \cdot b\alpha$,

2) $a(\alpha\beta) = (a\alpha)\beta$,

3) $a\varepsilon = a$, where ε is the unit element of B.

Since we wish to emphasize that we investigate the extension of A by B with a *given* associated homomorphism, in other words, that the way in which the elements of B act as operators on A is fixed, we shall speak of the *extensions of the abelian group A by the group of operators B.*

If G is one of these extensions, then the automorphism $a \to a^\alpha$ of A (see the preceding section) does not depend on the choice of the representative in the coset $g_\alpha A$ and coincides with the automorphism induced by the operator α, so that $a^\alpha = a\alpha$. Thus, *an extension of an abelian group A by a group of operators B is completely determined by the factor system $m_{\alpha,\beta}$ subject to condition* (2) *of the preceding section*; condition (1) coincides with condition (2) in the definition of an operator group, because A is abelian.

Let us consider all possible factor systems $m_{\alpha,\beta}$, $\alpha, \beta \in B$, that can be chosen in a group A with a group of operators B, subject to (2). One such system always exists, namely $m_{\alpha,\beta} = 1$ for all α and β. If $m_{\alpha,\beta}$ and $n_{\alpha,\beta}$ are two such factor systems then the products

$$m_{\alpha,\beta}\, n_{\alpha,\beta}$$

also satisfy condition (2) in view of the commutative law in A, that is, they form another factor system.

This "multiplication" of factor systems is associative and commutative; the rôle of the unit element is played by the system $m_{\alpha,\beta} = 1$ for all α and β; the inverse of the system $m_{\alpha,\beta}$ is the system $m_{\alpha,\beta}^{-1}$, which, as is easily verified, satisfies condition (2). We therefore obtain an abelian group, which we denote by $F(A, B)$.

If we associate with every element α of B an arbitrary element c_α of A, then the system of elements

$$m_{\alpha,\beta} = c_{\alpha\beta}^{-1} (c_\alpha^\beta) c_\beta \tag{9}$$

will satisfy condition (2) and will therefore be a factor system. All such factor systems form a subgroup $T(A, B)$ of $F(A, B)$.

From results in the preceding section, in particular from (8), it follows that *all non-equivalent extensions of an abelian group A by a group of*

operators B correspond one-to-one to the cosets of $T(A, B)$ in $F(A, B)$, that is, to the elements of the factor group

$$F(A, B)/T(A, B).$$

We call this factor group the *group of extensions of the abelian group A by the group of operators B.*

The group of extensions could, of course, have been constructed by taking as its elements the classes of equivalent extensions themselves and by defining multiplication of these classes suitably. In another context, in § 51, the reader will come across the multiplication of extensions starting from this construction.

We note the following analogy. If we wish to get an over-all picture of all the automorphisms of a group, we have to investigate its group of automorphisms. Similarly, the task of getting such a picture of non-equivalent extensions of an abelian group A by an operator group B reduces essentially to the investigation of the corresponding group of extensions. The remainder of the present section is devoted to this task.

Cohomology groups. We shall write the abelian group A with elements $a, b, \ldots$ in additive notation and its group of operators B with elements $\alpha, \beta, \ldots$ in multiplicative notation. Every function $f(\alpha_1, \alpha_2, \ldots, \alpha_n)$ of n elements of B with values in A shall be called an n-dimensional *cochain.* In particular, the zero-dimensional cochains will simply be the elements of A.

If we define addition of n-dimensional chains by the equation

$$(f_1 + f_2)(\alpha_1, \alpha_2, \ldots, \alpha_n) = f_1(\alpha_1, \alpha_2, \ldots, \alpha_n) + f_2(\alpha_1, \alpha_2, \ldots, \alpha_n),$$

we obtain an abelian group $C^n(B, A)$. In particular, $C^0(B, A) = A$.

With every n-dimensional cochain f, $n \geqq 0$, we associate an $(n+1)$-dimensional cochain δf called the *coboundary* of the chain f and defined as follows:

$$\begin{aligned}(\delta f)(\alpha_1, \alpha_2, \ldots, \alpha_{n+1}) = {} & f(\alpha_2, \ldots, \alpha_{n+1}) + \\ & + \sum_{k=1}^{n} (-1)^k f(\alpha_1, \ldots, \alpha_{k-1}, \alpha_k \alpha_{k+1}, \alpha_{k+2}, \ldots, \alpha_{n+1}) + \\ & + (-1)^{n+1} f(\alpha_1, \ldots, \alpha_n)\, \alpha_{n+1}. \qquad (10)\end{aligned}$$

It is easy to verify that

$$\delta(f_1 + f_2) = \delta f_1 + \delta f_2, \qquad (11)$$

so that the mapping $f \to \delta f$ is a homomorphism of $C^n(B, A)$ into $C^{(n+1)}(B, A)$.

The following important relation holds:

$$\delta(\delta f) = 0 \tag{12}$$

or, in words: the coboundary of a coboundary is zero.

For if f is an n-dimensional cochain, then $\delta(\delta f)$ is an $(n+2)$-dimensional cochain, that is, a function of $\alpha_1, \alpha_2, \ldots, \alpha_{n+2}$. If we calculate it using (10), we are led to equation (12), because every summand occurs twice with opposite signs: suppose that in the development of $\delta(\delta f)$ a given summand occurs in the following way: after the first application of (10) we take the k-th summand, $0 \leqq k \leqq n+2$, and after this we again apply (10) to it and take the l-th summand, $0 \leqq l \leqq n+1$, then this term has the sign $(-1)^{k+l}$. It remains to show what these k and l are for each term. We do this in the form of a table, which will complete the proof of (12).

Type of Summand	k, l	Sign
$f(\alpha_1, \ldots, \alpha_{k-1}\alpha_k\alpha_{k+1}, \ldots, \alpha_{n+2})$, $2 \leqq k \leqq n+1$	$k, k-1$	$(-1)^{2k-1}$
	$k-1, k-1$	$(-1)^{2k-2}$
$f(\alpha_1, \ldots, \alpha_l\alpha_{l+1}, \ldots, \alpha_k\alpha_{k+1}, \ldots, \alpha_{n+2})$, $1 \leqq l, l+1 \leqq k, k \leqq n+1$	k, l	$(-1)^{k+l}$
	$l, k-1$	$(-1)^{k+l-1}$
$f(\alpha_2, \ldots, \alpha_k\alpha_{k+1}, \ldots, \alpha_{n+2})$, $2 \leqq k \leqq n+1$	$k, 0$	$(-1)^k$
	$0, k-1$	$(-1)^{k-1}$
$f(\alpha_1, \ldots, \alpha_k\alpha_{k+1}, \ldots, \alpha_{n+1})\,\alpha_{n+2}$, $1 \leqq k \leqq n$	$n+2, k$	$(-1)^{n+k+2}$
	$k, n+1$	$(-1)^{n+k+1}$
$f(\alpha_3, \ldots, \alpha_{n+2})$	$1, 0$	-1
	$0, 0$	1
$f(\alpha_1, \ldots, \alpha_n)\,\alpha_{n+1}\alpha_{n+2}$	$n+2, n+1$	$(-1)^{2n+3}$
	$n+1, n+1$	$(-1)^{2n+2}$

We shall call an n-dimensional cochain an n-dimensional *cocycle* if $\delta f = 0$. From (11) it follows that the n-dimensional cocycles form a subgroup of $C^n(B, A)$, which we denote by $Z^n(B, A)$.

On the other hand, for $n > 0$ the n-dimensional cochains that are co-

boundaries of some $(n-1)$-dimensional cochains form, again by (11), a subgroup of $C^n(B, A)$, which we denote by $D^n(B, A)$. Since by (12) every coboundary is a cocycle, we have

$$D^n(B, A) \subseteq Z^n(B, A). \tag{13}$$

For $n = 0$ we put $D^0(B, A) = 0$; (13) then remains valid.

The factor group $H^n(B, A) = Z^n(B, A)/D^n(B, A)$ is called the *n-th cohomology group of* B over A.[1]

The cohomology groups for $n = 0, 1, 2$. By definition, a zero-dimensional cochain f is an element a of A. Then, by (10),

$$(\delta f)(\alpha_1) = a - a\alpha_1. \tag{14}$$

Therefore f is a cocycle if and only if $a\alpha_1 = a$ for all α_1 of B. Taking into account that $D^0(B, A) = 0$, we obtain:

The zero-dimensional cohomology group $H^0(B, A)$ is the subgroup of A consisting of all the elements that are mapped onto themselves by all the operators of B.

If $f = f(\alpha_1)$ is a one-dimensional cochain, then by (10)

$$(\delta f)(\alpha_1, \alpha_2) = f(\alpha_2) - f(\alpha_1\alpha_2) + f(\alpha_1)\alpha_2. \tag{15}$$

The cochain $f(\alpha_1)$ is therefore a cocycle if and only if

$$f(\alpha_1\alpha_2) = f(\alpha_2) + f(\alpha_1)\alpha_2. \tag{16}$$

The mappings of B into A subject to this condition are called *crossed homomorphisms*. They are studied in a number of papers, particularly in connection with their application to the theory of fields. Historically, the first paper is one by Schur [2], and some of the latest are the papers by Baer [28, 31].

By (14) a cochain $f(\alpha_1)$ belongs to $D^1(B, A)$ if and only if there exists an element a in A such that

$$f(\alpha_1) = a - a\alpha_1. \tag{17}$$

Such crossed homomorphisms are called *principal*. Therefore, *the first cohomology group $H^1(B, A)$ is the factor group of the subgroup of the prin-*

[1] The author uses the terms homology, chain, boundary, and cycle without the prefix 'co'; the text gives the accepted topological terminology. [*Trans.*]

cipal homomorphisms in the group of the crossed homomorphisms of B into A.

We are mainly interested in the *second* cohomology group. If $f(\alpha_1, \alpha_2)$ is a two-dimensional cochain, then by (10)

$$(\delta f)(\alpha_1, \alpha_2, \alpha_3) = f(\alpha_2, \alpha_3) - f(\alpha_1\alpha_2, \alpha_3) + \\ + f(\alpha_1, \alpha_2\alpha_3) - f(\alpha_1, \alpha_2)\alpha_3. \tag{18}$$

Thus, f is a cocycle if and only if

$$f(\alpha_1, \alpha_2\alpha_3) + f(\alpha_2, \alpha_3) = f(\alpha_1\alpha_2, \alpha_3) + f(\alpha_1, \alpha_2)\alpha_3 \tag{19}$$

or, comparing (19) with (2), if f is a factor system of A with the group of operators B; therefore

$$Z^2(B, A) = F(A, B).$$

On the other hand, by (15) a cochain $f(\alpha_1, \alpha_2)$ belongs to $D^2(B, A)$ if and only if there exists a one-dimensional cochain $\varphi(\alpha_1)$ such that

$$f(\alpha_1, \alpha_2) = \varphi(\alpha_2) - \varphi(\alpha_1\alpha_2) + \varphi(\alpha_1)\alpha_2. \tag{20}$$

Comparing this with (9), we find

$$D^2(B, A) = T(A, B).$$

Therefore, *the second cohomology group $H^2(B, A)$ coincides with the group of extensions of A by the group of operators B.*

Some interpretations of cohomology groups $H^n(B, A)$ for $n \geqq 3$ can be found in papers by Eilenberg and MacLane [4, 6].

§ 50. Calculation of the second cohomology group

The interpretation of the group of extensions of an abelian group A by a group of operators B as the second cohomology group of B over A does not facilitate the investigation of the group. However, there exist methods that enable us to reduce the calculation of the group $H^n(B, A)$ to the calculation of a certain group $H^k(B, A')$, where $k < n$, but where A' has, in general, a more complicated structure than the original group A. The working of one such method will be illustrated in the present section, in which we explain a calculation of the group $H^2(B, A)$, making use of an arbitrary

representation of B as a factor group of a free group (see MacLane [1]). Let

$$B = S/R,$$

where S is a free group with elements $x, y, \ldots$. If for arbitrary elements a of A and x of S we put

$$ax = a(xR) \tag{21}$$

—the coset xR is regarded here as an element of B—then S becomes a group of operators for A. Conditions 1)-3) of the preceding section are verified without any difficulty. Since R is the unit element of B, it follows from (21) that for an arbitrary element r of R

$$ar = a. \tag{22}$$

Moreover, the transformation of the normal subgroup R by an arbitrary element of S induces an automorphism in R. This allows us to regard the elements of S also as operators for R.

R and A are now operator groups with one and the same group of operators S. An *operator homomorphism* φ of R into A is therefore a homomorphism of R into A such that

$$\varphi(x^{-1}rx) = \varphi(r)x, \; r \in R, \; x \in S. \tag{23}$$

If φ and ψ are two operator homomorphisms of R into A, then their sum, defined by the equation

$$(\varphi + \psi)(r) = \varphi(r) + \psi(r),$$

is also an operator homomorphism. Under this addition the operator homomorphisms of R into A form an abelian group which we call the *group of operator homomorphisms* and denote by $Q(R, A; S)$.

If we consider, further, a crossed homomorphism $\varphi(x)$ of S into A, that is (see (16)),

$$\varphi(xy) = \varphi(y) + \varphi(x)y, \tag{24}$$

then by (22) the mapping φ applied to the elements of R is a homomorphism. This is an operator homomorphism: by (24) and (22)

$$\varphi(x^{-1}rx) = \varphi(x) + \varphi(x^{-1}r)x = \varphi(x) + \varphi(r)x + \varphi(x^{-1})rx =$$
$$= \varphi(x) + \varphi(r)x + \varphi(x^{-1})x.$$

Putting $r = 1$ in this equation and taking into account that (24) implies $\varphi(1) = 0$, we find

$$\varphi(x)+\varphi(x^{-1})x=0,$$

and therefore

$$\varphi(x^{-1}rx)=\varphi(r)x.$$

We denote by $Q'(R, A; S)$ the totality of operator homomorphisms of R into A which, in the sense indicated, are induced by crossed homomorphisms of S into A. This is a subgroup of $Q(R, A; S)$, because the crossed homomorphisms of S into A form a group under addition,

$$(\varphi+\psi)(x)=\varphi(x)+\psi(x)$$

namely $Z'(S, A)$.

Our object is to prove the following theorem:

MACLANE'S THEOREM. *The second cohomology group of B over A is isomorphic to the factor group of $Q'(R, A; S)$ in the group of operator homomorphisms $Q(R, A; S)$:*

$$H^2(B, A)\simeq Q(R, A; S)/Q'(R, A; S).$$

We begin the proof by choosing a representative in each coset of R in S, and denoting by s_α the representative of that coset which is the element α of B, so that

$$\alpha=s_\alpha R. \tag{25}$$

Then

$$s_\alpha s_\beta=s_{\alpha\beta}r(\alpha, \beta), \tag{26}$$

where $r(\alpha, \beta)\epsilon R$ and the factors $r(\alpha, \beta)$ are, of course, linked by equations of type (2). In R itself we choose the unit element as representative, that is, $s_\varepsilon=1$, where ε is the unit element of B.

Now let $\varphi(r)$ be an arbitrary operator homomorphism of R into A. Then

$$\bar{\varphi}(\alpha, \beta)=\varphi(r(\alpha, \beta)) \tag{27}$$

is a two-dimensional cochain of B in A, that is, an element of $C^2(B, A)$.

It is even a cocycle: for

$$(\delta\bar{\varphi})(\alpha, \beta, \gamma)=\varphi(r(\beta, \gamma))-\varphi(r(\alpha\beta, \gamma))+ \\ +\varphi(r(\alpha, \beta\gamma))-[\varphi(r(\alpha, \beta))]\gamma.$$

Moreover, using (25), (21), and the definition of an operator homomorphism—that is, (23)—we obtain that

$$[\varphi(r(\alpha,\ \beta))]\,\gamma = [\varphi(r(\alpha,\ \beta))]\,s_\gamma = \varphi(s_\gamma^{-1} r(\alpha,\ \beta)\, s_\gamma).$$

Finally, taking into account that φ is a homomorphism of R into A and that the elements $r(\alpha, \beta)$ are linked by equations of type (2), we see that

$$(\delta\bar{\varphi})(\alpha,\ \beta,\ \gamma) = 0,$$

that is, $\bar{\varphi}(\alpha,\ \beta) \in Z^2(B,\ A)$.

The mapping

$$\varphi(r) \to \bar{\varphi}(\alpha,\ \beta) \tag{28}$$

carries the sum of two operator homomorphisms of R into A into the sum of the corresponding two-dimensional cocycles, in other words, it is a homomorphic mapping of $Q(R, A; S)$ into $Z^2(B, A)$. Mapping the latter group in the canonical way onto its factor group $H^2(B, A)$ *we arrive at a homomorphic mapping of* $Q(R, A; S)$ *into* $H^2(B, A)$.

Let us show that *this homomorphism maps* $Q(R, A; S)$ *onto the whole group* $H^2(B, A)$. For this purpose we choose an arbitrary element of $H^2(B, A)$, that is, an arbitrary coset of $D^2(B, A)$ in $Z^2(B, A)$, and a cocycle $f(\alpha, \beta)$ as a representative of this coset. We can take this cocycle to be *normalized*; that is, we can take it to satisfy the equation

$$f(\alpha,\ \varepsilon) = f(\varepsilon,\ \beta) = 0, \tag{29}$$

where ε is the unit element of B.

For if the cocycle $f(\alpha, \beta)$ is chosen arbitrarily, then as we know, it serves as the factor system for some extension of A by the group of operators B linked in this extension with a certain choice of representatives in the cosets of A. If we make a different choice of representatives *by taking the unit element as representative of the unit coset* we obtain an equivalent extension, that is, the new factor system remains in the chosen coset of $D^2(B, A)$ in $Z^2(B, A)$. Moreover, the new factor system is now normalized, as equations (5) and (6) show.

We now construct a mapping $\varphi(x)$ of S into A such that the following property holds: For any x and y in S

$$\varphi(xy) = \varphi(x)y + \varphi(y) + f(xR,\ yR). \tag{30}$$

Since the cocycle $f(\alpha, \beta)$ is normalized, it follows from (30) that

$$\varphi(1) = 0. \tag{31}$$

Further, if we choose in S a system of free generators and for every element s of that system put

$$\varphi(s)=0, \tag{32}$$

we do not obtain a contradiction to (30). From (30) it now follows that

$$\varphi(s^{-1})=-f(sR, s^{-1}R). \tag{33}$$

Let $\varphi(y)$ be already defined for all elements y whose reduced length in the given system of free generators is less than k and let x be an element of length k. Expressing the word x as a product of two words between which there are no cancellations and using (30), we define a value of $\varphi(x)$. This is independent of the choice of the mode of expressing x as a product of two words of length l_1 and l_2, where $l_1+l_2=k$: it is easy to verify on the basis of (30) and equation (19), which holds for the cycle f, that

$$\varphi(x\cdot yz)=\varphi(xy\cdot z);$$

therefore if the word x has the form

$$x=s_1^{\varepsilon_1}\, s_2^{\varepsilon_2}\, \ldots\, s_k^{\varepsilon_k},$$

then

$$\varphi(s_1^{\varepsilon_1}\cdot(s_2^{\varepsilon_2}\ldots s_k^{\varepsilon_k}))=\varphi((s_1^{\varepsilon_1}s_2^{\varepsilon_2})\cdot(s_3^{\varepsilon_3}\ldots s_k^{\varepsilon_k}))=\ldots=$$
$$=\varphi((s_1^{\varepsilon_1}\ldots s_{k-1}^{\varepsilon_{k-1}})\cdot s_k^{\varepsilon_k}).$$

The mapping $\varphi(x)$ is therefore defined for all x. We have to show, however, that (30) *does, in fact, hold for arbitrary* x *and* y. If there are no cancellations between x and y, then this follows from what we have shown in the preceding paragraph. Moreover, it is easy to verify that the statement is true when one of the elements x, y is 1 and also when they are both of length 1. For

$$\varphi(s^{-1}s)=\varphi(1)=0,$$

but by (32) and (33)

$$\varphi(s^{-1})s+\varphi(s)+f(s^{-1}R, sR)=-f(sR, s^{-1}R)s+f(s^{-1}R, sR),$$

and the right-hand side of this equation is zero: we can deduce this from (21) and (19), putting $a_1=sR$, $a_2=s^{-1}R$, $a_3=sR$.

Suppose, then, that (30) is already proved for every pair of elements

the sum of whose lengths is less than that of x and y, and suppose that cancellations occur between x and y. If

$$x = x's, \quad y = s^{-1}y',$$

where s is one of the free generators and the expressions are *reduced*, then by the induction hypothesis

$$\varphi(xy) = \varphi(x'y') = \varphi(x')y' + \varphi(y') + f(x'R, y'R).$$

On the other hand, by (32) and (33),

$$\varphi(x) = \varphi(x')s + f(x'R, sR),$$
$$\varphi(y) = -f(sR, s^{-1}R)y' + \varphi(y') + f(s^{-1}R, y'R),$$

and therefore

$$\varphi(x)y + \varphi(y) + f(xR, yR) = \varphi(x')y' + f(x'R, sR)s^{-1}y' -$$
$$-f(sR, s^{-1}R)y' + \varphi(y') + f(s^{-1}R, y'R) + f(x'sR, s^{-1}y'R) =$$
$$= \varphi(x')y' + \varphi(y') + f(x'R, y'R).$$

The last equation has been obtained by applying (19) twice, first with

$$\alpha_1 = sR, \ \alpha_2 = s^{-1}R, \ \alpha_3 = y'R,$$

and then with

$$\alpha_1 = x'R, \ \alpha_2 = sR, \ \alpha_3 = s^{-1}y'R.$$

The case $x = x's^{-1}$, $y = sy'$ is verified by the same method.

The mapping $\varphi(x)$ of S into A that we have constructed has the property (30). If $r \in R$, then by (22) and (29)

$$\varphi(xr) = \varphi(x) + \varphi(r). \tag{34}$$

In particular, for $r_1, r_2 \in R$,

$$\varphi(r_1r_2) = \varphi(r_1) + \varphi(r_2),$$

so that *the mapping $\varphi(r)$, $r \in R$, is a homomorphism of R into A. This is an operator homomorphism*:

$$\varphi(x^{-1}rx) = \varphi(x^{-1}r)x + \varphi(x) + f(x^{-1}rR, xR),$$

or by (34)

$$\varphi(x^{-1}rx) = \varphi(x^{-1})\,x + \varphi(r)\,x + \varphi(x) + f(x^{-1}R,\ xR).$$

For $r = 1$ we obtain

$$\varphi(x^{-1}x) = \varphi(1) = 0 = \varphi(x^{-1})\,x + \varphi(x) + f(x^{-1}R,\ xR),$$

and therefore

$$\varphi(x^{-1}rx) = \varphi(r)\,x.$$

We shall now show that *the operator homomorphism* $\varphi(r)$ *is carried by the mapping* (28) *into the chosen coset of* $D^2(B, A)$ *in* $Z^2(B, A)$. For by (27), (26), (21), (25), and (30),

$$\bar{\varphi}(\alpha,\ \beta) = \varphi\big(r(\alpha,\ \beta)\big) = \varphi(s_{\alpha\beta}^{-1}s_\alpha s_\beta) = \varphi(s_{\alpha\beta}^{-1})\,\alpha\beta + \varphi(s_\alpha s_\beta) + \\ + f(s_{\alpha\beta}^{-1}R,\ s_\alpha s_\beta R) = \varphi(s_{\alpha\beta}^{-1})\,\alpha\beta + \varphi(s_\alpha)\,\beta + \\ + \varphi(s_\beta) + f(\alpha,\ \beta) + f\left((\alpha\beta)^{-1},\ \alpha\beta\right).$$

However,

$$0 = \varphi(1) = \varphi(s_{\alpha\beta}^{-1}s_{\alpha\beta}) = \varphi(s_{\alpha\beta}^{-1})\,\alpha\beta + \varphi(s_{\alpha\beta}) + f\big((\alpha\beta)^{-1},\ \alpha\beta\big).$$

Therefore

$$\bar{\varphi}(\alpha,\ \beta) - f(\alpha,\ \beta) = \varphi(s_\alpha)\,\beta + \varphi(s_\beta) - \varphi(s_{\alpha\beta}),$$

and since $\varphi(s_\alpha)$ can be considered as a mapping of B into A, that is, as an element of $C^1(B, A)$, we have by (20)

$$\bar{\varphi}(\alpha,\ \beta) - f(\alpha,\ \beta)\ \varepsilon\ D^2(B,\ A), \tag{35}$$

and this is what we had to prove.

Thus we have a homomorphic mapping of $Q(R, A; S)$ onto $H^2(B, A)$. The main theorem will be proved if we can show that the kernel of this homomorphism is $Q'(R, A; S)$, in other words, that the elements of $Q'(R, A; S)$, and they only, go over into elements of $D^2(B, A)$ under the mapping (28).

Let $\varphi(r)$ be an operator homomorphism of R into A induced by a crossed homomorphism $\varphi(x)$ of S into A. Equation (24), which defines a crossed homomorphism, is a special case of (30), namely that which arises when the null cocycle is chosen for $f(\alpha, \beta)$,

$$f(\alpha, \beta) = 0. \tag{36}$$

Since in the last paragraph of the preceding proof we have not made use of any properties of the mapping $\varphi(x)$ except (30), relation (35) in our case takes the form

$$\bar{\varphi}(\alpha, \beta) \in D^2(B, A)$$

by (36), that is, the operator homomorphism $\varphi(r)$ is, in fact, mapped by (28) into $D^2(B, A)$.

Conversely, let an operator homomorphism $\varphi(r)$ be such that it is mapped by (28) into $D^2(B, A)$. There exists, then, a one-dimensional cochain $\psi(\alpha) \in C^1(B, A)$ such that

$$\bar{\varphi}(\alpha, \beta) = \psi(\beta) - \psi(\alpha\beta) + \psi(\alpha)\beta. \tag{37}$$

We note that

$$\psi(\varepsilon) = 0, \tag{38}$$

where ε is the unit element of B. For (26) leads to the equation $r(\varepsilon, \beta) = 1$, in view of $s_\varepsilon = 1$; and since φ maps R into A homomorphically,

$$\bar{\varphi}(\varepsilon, \beta) = \varphi\big(r(\varepsilon, \beta)\big) = \varphi(1) = 0.$$

Therefore by (37)

$$\psi(\beta) - \psi(\beta) + \psi(\varepsilon)\beta = \psi(\varepsilon)\beta = 0.$$

Putting $\beta = \varepsilon$, we arrive at (38) because of condition 3) of the definition of a group of operators.

We now define a mapping $f(x)$ of S into A as follows. Every element x of S can be written uniquely in the form

$$x = s_\alpha r, \quad r \in R.$$

We put

$$f(x) = \psi(\alpha) + \varphi(r). \tag{39}$$

If $x \in R$, then $\alpha = \varepsilon$, and from $s = 1$ and (38) we obtain

$$f(r) = \varphi(r) \text{ for } r \in R.$$

It remains to show that *the mapping $f(x)$ is a crossed homomorphism of S into A*. If

$$x = s_\alpha r, \quad y = s_\beta r',$$

then by (26)

$$xy = s_{\alpha\beta}\left[r(\alpha, \beta)(s_\beta^{-1} r s_\beta) r'\right].$$

Therefore, using (39), (37), (27), (23), and (21), we obtain

$$f(xy) = \psi(\alpha\beta) + \varphi[r(\alpha, \beta)(s_\beta^{-1} r s_\beta) r'] =$$
$$= \psi(\beta) + \psi(\alpha)\beta - \bar{\varphi}(\alpha, \beta) + \varphi\big(r(\alpha, \beta)\big) + \varphi(s_\beta^{-1} r s_\beta) + \varphi(r') =$$
$$= \psi(\beta) + \psi(\alpha)\beta + \varphi(r)\beta + \varphi(r') = f(y) + f(x)\beta =$$
$$= f(y) + f(x)y.$$

On comparing this with (24) we see that $f(x)$ is, in fact, a crossed homomorphism.

This completes the proof of MacLane's Theorem.

§ 51. Extensions of non-commutative groups

We now pass on to a survey of the extensions of a *non-commutative* group A by means of a group B. We shall follow a paper by Eilenberg and MacLane [5]. As we have shown at the end of § 48 we can confine ourselves here to the consideration of extensions associated with a given homomorphism θ of B into $\mathfrak{A}$, the group of automorphism classes of A.

However, not every homomorphism of B into $\mathfrak{A}$ is associated with some extension of A by B (for an example, see Baer [4]) and we begin by establishing conditions under which this will hold.

Let θ be an arbitrary homomorphism of B into $\mathfrak{A}$. In every automorphism class $\theta(\alpha)$, $\alpha \in B$, we select an automorphism φ_α. The automorphisms $\varphi_\alpha\varphi_\beta$ and $\varphi_{\alpha\beta}$ lie in the same automorphism class; therefore $\varphi_{\alpha\beta}^{-1}\varphi_\alpha\varphi_\beta$ is an inner automorphism and is induced by some element $h(\alpha, \beta)$ of A.

Let the symbol $< a >$ denote the inner automorphism of A induced by the element a. Thus

$$\varphi_\alpha\varphi_\beta = \varphi_{\alpha\beta} < h(\alpha, \beta) >. \tag{40}$$

Using the associative law for the multiplication of automorphisms and taking into account that for an arbitrary automorphism φ of A and any element a of A the equation

$$\varphi^{-1} < a > \varphi = < a\varphi > \tag{41}$$

holds, we consider the product $\varphi_\alpha\varphi_\beta\varphi_\gamma$ and arrive at the equation

$$< h(\alpha, \beta\gamma)\, h(\beta, \gamma) > = < h(\alpha\beta, \gamma) \cdot h(\alpha, \beta)\, \varphi_\gamma >.$$

Elements that induce the same inner automorphism differ from one another

by an element of the center. There therefore exists an element $z(\alpha, \beta, \gamma)$ in the center Z of A such that

$$h(\alpha, \beta\gamma)\, h(\beta, \gamma)\, z(\alpha, \beta, \gamma) = h(\alpha\beta, \gamma) \cdot h(\alpha, \beta)\, \varphi_\gamma. \tag{42}$$

We have obtained a three-dimensional cochain $z(\alpha, \beta, \gamma)$ of B in the abelian group Z. We could prove that this cochain is actually a cocycle, but this is not essential for the argument.

The cochain $z(\alpha, \beta, \gamma)$ depends on the choice of the automorphism φ_α and on the element $h(\alpha, \beta)$. Let us show that *the coset of $D^3(B, Z)$ in $C^3(B, Z)$ in which this cochain lies is uniquely determined by the automorphism θ alone.*

Suppose, then, that the elements $h(\alpha, \beta)$ are replaced by elements $h'(\alpha, \beta)$ that induce the same inner automorphism of A. Then there exist elements $f(\alpha, \beta)$ in the center of A such that

$$h'(\alpha, \beta) = h(\alpha, \beta) f(\alpha, \beta).$$

If we now calculate, by formula (42), the cochain $z'(\alpha, \beta, \gamma)$ corresponding to the elements $h'(\alpha, \beta)$, we obtain

$$z'(\alpha, \beta, \gamma) = [f^{-1}(\beta, \gamma) f^{-1}(\alpha, \beta\gamma) f(\alpha\beta, \gamma) \cdot f(\alpha, \beta)\, \varphi_\gamma]\, z(\alpha, \beta, \gamma).$$

By (18) the expression in brackets is the coboundary of the two-dimensional cochain $f(\alpha, \beta)$, so that the cochains z and z' lie in the same coset of $D^3(B, Z)$. Note that $f(\alpha, \beta)$ is an arbitrary two-dimensional cochain of B in Z, so that *we can obtain as $z'(\alpha, \beta, \gamma)$ every cochain of the coset of $D^3(B, Z)$ in which $z(\alpha, \beta, \gamma)$ lies.*

Suppose, further, that the automorphisms φ_α are replaced by automorphisms φ_α' lying in the same automorphism classes $\theta(\alpha)$. There then exist elements k_α in A such that

$$\varphi_\alpha' = \varphi_\alpha < k_\alpha >. \tag{43}$$

Then, by (40) and (41),

$$\varphi_\alpha' \varphi_\beta' = \varphi_{\alpha\beta} < h(\alpha, \beta)\, (k_\alpha \varphi_\beta)\, k_\beta > = \varphi_{\alpha\beta}' < k_{\alpha\beta}^{-1} h(\alpha, \beta)\, (k_\alpha \varphi_\beta)\, k_\beta >.$$

Since by what we have shown above the choice of elements $h'(\alpha, \beta)$ is at our disposal, we put

$$h'(\alpha, \beta) = k_{\alpha\beta}^{-1} h(\alpha, \beta)\, (k_\alpha \varphi_\beta)\, k_\beta,$$

and hence by (43)

$$k_{\alpha\beta} h'(\alpha, \beta) = h(\alpha, \beta)\, k_\beta\, (k_\alpha \varphi_\beta'). \tag{44}$$

We use this last equation several times, taking as α and β first the elements $\alpha\beta$ and γ, then α and β themselves, then β and γ, and so on, and we also take into account (43), (40), and (42); we thus obtain

$$\begin{aligned}
k_{\alpha\beta\gamma}h'(\alpha\beta,\gamma)[h'(\alpha,\beta)\varphi'_\gamma] &= h(\alpha\beta,\gamma)k_\gamma[k_{\alpha\beta}h'(\alpha,\beta)]\varphi'_\gamma = \\
&= h(\alpha\beta,\gamma)k_\gamma[h(\alpha,\beta)k_\beta(k_\alpha\varphi'_\beta)]\varphi'_\gamma = \\
&= h(\alpha\beta,\gamma)(h(\alpha,\beta)\varphi_\gamma)k_\gamma[k_\beta(k_\alpha\varphi'_\beta)]\varphi'_\gamma = \\
&= h(\alpha,\beta\gamma)h(\beta,\gamma)z(\alpha,\beta,\gamma)k_\gamma(k_\beta\varphi'_\gamma)(k_\alpha\varphi'_\beta\varphi'_\gamma) = \\
&= h(\alpha,\beta\gamma)k_{\beta\gamma}h'(\beta,\gamma)(k_\alpha\varphi'_\beta\varphi'_\gamma)z(\alpha,\beta,\gamma) = \\
&= h(\alpha,\beta\gamma)k_{\beta\gamma}(k_\alpha\varphi'_{\beta\gamma})h'(\beta,\gamma)z(\alpha,\beta,\gamma) = \\
&= k_{\alpha\beta\gamma}h'(\alpha,\beta\gamma)h'(\beta,\gamma)z(\alpha,\beta,\gamma).
\end{aligned}$$

Hence

$$h'(\alpha\beta,\gamma)[h'(\alpha,\beta)\varphi'_\gamma] = h'(\alpha,\beta\gamma)h'(\beta,\gamma)z(\alpha,\beta,\gamma);$$

in other words, with our choice of the elements $h'(\alpha,\beta)$ the cochain $z(\alpha,\beta,\gamma)$ remains unchanged. Together with what we have shown above, this completes the proof.

A homomorphism θ of B into $\mathfrak{A}$ is associated with an extension of A by B if and only if the coset of $D^3(B,A)$ that contains the cochain $z(\alpha,\beta,\gamma)$ defined by (42) is the coset $D^3(B,A)$ itself.

For suppose there is an extension G of A by B associated with θ. For a definite choice of the coset representatives of A this extension is defined by a factor system $m_{\alpha,\beta}$ and a system of automorphisms $a \to a^\alpha$ satisfying conditions (1) and (2). We can take for the automorphisms φ_α the automorphisms $a \to a^\alpha$, and for the elements $h(\alpha,\beta)$ the factors $m_{\alpha,\beta}$. From (1) it follows that (40) holds, and (2) shows that we must put

$$z(\alpha,\beta,\gamma) = 1 \text{ for all } \alpha,\beta,\gamma \in B \tag{45}$$

in (42). This proves the first part of the theorem.

Conversely, suppose that the homomorphism θ is such that the chain $z(\alpha,\beta,\gamma)$ obtained by some choice of the automorphisms φ_α and of the elements $h(\alpha,\beta)$ belong to $D^3(B,Z)$. We have seen above that by changing the elements $h(\alpha,\beta)$, if necessary, we can obtain an arbitrary element of $D^3(B,Z)$ as $z(\alpha,\beta,\gamma)$ and, in particular, the chain (45). In the latter case, however, (40) and (41) turn into (1) and (2); that is, there exists an extension of A by B given by the factor system $h(\alpha,\beta)$ and the system of automorphisms φ_α. This extension is obviously associated with the homomorphism θ.

We shall now give a survey of the non-equivalent extensions of A by B associated with θ. To begin with, we remark that, since every automorphism of A induces an automorphism of the center Z of A and since automorphisms in the same automorphism class of A induce the same automorphism of Z, the automorphism θ makes B into a group of operators for Z.

Suppose there exist extensions of A by B associated with θ. We show that *there exists a one-to-one correspondence between all non-equivalent extensions of A by B associated with θ and all non-equivalent extensions of the center Z of A by the group of operators B corresponding to the homomorphism θ*. The problem that interests us is thus reduced to results of the preceding two sections.

Let G be one of the extensions of A by B associated with θ, and let H be an arbitrary extension of Z by the group of operators B. We consider all the possible pairs

$$(g, h),\ g \in G,\ h \in H,$$

subject to the condition that *the cosets gA and hZ correspond to one and the same element α of B*.

The operation

$$(g, h)(g', h') = (gg', hh')$$

turns the set of all such pairs into a group, which we denote by $\tilde{G}$. The pairs of the form (a, z), $a \in A$, $z \in Z$, form a normal subgroup $\tilde{A}$ of G, and the pairs of the form (z, z^{-1}), $z \in Z$, a normal subgroup N.

The group

$$G' = \tilde{G}/N$$

has a normal subgroup $A' = \tilde{A}/N$, which is isomorphic to A, because one and only one element of the form $(a, 1)$ is contained in every coset of N in $\tilde{A}$. The factor group

$$B' = G'/A' \simeq \tilde{G}/\tilde{A}$$

is isomorphic to B: if (g, h) is an element of $\tilde{G}$, then the coset $(g, h)\tilde{A}$ will contain precisely the elements of the form (g_1, h_1), where $g_1 \in gA$, $h_1 \in hZ$. By associating with the coset $(g, h)\tilde{A}$ that element α of B which corresponds to the cosets gA and hZ, we obtain an isomorphism between B' and B. *G' is therefore an extension of A by B.*

Suppose that the extension G of A is given in terms of the representa-

tives g_α of the cosets of A by the factor system $m_{\alpha,\beta}$ and the automorphisms $a \to a^\alpha$ (see § 48), and that the extension H of Z in terms of the representatives h_α of the cosets of Z is given by the factor system $n_{\alpha,\beta}$; the automorphisms are in this case determined by the fact that B is a group of operators. From what we have shown above, it follows that we can choose the elements

$$g'_\alpha = (g_\alpha, h_\alpha)N \tag{46}$$

as representatives of the cosets of A in G'.

Let us find the factors and automorphisms defining the extension G' for this choice of representatives.

$$g'_\alpha g'_\beta = (g_\alpha, h_\alpha)N \cdot (g_\beta, h_\beta)N = (g_\alpha g_\beta, h_\alpha h_\beta)N =$$
$$= (g_{\alpha\beta} m_{\alpha,\beta}, h_{\alpha\beta} n_{\alpha,\beta})N = (g_{\alpha\beta}, h_{\alpha\beta})N \cdot (m_{\alpha,\beta}, n_{\alpha,\beta})N.$$

However, $(n_{\alpha,\beta}, n_{\alpha,\beta}^{-1})$ belongs to N, so that

$$(m_{\alpha,\beta}, n_{\alpha,\beta})N = (m_{\alpha,\beta} n_{\alpha,\beta}, 1)N,$$

which corresponds to the element $m_{\alpha,\beta} n_{\alpha,\beta}$ of A. Thus, the elements

$$m'_{\alpha,\beta} = m_{\alpha,\beta} n_{\alpha,\beta} \tag{47}$$

form the required factor system. On the other hand, by transforming the element α of A, that is, the coset $(a, 1)N$, by g_α', we obtain

$$(g_\alpha^{-1}, h_\alpha^{-1})N \cdot (a, 1)N \cdot (g_\alpha, h_\alpha)N = (a^\alpha, 1)N = a^\alpha. \tag{48}$$

The automorphism induced in A by the element g_α' of the extension G' therefore coincides with the automorphism induced in A by the element g_α of the extension G. It follows, in particular, that G' *is associated with the same homomorphism* θ *as* G.

Since the extension G' of A is completely determined by the extension G of A and the extension H of Z, we introduce the following notation for G':

$$G' = (G, H). \tag{49}$$

Taking G as fixed, we shall now show that *every extension* G' *of* A *by* B, *associated with* θ, *is equivalent to an extension of the form* (G, H) *for a suitable choice of the extension* H *of* Z *by the group of operators* B.

For since G' is associated with θ, the representatives g_α' of the cosets of A can be so chosen that the automorphisms induced by them in A are the

same as the automorphisms $a \to a^{\alpha}$ induced by the elements g_{α} of G. Suppose that with this choice of representatives the factor system for G' is formed by the elements $m'_{\alpha,\beta}$. It follows from (1) that the elements $m_{\alpha,\beta}$ and $m'_{\alpha,\beta}$ induce the same inner automorphism of A, in other words, that they differ by an element of the center

$$m'_{\alpha,\beta} = m_{\alpha,\beta} n_{\alpha,\beta}, \quad n_{\alpha,\beta} \in Z. \tag{50}$$

Using (2) for the elements $m'_{\alpha,\beta}$ and taking into account that the elements $n_{\alpha,\beta}$ lie in the center of A and that the elements $m_{\alpha,\beta}$ also satisfy (2), we see that the elements $n_{\alpha,\beta}$ satisfy the same equation (2), in other words, that they are a factor system of an extension H of Z by the group of operators B.

Comparing (50) with (47) and taking into account (48) and the fact that the automorphisms corresponding to the extensions G and G' coincide, we find that the extensions G' and (G, H) are equivalent.

To complete the proof of the theorem it now remains to show *that if* H_1 *and* H_2 *are two extensions of* Z *by the group of operators* B, *then the extensions*

$$G'_1 = (G, H_1) \text{ and } G'_2 = (G, H_2)$$

are equivalent if and only if H_1 *and* H_2 *are equivalent.*

Suppose that φ is an equivalent mapping of H_1 onto H_2. Then

$$(g, h_1) \to (g, h_1\varphi) = (g, h_2)$$

is an isomorphic mapping of $\tilde{G}_1$ onto $\tilde{G}_2$ in which $\tilde{A}$, and consequently N, is mapped identically onto itself. From this we easily deduce the equivalence of the extensions G_1' and G_2'.

Suppose, conversely, that an equivalent mapping ψ of G_1' onto G_2' is given. Let G be given, as before, by the factor system $m_{\alpha,\beta}$ and the system of automorphisms $a \to a^{\alpha}$, and H_i, $i = 1, 2$, by the factor systems $n^{(i)}_{\alpha,\beta}$. Then we know that the extensions G_i', $i = 1, 2$, are given in accordance with (46) in terms of the representatives $g'_{i\alpha}$ by the same system of automorphisms $a \to a^{\alpha}$ and, by (47), by the factor systems $m_{\alpha,\beta} n^{(i)}_{\alpha,\beta}$.

Since ψ is an equivalent isomorphism, the elements $g'_{1\alpha}\psi$ and $g'_{2\alpha}$ lie in the same coset of A, so that

$$g'_{1\alpha}\psi = g'_{2\alpha} b_{\alpha}, \quad b_{\alpha} \in A. \tag{51}$$

We know that for arbitrary a of A

$$ag'_{1\alpha} = g'_{1\alpha}a^{\alpha}.$$

Applying the mapping ψ to this equation and taking (51) into account, we obtain

$$ag'_{2\alpha}b_{\alpha} = g'_{2\alpha}b_{\alpha}a^{\alpha}.$$

However

$$ag'_{2\alpha} = g'_{2\alpha}a^{\alpha},$$

so that

$$g'_{2\alpha}a^{\alpha}b_{\alpha} = g'_{2\alpha}b_{\alpha}a^{\alpha},$$

and hence

$$a^{\alpha}b_{\alpha} = b_{\alpha}a^{\alpha}.$$

But the element a^{α} ranges over the whole group A as a does; therefore b_{α} lies in the center,

$$b_{\alpha} \in Z. \tag{52}$$

We know, further, that

$$g'_{1\alpha}g'_{1\beta} = g'_{1,\alpha\beta}m_{\alpha,\beta}n^{(1)}_{\alpha,\beta}.$$

Applying the mapping ψ to this equation and taking (51) into account, we find

$$g'_{2\alpha}b_{\alpha}g'_{2\beta}b_{\beta} = g'_{2,\alpha\beta}b_{\alpha\beta}m_{\alpha,\beta}n^{(1)}_{\alpha,\beta}.$$

However

$$g'_{2\alpha}g'_{2\beta} = g'_{2,\alpha\beta}m_{\alpha,\beta}n^{(2)}_{\alpha,\beta},$$

and therefore, since $b_{\alpha\beta} \in Z$

$$b^{\beta}_{\alpha}b_{\beta} = b_{\alpha\beta}n^{(2)\,-1}_{\alpha,\beta}n^{(1)}_{\alpha,\beta}.$$

Going over to the additive notation in Z we see that the difference of the cycles $n^{(1)}_{\alpha,\beta}$ and $n^{(2)}_{\alpha,\beta}$ is the boundary of the one-dimensional chain b_{α}, and as we know from § 49, this implies the equivalence of the extension H_1 and H_2. This completes the proof of the theorem.

§ 52. Special cases

The classification that we have obtained in the preceding sections of non-equivalent extensions of a group A by means of a group B is simplified considerably when restrictions of one kind or another are imposed on A or B or on the extensions to be examined.

Central extensions. An extension G of an abelian group A by a group B is called *central* if A lies in the center of G. This is equivalent to saying that

the automorphisms $a \to a^{\alpha}$ of A corresponding to this extension in the sense of § 48 are all equal to the identity. In other words (see the beginning of § 49), the central extensions of an abelian group A by a group B are those extensions that we obtain by considering B as a group of operators for A satisfying the conditions

$$a\alpha = a \tag{53}$$

for all a of A and all α of B. We can therefore speak of the *group of central extensions.*

Let us apply the theory of § 50 to this case, in which B is considered as being expressed in the form

$$B = S/R,$$

where S is a free group. Equation (21) now turns into

$$ax = a, \quad a \in A, \quad x \in S,$$

and the operator homomorphism φ of R into A is, by (23), defined by

$$\varphi(x^{-1}rx) = \varphi(r), \qquad r \in R, \qquad x \in S.$$

It therefore maps all the elements of R that are conjugate in S into the same element; in other words, it carries every commutator of the form $r^{-1}x^{-1}rx$. into the null element. Finally, (24) shows that the crossed homomorphisms of S in A are simply homomorphisms. We therefore have the following theorem.

THEOREM. *The group of central extensions of an abelian group A by means of a group B expressed in the form S/R, where S is a free group, is isomorphic to the factor group U/V, where U is the group of those homomorphisms of R into A that map the commutator group $[R, S]$ into the null element and V is the subgroup of those homomorphisms of R into A that are induced by the homomorphisms of S into A.*

In connection with central extensions see also Baer [32].

Abelian extensions. Not every central extension of an abelian group A by another abelian group B is abelian; this follows from the existence of nilpotent groups of class 2. Let us see how to single out the abelian extensions from the group of all central extensions of A by B.

We know that the central extensions of A by B are determined by the identity automorphisms and by factor systems $m_{\alpha,\beta}$. If B is abelian, then

it follows from (3) that *the extension G is abelian if and only if the factor system $m_{\alpha,\beta}$ is symmetrical, that is,*

$$m_{\alpha,\beta} = m_{\beta,\alpha} \quad \textit{for all } \alpha, \beta \textit{ of } B.$$

Symmetrical factor systems obviously form a subgroup of the group $F(A, B)$ of all factor systems (see the beginning of § 49). Moreover, by (53) and the commutative law in B, equation (9) shows that in our case the subgroup $T(A, B)$ consists of symmetric factor systems. In view of this we can say that *non-equivalent abelian extensions of a group A by a group B form a subgroup of the group of all central extensions of A by B.*

Let us find this group of abelian extensions, making use of the characterization of central extensions obtained above. Let the abelian group B be represented as a factor group S_0/R_0 of a free abelian group S_0. We take the free non-commutative group S with the same free generators as S_0. Then

$$B = S/R,$$

and if S' is the derived group of S, then $S' \subseteq R$ and

$$S/S' = S_0, \qquad R/S' = R_0. \tag{54}$$

The beginning of the proof of the theorem in § 50 shows that we have to select the elements of $Q(R, A; S)$ which, in the mapping (28), go over into a cycle $\overline{\varphi}(\alpha, \beta)$ with the property

$$\overline{\varphi}(\alpha, \beta) = \overline{\varphi}(\beta, \alpha). \tag{55}$$

We keep in mind here that $Q(R, A; S)$ now consists of those homomorphisms of R into A which map the commutator group $[R, S]$ into the null element.

If coset representatives s_α of R in S are chosen in accordance with (25), then (26) is satisfied and we also have

$$s_\beta s_\alpha = s_{\beta\alpha} r(\beta, \alpha).$$

Since now $\alpha\beta = \beta\alpha$, we obtain

$$s_\alpha^{-1} s_\beta^{-1} s_\alpha s_\beta = r^{-1}(\beta, \alpha) r(\alpha, \beta).$$

Let φ be an arbitrary element of $Q(R, A; S)$. Then by (27) and the commutative law in the group A, which we regard as written additively,

$$\varphi(s_\alpha^{-1} s_\beta^{-1} s_\alpha s_\beta) = \overline{\varphi}(\alpha, \beta) - \overline{\varphi}(\beta, \alpha).$$

Thus (55) is satisfied if and only if the homomorphism φ maps every commutator of the form $s_\alpha^{-1}s_\beta^{-1}s_\alpha s_\beta$ into the null element. The homomorphisms φ with these properties form a subgroup of $Q(R, A; S)$, which we denote by $\bar{Q}(R, A; S)$.

If φ belongs to $\bar{Q}(R, A; S)$ then it maps altogether every commutator $x^{-1}y^{-1}xy$ of S, that is, the whole derived group S', into the null element. For if

$$x = s\,r_1, \quad y = s_\beta r_2, \qquad r_1,\ r_2 \in R,$$

then

$$x^{-1}y^{-1}xy = r_1^{-1}s_\alpha^{-1}r_2^{-1}s_\beta^{-1}s_\alpha r_1 s_\beta r_2 = r_1^{-1}(s_\alpha^{-1}r_2^{-1}s_\alpha)(s_\alpha^{-1}s_\beta^{-1}s_\alpha s_\beta)(s_\beta^{-1}r_1 s_\beta)r_2.$$

Taking into account that φ, by assumption, maps $[R, S]$ as well as $s_\alpha^{-1}s_\beta^{-1}s_\alpha s_\beta$ into the null element, we find that

$$\varphi(x^{-1}y^{-1}xy) = -\varphi(r_1) - \varphi(r_2) + \varphi(r_1) + \varphi(r_2) = 0.$$

Thus, $\bar{Q}(R, A; S)$ consists of all the homomorphisms of R into A that map S' into the null element. On the other hand, every element of $Q'(R, A; S)$ obviously maps the whole group S' into the null element. Thus, *the group of abelian extensions of A by B is isomorphic to the factor group of $\bar{Q}(R, A; S)$ with respect to $Q'(R, A; S)$*; making use of (54) we arrive at the following final result (Eilenberg and MacLane [1]).

The group of abelian extensions of an abelian group A by an abelian group B, expressed in the form of a factor group S_0/R_0 of a free abelian group S_0, is isomorphic to the factor group of the group of all homomorphisms of R_0 into A with respect to all those homomorphisms that are induced by the homomorphisms of S_0 into A.

Extensions of groups without center. Let A be a group without center, that is, $Z = E$. If θ is an arbitrary homomorphism of B into the group $\mathfrak{A}$ of automorphism classes of A, then the theorem of § 51 shows that this homomorphism is always associated with an extension of A by B, because it follows from $Z = E$ that the chain $z(\alpha, \beta, \gamma)$ can only be null.

On the other hand, there exists only one extension of the unit group by means of B, namely B itself, and therefore by § 51 only one extension of A by B associated with the given homomorphism θ. So we have arrived at the following result:

The non-equivalent extensions of a group A without center by a group stand in one-to-one correspondence with the distinct homomorphisms of B into the group $\mathfrak{A}$ of automorphism classes.

Splitting extensions. Suppose G is an extension of a group A by a group B such that we can choose, in the cosets gA, representatives g_α, $\alpha \in B$, with the property

$$g_\alpha g_\beta = g_{\alpha\beta},$$

that is,

$$m_{\alpha,\beta} = 1.$$

The representatives g_α then form a subgroup B' of G, isomorphic to B; moreover, the subgroups A and B' generate the whole group G, and their intersection is E. Such an extension G is said to be *splitting*; we also say that G is a *semi-direct* product of the normal subgroup A and the subgroup B'. Among the splitting extensions there is, of course, the direct product of A and B.

Non-equivalent splitting extensions of an abelian group A by a group B stand in one-to-one correspondence with the distinct homomorphisms of B into the group of automorphisms of A.

For we have shown in § 49 that for an abelian group A with a group of operators B there exists an extension defined by the factor system $m_{\alpha,\beta} = 1$.

Every extension G of an arbitrary group A by means of a free group B is a splitting extension.

For if we choose arbitrary representatives of those cosets of A in G that correspond to free generators of B and then determine representatives of all the other cosets in the natural way, we obtain the required decomposition of G.

PART FOUR

SOLVABLE AND NILPOTENT GROUPS

CHAPTER XIII

FINITENESS CONDITIONS, SYLOW SUBGROUPS, AND RELATED PROBLEMS

§ 53. Finiteness conditions

Many theorems that were first proved for finite groups have been successfully extended to much wider classes of groups. Restrictions of one kind or another are usually imposed on the groups in question but restrictions much weaker than the finiteness of the number of elements. We begin by giving a survey of such *finiteness conditions*, but we shall confine ourselves to those most frequently used.

A very weak finiteness condition is *periodicity of the group*. Occasionally it is necessary to replace it by a restriction that is possibly stronger, namely, the condition of local finiteness: a group is called *locally finite* if every finite subset of the group generates a finite subgroup.

It is obvious that a locally finite group is periodic; the problem of whether the converse is true is another formulation of Burnside's problem (see § 38). In the following chapters the reader will become acquainted with several theorems in which the local finiteness of periodic groups is proved under various additional restrictions; for abelian groups the two conditions are obviously equivalent.

The following theorem (Schmidt [7]) will be used in the sequel.

An extension G of a locally finite group A by a locally finite group B is itself locally finite.

That G is periodic, is obvious. Suppose that M is a finite set of elements $x_1, x_2, \ldots, x_n$ of G. From the local finiteness of B it follows that H/A is finite, where

$$H = \{A, M\}.$$

We shall assume that every coset of A in H contains at least one element of M; for this purpose it may be necessary to supplement M by a finite number of elements. Every product $x_i x_j$ lies in one of the cosets of A in H and can therefore be represented in at least one way as a product of an element of M by an element of A. For every pair of subscripts i, j we choose one such representation

$$x_i x_j = x_k a_{ij}, \qquad a_{ij} \in A.$$

Since G is periodic, every element of the subgroup $\{M\}$ can be represented as a product of elements x_i with exponents $+1$, and therefore also as a product of elements of M by an element which is a product of elements of the form a_{ij}, in other words, by an element of the subgroup generated by all the elements a_{ij}. The latter subgroup, however, is finite, because A is locally finite and the number of elements a_{ij} is finite. Hence there follows the finiteness of $\{M\}$, that is, the local finiteness of G.

A much more stringent condition than local finiteness is that of local normality: a group G is called *locally normal* if every finite subset is contained in a finite normal subgroup of G. In § 55 we shall come across groups of this type.[1]

Closely related to locally normal groups are the groups in which all classes of conjugate elements are finite, which we call, for brevity, *groups with finite classes*. To this type of groups belong not only all finite groups, but also all abelian groups.[n]

The following theorem holds.

Every periodic group with finite classes is locally normal, and conversely.

That a locally normal group is also periodic, and that every one of its elements lies in a finite class of conjugates, is clear. The direct part of the theorem follows from the following Lemma of Dicman [Dietzmann] [1].

DIETZMANN'S LEMMA: *If $\mathfrak{M}$ is a finite normal subset of an arbitrary group G consisting of elements of finite order, then the subgroup $\{\mathfrak{M}\}$ generated by it is also finite.*[2]

For suppose that $\mathfrak{M}$ consists of k elements, that m is the least common multiple of the orders of all the elements of $\mathfrak{M}$, and that $A = \{\mathfrak{M}\}$. Every element of A can be expressed as a product of elements of $\mathfrak{M}$. For the proof of the lemma it is sufficient to show that for every element a of A among these expressions there is one that consists of not more than $k(m-1)$ factors.

Suppose that we have some expression

$$a = a_1 a_2 \dots a_l, \quad a_i \in \mathfrak{M}, \quad i = 1, 2, \dots, l, \tag{1}$$

and that $l > k(m-1)$. In this case at least one of the elements of $\mathfrak{M}$, say a_0, occurs in (1) not fewer than m times. If a_i is the first element in (1)

[1] It would be more in keeping with the systematic terminology if groups of this class were called *locally finite and normal*. [*Trans.*]

[2] A subset of a group is called *normal* or *self-conjugate* if it consists of complete classes of conjugate elements of the group. [*Trans.*]

equal to a_0, then putting $a_0^{-1}a_j a_0 = a_j'$, we obtain

$$a = a_0 a_1' \cdots a_{i-1}' a_{i+1} \cdots a_l,$$

where $a_j' \in \mathfrak{M}$, because $\mathfrak{M}$ is normal. Applying this device to the first element among $a_{i+1}, \ldots, a_l$ that is equal to a_0, and then to the first of the remaining elements, and so on, we arrive, after a finite number of steps, at an expression for a in terms of the elements of $\mathfrak{M}$

$$a = a_0^m \bar{a}_1 \bar{a}_2 \cdots \bar{a}_{l-m},$$

which, because of $a_0^m = 1$, leads to an expression with $l - m$ factors. This proves that A is finite.

In order to deduce the above theorem from Dietzmann's Lemma it only remains to remark that a normal subset generates a normal subgroup and that in a group with finite classes every finite subset is contained in a finite normal subset.

Next we mention the condition of finiteness of the layers. A group is said to have *finite layers* if it contains only a finite number of elements of any given order. A group with finite layers cannot contain elements of infinite order (because it would then contain infinitely many), and it is therefore periodic. Moreover, every element of such a group can have only a finite number of conjugates. By the preceding theorem we now have: *Every group with finite layers is locally normal.*

A paper by Černikov [12] gives an almost exhaustive survey of the groups with finite layers. Some of their properties are also mentioned in a paper by Baer [40].

A number of finiteness conditions refer to the lattice of subgroups of the groups in question. The most important among them is the *minimal condition for subgroups*, that is, the condition that all descending chains of subgroups break off. Every group with this property is periodic, because an infinite cyclic group does not satisfy the minimal condition. However, it is not yet known *whether groups with minimal condition for subgroups are locally finite* nor *whether they are countable.*

If in a group G a normal subgroup N and its factor group G/N are groups with minimal condition, then G itself satisfies the minimal condition.

For let A and B be subgroups of G; where $A \subseteq B$, and $A \cap N = B \cap N$, $AN = BN$. If b is an arbitrary element of B, then from $b \in AN$ we have $b = ax$, where $a \in A$, $x \in N$. Hence $x = a^{-1}b \in B$, that is, $x \in (B \cap N)$, and therefore $x \in (A \cap N) \subseteq A$. Thus we have shown that $b = ax \in A$, so that

$A = B$. Therefore if an infinite decreasing chain of subgroups exists in G, then such a chain also exists in at least one of the groups N and G/N: if a chain of subgroups

$$A_1 \supset A_2 \supset \ldots \supset A_k \supset \ldots,$$

is given, then an infinite number of distinct terms must occur either in the chain of intersections of these subgroups with N or in the chain of subgroups of G/N that correspond to the products of the given groups with N.

From this theorem it follows that *the direct product of two or, more generally, any finite number of groups with minimal condition is itself a group with minimal condition.* Obviously, no subgroup of a group with minimal condition can be the direct product of an infinite number of groups.

Every abelian group with minimal condition is the direct product of a finite abelian group and a finite number of groups of type p^∞ for prime numbers p, not necessarily distinct. Conversely, every such direct product satisfies the minimal condition.

The second part of the theorem follows from the above remark about direct products, because all proper subgroups of a group of type p^∞ are finite (see § 7), and such a group therefore satisfies the minimal condition. For the proof of the first part, we decompose the abelian group G with minimal condition, as a periodic abelian group, into the direct product of a finite number of primary groups. In § 25 we showed that a primary abelian group either is decomposable into the direct product of finite cyclic groups and of groups of type p^∞ or else cannot be decomposed at all into the direct product of indecomposable groups so that every one of its direct decompositions contains at least one decomposable factor. For groups with minimal condition this latter case cannot arise, because it leads to an infinite descending chain of subgroups; therefore only the first case remains, and the number of direct factors must be finite.

The maximal condition for subgroups is also used frequently, that is, the condition that all ascending chains of subgroups break off. *This condition is equivalent to the assumption that the group itself and all its subgroups have finite numbers of generators.* For suppose that all ascending chains of subgroups of a group G break off, and let A be a subgroup of G. We choose an element a_1 in A and denote its cyclic subgroup by A_1. Suppose we have already chosen a finitely generated subgroup A_n in A. If it is distinct from A, then we choose an element a_{n+1} in A, but outside A_n, and put $A_{n+1} = \{A_n, a_{n+1}\}$. The ascending chain of subgroups

$$A_1 \subset A_2 \subset \ldots \subset A_n \subset \ldots$$

must break off; that is, for some n we must have $A_n = A$. Hence it follows that A is finitely generated. Conversely, if there exists an infinite ascending chain of subgroups of G, $B_1 \subset B_2 \subset \ldots \subset B_n \subset \ldots$, then we know from § 7 that the union of this chain cannot have a finite system of generators.

By analogy with the minimal and maximal conditions for subgroups we can introduce the very much weaker *minimal and maximal conditions for normal subgroups*. Groups with minimal condition for normal subgroups are studied in a paper by Baer [41]. For certain special types of groups the minimal condition for subgroups can be deduced from the minimal condition for normal subgroups—see Jennings [1], Ado [3], Černikov [11], Gluškov [4].°

The condition of being *finitely generated* can also be regarded as a finiteness condition; groups with this property have been studied in Chapter X. We also mention the condition that *the number of classes of conjugates is finite*. But groups of this type can have a very complicated structure, as the following theorem shows (G. Higman, B. H. Neumann and Hanna Neumann [1]).

Every torsion-free group G can be embedded in a torsion-free group in which all the elements other than the unit element are conjugate, so that the group has only two classes of conjugates.

Applying Lemma 2 of § 38 we embed G in a group G' generated by G and by elements $h_{a,b}$ for all ordered pairs a, b of elements of G other than 1, where

$$h_{a,b}^{-1} a h_{a,b} = b.$$

In G' all the elements of G other than the unit element are conjugate. G' is also torsion-free, since the elements $h_{a,b}$ generate a free subgroup of G' so that G' is an extension of a torsion-free group by a torsion-free group. Applying the same construction to G' and proceeding further, we obtain an ascending sequence of torsion-free groups

$$G \subset G' \subset G'' \subset \ldots \subset G^{(n)} \subset \ldots,$$

whose union satisfies the conditions of the theorem.

We mention, finally, the condition of *finiteness of the rank*, introduced by Mal'cev [4].

A group G has finite *general rank* r if r is the smallest number with the property that every finite set of elements of G *is contained in* a subgroup with no more than r generators.

A group G has finite *special rank* r if r is the smallest number with the property that every finite set of elements of G *generates* a subgroup with no more than r generators.

It is clear that *the general rank of a group is less than, or equal to, its special rank*. The restricted countable symmetric group (see § 4) is an example of a group with finite general rank; the rank is 2, because every finite set of elements of the group is contained in a finite symmetric subgroup, that is, a subgroup with two generators, while the special rank is infinite. Indeed, every finite group whatsoever is contained in the restricted countable symmetric group, but the minimal number of generators of finite groups is not bounded.

For abelian groups the general and special ranks coincide, since every subgroup of an abelian group with n generators has not more than n generators. For torsion-free abelian groups these ranks are equal to rank in the sense of § 19.

§ 54. Sylow subgroups. The centers of p-groups

Among the many theorems on finite groups that derive deep properties of the groups from arithmetic properties of their orders, one of the most important is *Sylow's First Theorem*:

SYLOW'S FIRST THEOREM: *If the order n of a finite group G is divisible by the k-th power of a prime number p, then G has a subgroup of order p^k.*

We shall prove this theorem by induction on n; it is obvious for $n = 1$. We can assume that $k > 0$.

If the order of the center of G is divisible by p, then it follows from the fundamental theorem on finite abelian groups (§ 20) that the center of G contains an element a of order p, and the cyclic subgroup $\{a\}$ is normal in G. The factor group $G/\{a\}$ has order n/p, which is divisible by p^{k-1}, and therefore, by the induction hypothesis, it contains a subgroup of order p^{k-1}. To this subgroup there corresponds in G a subgroup of order p^k.

If the order of the center is not divisible by p, then we proceed as follows: We divide the elements of G outside the center into distinct classes of conjugates and denote the number of elements in these classes by $l_1, l_2, \ldots, l_s$. If c is the order of the center, $c \geqq 1$, then

$$n = c + \sum_{i=1}^{s} l_i.$$

Since n is divisible by p and $(c, p) = 1$, at least one of the numbers l_i must also be prime to p. Hence it follows that there exists a proper subgroup N of G (namely the normalizer of one of its elements) whose index is prime to p, so that its order is divisible by p^k. By the induction hypothesis, N has a subgroup of order p^k. This completes the proof of the theorem.

A special case of the theorem (for $k = 1$) is *Cauchy's Theorem.*

CAUCHY'S THEOREM: *If the order of a finite group G is divisible by a prime number p, then G has elements of order p.*

If p^m is the highest power of the prime number p by which the order n of a finite group G is divisible, then it follows from Sylow's first theorem that G has subgroups of order p^m. These subgroups are called the *Sylow p-subgroups* of G.

The Sylow subgroups of finite groups have a number of important properties which we shall now establish for arbitrary (that is, not necessarily finite) groups after appropriately generalizing the concept of a Sylow subgroup (Dietzmann, Kuroš, and Uzkov [1]).

Let Π be a non-empty set of prime numbers, finite or infinite. A periodic group G is called a *Π-group* if all the prime divisors of the order of every element of G belong to Π. If the set Π consists of a single prime number p, then we have the concept of a *p-group*: this is a group in which the orders of all the elements are powers of p. In the case of an abelian group, this concept is the same as that of a p-primary group.

A finite group G is a p-group if and only if its order is a power of p.

For if G is of order p^n, then the order of every element of G is, by Lagrange's Theorem, a divisor of p^n, that is, a power of p. But if the order of G is divisible by a prime number q other than p then, by Cauchy's theorem, G has elements of order q and is therefore not a p-group.

Π-groups that are subgroups of a larger, but not necessarily periodic, group G will be called *Π-subgroups* of G. A special case are the p-subgroups.

A Π-subgroup Q of a group G is called a *Sylow Π-subgroup* of G if it is not contained in any larger *Π-subgroup* of G.

In particular, a *Sylow p-subgroup* of an arbitrary group G is a p-subgroup that is not contained in any larger p-subgroup of G. For finite groups this concept is the same as the one we have introduced above under the same name, in connection with Sylow's first theorem; this will be proved at the end of this section.

From now on we shall take the set Π to be arbitrary but fixed.

Every group has Sylow Π-subgroups.

For if the group contains no Π-subgroups other than E, then E is such a subgroup. But if G has non-trivial Π-subgroups, then let Q_1 be one of them. Suppose that we have already found a well-ordered ascending sequence of Π-subgroups

$$Q_1 \subset Q_2 \subset \ldots \subset Q_\alpha \subset \ldots,$$

where α ranges over all the ordinal numbers less than a certain β. If $\beta - 1$ exists, and if $Q_{\beta-1}$ is not a Sylow Π-subgroup, then it is contained in some larger Π-subgroup, which we denote by Q_β. If β is a limit number, then we can take for Q_β the union of the ascending sequence of subgroups Q_α, $\alpha < \beta$, which is itself a Π-subgroup. This process of constructing an ascending sequence of subgroups must come to an end with some ordinal number whose cardinal number does not exceed the cardinal number of G itself. This proves the existence of Sylow Π-subgroups of G.

Incidentally, we have proved that *every Π-subgroup of G is contained in some Sylow Π-subgroup*. For in the preceding proof we could have taken an arbitrary Π-subgroup as Q_1.

If H is a subgroup of G, then two distinct Sylow Π-subgroups Q_1 and Q_2 of H cannot be contained in a single Π-subgroup of G. For otherwise they would be contained in the intersection of that subgroup with H, which is also a Π-subgroup. Also quite obvious is the following statement: If G is the union of an ascending sequence of groups $H_1, H_2, \ldots, H_n, \ldots$, and if Sylow Π-subgroups Q_n, $n = 1, 2, \ldots$ are chosen, where $Q_m \subseteq Q_n$ for $m < n$, then *the union of the ascending sequence $Q_1, Q_2, \ldots, Q_n, \ldots$ is a Sylow Π-subgroup of G.* We must add, however, that in general (for a given sequence H_n) not every Sylow Π-subgroup of G can be obtained in this way.

We now turn to *the normalizers of Sylow subgroups*, which play an essential rôle in the following. Let A and B be two Π-subgroups of a group G, A being normal in G. Every element of AB has the form ab, where $a \in A$, $b \in B$. If b has order n, then

$$(ab)^n = \bar{a} b^n = \bar{a}, \quad \bar{a} \in A.$$

If, further, $\bar{a}$ has order m, then

$$(ab)^{nm} = \bar{a}^m = 1,$$

so that *AB is also a Π-subgroup*. If B is a Sylow Π-subgroup of G, then

$AB = B$, that is, $A \subseteq B$. Thus we have shown that a normal Π-subgroup of G is contained in every Sylow Π-subgroup of G. *If the normal subgroup in question is itself a Sylow* Π*-subgroup, then it is the only Sylow* Π*-subgroup of* G. That is, since every subgroup is normal in its normalizer we arrive at the following theorem:

Each Sylow Π*-subgroup of an arbitrary group is the only Sylow* Π*-subgroup of its normalizer; in other words, it contains all the elements of the normalizer for which all the prime divisors of the orders belong to* Π.

Further properties of the normalizers of Sylow Π-subgroups are based on the following remark.

Every subgroup of a group G *that is conjugate to a Sylow* Π*-subgroup* Q *of* G *is itself a Sylow* Π*-subgroup. In particular, a Sylow* Π*-subgroup cannot be conjugate to one of its proper subgroups.*

For if $Q' = g^{-1}Qg$ and if Q' is contained in a larger Π-subgroup Q'' of G, then Q is contained in $gQ''g^{-1}$ as a proper subgroup, in contradiction to the definition of a Sylow subgroup.

From this we easily deduce the theorem:

The normalizer of a Sylow Π*-subgroup is its own normalizer.*

For let Q be a Sylow Π-subgroup of a group G, and let N be its normalizer in G. If an element x lies outside N, then $x^{-1}Qx \neq Q$. If nevertheless $x^{-1}Nx = N$, then $x^{-1}Qx \subset N$; this, however, contradicts the fact that a Sylow subgroup of G is the only Sylow subgroup of its normalizer. This shows than an element x outside N cannot be permutable with N.

A fundamental problem in the theory of Sylow subgroups is to find conditions under which all the Sylow Π-subgroups of a given group are conjugate so that they form a single class of conjugate subgroups. We first mention two results that can be obtained under this assumption of conjugacy.

If all the Sylow Π*-subgroups of a group* G *are conjugate and if* A *is a normal subgroup of* G*, then the intersection of* A *with a Sylow* Π*-subgroup* Q *of* G *is a Sylow* Π*-subgroup of* A.

For if $A \cap Q = D$ is not a Sylow Π-subgroup of A, then it is properly contained in a Sylow Π-subgroup D' of A, which in turn lies in a Sylow Π-subgroup Q' of G. By assumption, $g^{-1}Q'g = Q$, $g \in G$, and so $g^{-1}D'g \subseteq Q$; but since A is normal, $g^{-1}D'g \subseteq A$ and $g^{-1}D'g \subseteq D$. Hence it follows that $D' \subseteq gDg^{-1}$, so that $D' \subset gD'g^{-1}$. But since $gD'g^{-1} \subset A$, we arrive at a contradiction to the fact that D' is a Sylow Π-subgroup of A.

If Q *is a Sylow* Π*-subgroup of* G, N *its normalizer in* G, *and* H *a sub-*

group of G containing N, and if all the Sylow Π-subgroups of H are conjugate, then H is its own normalizer in G.

If g is an element of G such that $g^{-1}Hg = H$, then $g^{-1}Qg \subset H$. Therefore, by assumption, H contains an element h such that $h^{-1}g^{-1}Qgh = Q$, and hence $gh \in N$; that is, $gh \in H$ and $g \in H$.

Using the concept of a free product and the theorem on the subgroups of a free product (see § 34) we could construct examples of groups showing that these two theorems cease to be valid without the assumptions on the conjugacy of the Sylow subgroups under which they have been proved.[P] Moreover, as the example of the symmetric group of degree 3 shows, in the first theorem the normal subgroup cannot be replaced by an arbitrary subgroup.

The problem of finding conditions under which the Sylow subgroups of a given group are conjugate will be treated here only for the case of Sylow p-groups; we shall come to Sylow Π-groups in the next chapter.

First of all we prove the following statement about p-groups.

If a p-group G contains a subgroup A of finite index j, then j is a power of p.

For we know from § 11 that under these conditions A contains a normal subgroup D of G, also of finite index. The factor group G/D is a finite p-group, so that by what we have proved above its order is a power of p, say p^n. To A there corresponds in G/D the subgroup A/D, also of index j. Therefore j is a divisor of p^n.

Now we proceed to the proof of the following theorem (Kuroš [15]).

If a group contains a p-subgroup A having a finite number of conjugates, then we can find for every p-subgroup B of G at least one subgroup that is conjugate to A and that generates, together with B, a p-subgroup. If, in addition, none of the subgroups conjugate to A generates, together with A, a p-subgroup, then the number of subgroups conjugate to A is congruent to 1 (modulo p).

Suppose that the subgroups $A^{(1)}, \ldots, A^{(k)}$, conjugate to A, are such that

$$C = \{A, A^{(1)}, \ldots, A^{(k)}\}$$

is a p-subgroup, but that no further subgroup conjugate to A can be added to C without destroying this property. If the assumptions of the second part of the theorem are satisfied, then, of course, $C = A$. Every subgroup conjugate to C is generated by subgroups conjugate to A; C therefore has only a finite number of conjugate subgroups. No two subgroups conjugate

to C can together generate a p-group, because otherwise C, together with one of its conjugate subgroups, would also generate a p-group, contrary to the definition of C.

We now choose an arbitrary p-subgroup Q of G and denote by $\mathfrak{M}$ the system of all the subgroups conjugate to C whose normalizers do not contain Q. The system $\mathfrak{M}$ may be empty. If not, and if a subgroup C' belongs to $\mathfrak{M}$, then *the number of subgroups that are conjugate to C' under transformations by elements of Q is finite and is a positive power of p*: this number is equal to the index in Q of the intersection of Q with the normalizer of C'; but this intersection is different from Q and it only remains to refer to the above result on the indices of subgroups of p-groups.

If

$$C'' = q^{-1}C'q, \quad q \in Q,$$

then C'' belongs to $\mathfrak{M}$: if the normalizer of C'' contained Q, then by the inverse transformation we would find that Q occurs in the normalizer of C'. Making use of the fact that Q is a subgroup we deduce that $\mathfrak{M}$ splits into disjoint subsystems of subgroups that are conjugate under transformations by elements of Q; therefore, if $\mathfrak{M}$ is not empty, then *the total number of subgroups occurring in $\mathfrak{M}$ is divisible by p*.

Let us now take as Q the subgroup C. The normalizer of any subgroup C' conjugate to C and distinct from it cannot contain C; otherwise C and C' would together generate a p-subgroup, as we have shown in this section; but this is impossible. Therefore, in this case $\mathfrak{M}$ consists of all the subgroups conjugate to C except C itself, and *the total number of subgroups conjugate to C is congruent to* 1 (modulo p). This proves the second part of the theorem.

Finally we choose as Q the given p-subgroup B. In this case the system $\mathfrak{M}$ cannot contain all the subgroups conjugate to C, since the number of elements in the system is congruent to 1 (modulo p), while the number of subgroups occurring in $\mathfrak{M}$ must be divisible by p or $\mathfrak{M}$ must be empty. There exists, then, a subgroup C' conjugate to C whose normalizer contains B, and $\{C, B\}$ is then a p-group. *A fortiori* every subgroup in C' conjugate to A generates, together with B, a p-group. This concludes the proof.

From this result we deduce the following theorem, first proved in the paper by Dietzmann, Kuroš, and Uzkov [1].

If a Sylow p-subgroup P of a group G has a finite number of conjugates, in other words, if its normalizer N in G has finite index, then the conjugates of P exhaust all Sylow p-subgroups of G. Their number is congruent to 1 (modulo p).

Another proof of the theorem was given by Baer [25]; his method has been used in the proof of the preceding theorem. Some generalizations of the theorem can be found in papers by Kuroš [15] and Dietzmann [6, 7].

The assumption of finiteness of the number of conjugates of P cannot be omitted in the formulation of the theorem. For let G be the free product of two arbitrary p-groups

$$G = P_1 * P_2.$$

If P_1 is not a Sylow p-subgroup of G, then it is contained in a Sylow p-subgroup $\overline{P}_1$. Like every p-group, the latter cannot be decomposed into a free product and by the subgroup theorem (§ 34) is therefore conjugate to a subgroup of one of the free factors P_1, P_2. However, since no element of P_1 can be conjugate to an element of P_2, the Sylow p-subgroup $\overline{P}_1$ is conjugate to some subgroup of P_1, that is, to a proper subgroup of itself, which we know to be impossible. This proves that P_1 and P_2 are Sylow p-subgroups of G, although not conjugate and possibly not even isomorphic.

The restricted countable symmetric group S is an example of a periodic group having non-isomorphic Sylow p-subgroups. For if we represent S in two ways as the union of ascending sequences of finite symmetric groups, the degrees of these groups being $p, p^2, \ldots, p^n, \ldots$ the first time and $p+p, p^2+p, \ldots, p^n+p, \ldots$ the second time, and if we take the union of the ascending sequences of Sylow p-subgroups of these groups, then for suitable choices of these sequences we can obtain two Sylow p-subgroups of S: one is a group without center (see Kuroš [9]), and the other has a cyclic group of order p as a direct factor and is therefore a group with a non-trivial center.

On the other hand, Baer [25] has given an example of a group in which all the Sylow p-subgroups are conjugate, although there are infinitely many of them.

In the case of finite groups the above theorem turns into *Sylow's Second Theorem*, first proved by Sylow [1] and again by Frobenius [1].

SYLOW'S SECOND THEOREM. *All Sylow p-subgroups of a finite group are conjugate, and the number of such subgroups is congruent to* 1 (modulo p).

In the formulation of this theorem we used the definition of a Sylow p-subgroup as a p-subgroup that is not contained in a larger p-subgroup. From Sylow's First Theorem we have already deduced that if p^m is the highest power of p dividing the order of a finite group G, then G has subgroups of order p^m. By Lagrange's theorem these subgroups cannot be contained in larger p-subgroups. On the other hand, if there existed a sub-

group of order p^l in G, $l < m$, not contained in a larger p-subgroup, then by the theorem just proved it would be conjugate to a subgroup of order p^m, which is clearly impossible. *This proves the equivalence of the two previous definitions of a Sylow p-subgroup of a finite group.*

The centers of p-groups. The following theorem plays an important rôle in the theory of finite groups.

Every finite p-group has a center different from E.

This theorem can be deduced from the following theorem of Dietzmann [1] which refers to arbitrary (not necessarily finite) p-groups.

If a p-group has a finite class of conjugate elements other than the unit element, then its center is different from E.

Suppose that a p-group G has a finite class $\mathfrak{A}$ of conjugate elements. Then by Dietzmann's Lemma (see the preceding section) the (normal) subgroup $A = \{\mathfrak{A}\}$ is finite. Hence every element of A is contained in a finite class of elements conjugate in G, so that the index of its normalizer in G is finite and, as shown above, is a power of p. Suppose the normal subgroup A splits into q classes of conjugate elements consisting of p^{α_1}, $p^{\alpha_2}, \ldots, p^{\alpha_q}$ elements, respectively. If the order of A is p^n, then

$$p^n = p^{\alpha_1} + p^{\alpha_2} + \ldots + p^{\alpha_q}.$$

However, the unit element occurs among these classes, say $p^{\alpha_1} = 1$, so we see that some of the numbers $p^{\alpha_2}, \ldots, p^{\alpha_q}$ must also be equal to 1, and this implies the existence of a non-trivial center of G. This completes the proof.

Infinite p-groups by no means always have a center. The first example of a p-group without center was published by Kuroš [9]. A much simpler example of such a group was constructed by Schmidt [6]. See also Baer [24].

§ 55. Local properties

Let W be some property which appertains to groups, and let G be a group in which every finitely generated subgroup has the property W. It need by no means follow from this that G itself has the property W, and this leads in a natural way to the definition of a number of new classes of groups. An example is the class of locally finite groups. We also mention

locally free groups, that is, groups in which every finitely generated subgroup is free (see Kuroš [10], and also § 48 of the first edition of this book; also papers by Fuchs-Rabinovič [2] and Mal'cev [4].

By the Nielsen-Schreier Theorem, all free groups belong to the class of locally free groups. The definition of a locally free group is also satisfied by the additive group of rational numbers and all its subgroups; for in these groups every finite subset generates an infinite cyclic subgroup.

On the other hand, the property W may be such that if it holds for all finitely generated subgroups of G, then it also holds for G itself; the simplest example is the commutativity of the group. "Local theorems" of this kind occur in many branches of the theory of groups. As a rule it is not necessary here to call for the use of all finitely generated subgroups, nor does the question of a local theorem have to be connected with finitely generated subgroups only. The natural statement of the problem is as follows (see Kuroš and Černikov [1]): A certain set L of subgroups of a group G is called a *local system of subgroups* of G if

(1) every element of G is contained in at least one subgroup of L,

(2) for any two subgroups of L (and hence any finite number of them) there is a subgroup of L containing them.

The system of all the finitely generated subgroups of a given group and the system of all its finitely generated normal subgroups are examples of local systems. Further examples, of course, are the system of all the subgroups of the given group, the system of all its normal subgroups, and—at the other extreme—the system consisting of the given group only.

We shall say that G *has the property* W *locally* if there exists at least one local system of subgroups such that all the subgroups occurring in it have the property W.[1] To prove *the local theorem for the property* W now consists in showing that a group has the property W if it has this property locally. Moreover, we shall sometimes have to impose additional restrictions on the local system in question: for example, we may require that all subgroups occurring in the system be normal.

A general method for proving local theorems has been indicated by Mal'cev [3]. This method utilizes the apparatus of mathematical logic and is based on a theorem of Mal'cev in the restricted predicate calculus. The theorem can also be proved easily by means of a method given below, which comes from a paper of Kuroš on the theory of compact topological spaces

[1] Many authors adhere to the more rigid convention that a group has a property *locally* if every finitely generated subgroup has the property. [*Trans.*]

(see also Kuroš [12]). This method also is used frequently to prove local theorems in the theory of groups.

Let S be a system of *finite* sets $A_\alpha, A_\beta, A_\gamma, \ldots$, *partially ordered* (see § 43) by a relation

$$A_\alpha \leqq A_\beta$$

(in words: A_α *precedes* A_β; A_β *follows* A_α). We make the following assumptions about the partial ordering in S:

(1) For any two sets A_α, A_β of S there exists a set A_γ in S such that $A_\alpha \leqq A_\gamma$, $A_\beta \leqq A_\gamma$.

We assume, further, that for every pair of sets A_α and A_β for which $A_\alpha \leqq A_\beta$, a single-valued mapping $\pi_{\beta\alpha}$ of A_β onto the whole of A_α is defined: it is called a *projection* of A_β onto A_α. Every element of A_β has a unique *image* in A_α under this projection; for every element of A_α there exists at least one *inverse image* in A_β. The projections defined in the system S must satisfy the following conditions:

(2) If $A_\alpha \leqq A_\beta$, $A_\beta \leqq A_\gamma$, then the projection $\pi_{\gamma\alpha}$ is the product of the projections $\pi_{\gamma\beta}$ and $\pi_{\beta\alpha}$.

(3) The projection $\pi_{\alpha\alpha}$ is the identity mapping of A_α onto itself.

A set P consisting of elements that occur in some of the sets A_α, that is, a subset of the union of all sets A_α of S, is called a *projection set* if P contains, together with any two elements a and b, an element c that is a common inverse image of a and b. Examples of projection sets are: the set consisting of a single element a of one of the A_α, and the set consisting of an element a and its images in all the sets A_γ preceding A_α.

From the definition of a projection set P it follows that P cannot contain more than one element from any one set A_α: two distinct elements of A_α cannot have a common inverse image in any set following A_α, because the projections are single-valued. Moreover, if P contains elements a and b from A_α and A_β, respectively, and $A_\alpha < A_\beta$, then by (2) a is an image of b.

A projection set containing exactly one element from *each* set A_α of S is called *complete*.

The following general theorem holds:

Theorem. *Every projection set P of the system S is part of some complete projection set.*

Proof. Let us well-order the system S without reference to the original partial ordering of S. The sets A_α, with transfinite indices, will now be written as $A^\lambda, A^\mu, A^\nu, \ldots$. We only assume that in the well-ordering in

question every set A_α having an element that occurs in P precedes every A_β having an empty intersection with P. In every set A^λ we wish to *label* an element a^λ such that *every finite system of labelled elements has a common inverse image in* S. We also assume that the elements of the projection set P are labelled in those sets A_α in which they are contained.

Suppose that the elements a^λ are already labelled in all sets A^λ for $\lambda < \mu$. Suppose further, that the set A^μ consists of $b_1, b_2, \ldots, b_n$ and that for every b_i, $1 \leqq i \leqq n$, we can find a finite system

$$a_i^{\lambda_1}, a_i^{\lambda_2}, \ldots, a_i^{\lambda_{s(i)}}, \quad \lambda_j < \mu, \quad j = 1, 2, \ldots, s(i), \tag{i}$$

of elements previously labelled such that the elements of the system (i) and b_i do not have a common inverse image in S. The union of all systems (i), $i = 1, 2, \ldots, n$, gives a finite system of labelled elements for which there therefore exists a common inverse image c belonging to a certain set A_β. We take a set A_γ following A_β and A^μ, and choose in it an element d, one of the inverse images of c. The image of d in A^μ is an element b_{i_0}. We find that b_{i_0} and the system (i_0) have a common inverse image, and this contradicts our assumption.

We have proved that a labelled element a^μ can be chosen in every set A^μ. If several elements of A^μ can serve as marked elements, then for the sake of definiteness we can regard the elements of A^μ as numbered and we always choose the element with the smallest number.

The set $\overline{P}$ of all labelled elements is a projection set. For if a^μ and a^ν are the labelled elements in A^μ and A^ν, then they have a common inverse image in some set A^λ following A^μ and A^ν. In A^λ an element a^λ is labelled, and since a^μ, a^ν, and a^λ must have a common inverse image, a^λ is, by (2), the common inverse image of a^μ and a^ν. The projection set $\overline{P}$ contains P and is complete. This concludes the proof of the theorem.[5]

If the definition of a projection $\pi_{\alpha\beta}$ is altered so that it is a single-valued mapping of A_β into A_α and not necessarily onto A_α, then on the basis of the theorem just proved *the existence of complete projection sets can be established* in this case as well.

For in A_α there exist elements x having an inverse image in every A_β, $A_\beta \geqq A_\alpha$: if A_α consists of $x_1, x_2, \ldots, x_n$ and if for every i, $i = 1, 2, \ldots, n$, we can find a set A_{β_i} such that $A_{\beta_i} > A_\alpha$, but that x_i has no inverse image in A_{β_i}, then a set $A_\gamma, A_\gamma \geqq A_{\beta_i}, i = 1, 2, \ldots, n$, cannot be mapped into A_α at all, which is impossible. We denote by A_α' the set of all elements x of A_α with the required properties. In the mapping $\pi_{\beta\alpha}$ the set A_β' is mapped onto the whole of A_α': if none of the inverse images $y_1, \ldots, y_k$

in A_β of the elements x of A_α' belongs to A_β', then there exists an A_γ, $A_\gamma > A_\beta$, in which none of these elements $y_1, \ldots, y_k$ has an inverse image. However, in that case x also has no inverse image in A_γ, which is impossible. We can now apply the proof of the above theorem to the sets A_α'.

Let us use this method to prove a theorem on Sylow p-subgroups (Baer [25]; the proof below is contained in a paper by Gol'berg [2]). We first introduce the following new concepts.

An automorphism φ of a group G is called *locally inner* if, given any finite set of elements $a_1, a_2, \ldots, a_n$ of G, we can find another element g, depending in general on the set in question, such that

$$a_i\varphi = g^{-1}a_i g, \quad i = 1, 2, \ldots, n.$$

Two subgroups A and B of G are called *locally conjugate* if there exists a locally inner automorphism of G mapping A onto B.

We wish to prove the following theorem:

Any two Sylow p-subgroups of a locally normal group are locally conjugate and therefore isomorphic.

Let P be a Sylow p-subgroup of a locally normal group G. We shall show that *the intersection of P with an arbitrary finite normal subgroup H_α of G is a Sylow p-subgroup of H_α.*

For if we denote by A_α the set of those Sylow p-subgroups of the finite group H_α which contain the intersection $P \cap H_\alpha$, then A_α is finite and not empty. The system S of finite sets A_α that is obtained when H_α ranges over all the finite normal subgroups of G becomes partially ordered if we put $A_\alpha \leqq A_\beta$ for $H_\alpha \subseteq H_\beta$. It is even a lattice, so that condition (1) is satisfied.

For $A_\alpha \leqq A_\beta$ a projection $\pi_{\beta\alpha}$ is defined as follows. If P' is a Sylow p-subgroup of H_β belonging to A_β, that is,

$$P' \supseteq P \cap H_\beta,$$

then we consider the intersection $P' \cap H_\alpha = P''$. Since H_α is normal in H_β and since all Sylow p-subgroups of the finite group H_β are conjugate, then, by what has been proved in the preceding section, P'' is a Sylow p-subgroup of H_α. Since

$$P'' = P' \cap H_\alpha \supseteq (P \cap H_\beta) \cap H_\alpha = P \cap H_\alpha,$$

P'' belongs to the set A_α. The mapping

$$P' \to P''$$

is a projection of A_β into A_α, and conditions (2) and (3) are satisfied: if

$$H_\alpha \subset H_\beta \subset H_\gamma$$

and if P' is a Sylow p-subgroup of H_γ, then

$$P' \cap H_\alpha = (P' \cap H_\beta) \cap H_\alpha.$$

The system S therefore contains a complete projection set. In other words, we can choose from every set A_α one Sylow p-subgroup P_α such that any two of them, P_α and P_β, are contained in a third, P_γ. It follows that the union of all the subgroups P_α is a p-subgroup of G containing the Sylow p-subgroup P and is therefore equal to P; hence for every α the p-subgroup P_α of H_α coincides with the intersection $P \cap H_\alpha$, and this is what we had to prove.

We now come to the proof of the theorem itself. Let P_1 and P_2 be two Sylow p-subgroups of the locally normal group G. If H_α is an arbitrary finite normal subgroup of G, then by what we have proved above the intersections $P_1 \cap H_\alpha$ and $P_2 \cap H_\alpha$ are Sylow p-subgroups of H_α and are therefore conjugate in H_α. We denote by A_α the set of all automorphisms of H_α that are induced by inner automorphisms of G and map $P_1 \cap H_\alpha$ onto $P_2 \cap H_\alpha$. The set A_α is finite and not empty. We put $A_\alpha \leqq A_\beta$ for $H_\alpha \subseteq H_\beta$ and define a projection $\pi_{\beta\alpha}$ as follows: If φ is an automorphism of H_β belonging to A_β, then it is induced by an inner automorphism of G and it therefore induces an automorphism φ' in the normal subgroup H_α; since φ maps $P_1 \cap H_\beta$ onto $P_2 \cap H_\beta$, φ' maps $P_1 \cap H_\alpha$ onto $P_2 \cap H_\alpha$, that is, φ' belongs to A_α. We shall then regard the projection $\pi_{\beta\alpha}$ as carrying φ into φ'.

Conditions (1), (2), and (3) are obviously satisfied, so that we can apply the theorem on the existence of a complete projection set. We can therefore select one automorphism from every set A_α such that any two of them, φ_α and φ_β, are induced by a certain φ_γ. The group G is locally normal, and therefore the totality of these automorphisms φ_α defines an automorphism of G which is locally inner and which in addition maps P_1 onto P_2. This concludes the proof.

The example of the restricted symmetric group, already mentioned in the preceding section, shows that in the formulation of this theorem local normality cannot be replaced by local finiteness.

§ 56. Normal and invariant systems

In the following chapters we shall make use of a generalization of the concept of a finite normal series (see § 16) and some generalizations of the Schreier and Jordan-Hölder Theorems connected with it. Preliminary results are in papers by Kuroš [4] and Birkhoff [2]; the full results in a paper by Kuroš [14]; see also Kuroš and Černikov [1].

Let G be a group with an arbitrary operator domain and let $\mathfrak{A} = [A_\alpha]$ be a system of admissible subgroups containing the unit subgroup $E = A_0$ and the whole group $G = A_\mu$. Further, let the indices α range over an index set $\mathfrak{M}$ ordered by means of a relation $<$ such that $\alpha < \beta$ implies $A_\alpha \subset A_\beta$; thus the system $\mathfrak{A}$ is ordered by set-theoretical inclusion. If $\mathfrak{M}$ contains an element immediately following α then we shall denote it by $\alpha + 1$ and we shall say that the subgroups A_α and $A_{\alpha+1}$ (where, of course, $A_\alpha \subset A_{\alpha+1}$) form a *jump* in $\mathfrak{A}$.

The ordered system of subgroups $\mathfrak{A}$ will be called *complete* if for an arbitrary subsystem of $\mathfrak{A}$ the unions and the intersections of the subgroups forming the subsystem belong to $\mathfrak{A}$, in other words, if for every Dedekind section taken in $\mathfrak{A}$ both the union of the subgroups forming the first class of the section and the intersection of the subgroups forming the second class belong to $\mathfrak{A}$. *Every ordered system of subgroups $\mathfrak{A}$ can be completed*: for this purpose it is sufficient to add to $\mathfrak{A}$ the unions of the first classes and intersections of the second classes of all sections; it is easy to verify that the resulting system of subgroups remains ordered and is complete.

Every complete system of subgroups $\mathfrak{A} = [A_\alpha]$ has jumps, and the jumps in the system are even everywhere dense. For, every element x of G, $x \neq 1$, defines a jump in the system $\mathfrak{A}$: we obtain a section in $\mathfrak{A}$ if we put into the first class the subgroups A_α not containing x and into the second class the subgroups A_α containing x. Since $\mathfrak{A}$ is complete, it contains the union of the subgroups of the first class and the intersection of the subgroups of the second class; these two subgroups are distinct—the first does not contain x, whereas the second does—and so they form a jump.

We can now define the fundamental concepts of the present section. A *normal system* of a group G is a complete ordered system of (admissible) subgroups $\mathfrak{A} = [A_\alpha]$ of G containing E and G and satisfying the following additional condition: for every jump A_α, $A_{\alpha+1}$ of $\mathfrak{A}$, A_α shall be a normal subgroup of $A_{\alpha+1}$. Among the normal systems there are, of course, all finite normal series of G.

A normal system $\mathfrak{A}'$ is called a *refinement* of the normal system $\mathfrak{A}$ if

every subgroup occurring in $\mathfrak{A}$ is also contained in $\mathfrak{A}'$. Note that here *every subgroup A' that occurs in $\mathfrak{A}'$ but does not belong to $\mathfrak{A}$ falls into a jump of the system $\mathfrak{A}$*, in other words, it lies between the union of all the subgroups of $\mathfrak{A}$ contained in A' and the intersection of all the subgroups of $\mathfrak{A}$ containing A'.

A normal system of G that does not admit further refinements is called a *composition system.*

Every normal system $\mathfrak{A}$ of a group G can be refined to a composition system.

To prove this we put $\mathfrak{A} = \mathfrak{A}_1$. Suppose now that normal systems $\mathfrak{A}_\gamma$ have already been defined for all cardinal numbers γ less than a certain δ such that they form an ascending sequence. If $\delta - 1$ exists and if $\mathfrak{A}_{\delta-1}$ is not yet a composition system, then we take as $\mathfrak{A}_\delta$ one of the refinements of $\mathfrak{A}_{\delta-1}$. But if δ is a limit number, then we denote the union of all $\mathfrak{A}_\gamma$, $\gamma < \delta$, by $\mathfrak{A}'_\delta$. In general, this system is not complete, but its completion, obtained by the method described above, satisfies all the requirements occurring in the definition of a normal system and can therefore be taken as $\mathfrak{A}_\delta$.

For it is obvious that $\mathfrak{A}_\delta$ is ordered by inclusion. Further, $\mathfrak{A}_\delta$ *is complete*—every section in $\mathfrak{A}_\delta$ gives rise to some section in every $\mathfrak{A}_\gamma$, $\gamma < \delta$, and the first (second) classes of all these sections have unions (intersections) that belong to $\mathfrak{A}_\gamma$ and therefore to $\mathfrak{A}'_\delta$; but then the union (intersection) of all these unions (intersections) is, by assumption, contained in $\mathfrak{A}_\delta$ and is the union of the whole first class (intersection of the whole second class) of the given section. Finally, $\mathfrak{A}_\delta$ *satisfies the normality condition for sections.* For, every jump A_α, $A_{\alpha+1}$ in $\mathfrak{A}_\delta$ determines a jump A_{α_γ}, $A_{\alpha_\gamma+1}$ in $\mathfrak{A}_\gamma$ such that for $\gamma < \gamma'$ we have $A_{\alpha_\gamma} \subseteq A_{\alpha_{\gamma'}}$, $A_{\alpha_\gamma+1} \supseteq A_{\alpha_{\gamma'}+1}$. Now A_α is the union of all A_{α_γ} and $A_{\alpha+1}$ is the intersection of all $A_{\alpha_\gamma+1}$, and since every A_{α_γ} is a normal subgroup of $A_{\alpha_\gamma+1}$ and therefore of $A_{\alpha+1}$, we see that A_α is a normal subgroup of $A_{\alpha+1}$.

The process of constructing the $\mathfrak{A}_\delta$ systems comes to an end with a certain $\delta = \delta_0$, and the system $\mathfrak{A}_{\delta_0}$ is the required composition system. This completes the proof of the theorem.

If all the inner automorphisms of the group are taken as operators, then the concept of a normal system turns into that of an *invariant system*—this is a system of normal subgroups of G, containing E and G, ordered by inclusion and complete; the normality condition for jumps is automatically satisfied here. The concept of a composition system now turns into that

of a *principal system*, that is, an invariant system that does not admit further invariant refinements.

A well-ordered ascending normal system will be called an *ascending normal series*; a finite normal series is a special case of this concept. Similarly we define the concepts of *ascending invariant series, ascending composition series*, and *ascending principal series*. Similarly, a well-ordered descending normal system will be called a *descending normal series*, and so on.

We now come to the generalization of the main theorems of § 16. If $\mathfrak{A} = [A_\alpha]$ is a normal system of a group G, then to every jump A_α, $A_{\alpha+1}$ in the system there corresponds a factor group $A_{\alpha+1}/A_\alpha$, called a *factor* of $\mathfrak{A}$. For the subgroups of G we have the following theorem.

If $\mathfrak{A} = [\mathfrak{A}_\alpha]$ is a normal system of a group G with an arbitrary operator domain, then every (admissible) subgroup F of G has a normal system whose factors are isomorphic to subgroups of distinct factors of $\mathfrak{A}$.

We put

$$B_\alpha = F \cap A_\alpha, \qquad 0 \leqq \alpha \leqq \mu.$$

The system $\mathfrak{B} = [B_\alpha]$ is an ordered system of subgroups of F, possibly with repetitions, and $B_0 = E$, $B_\mu = F$. From the fact that $\mathfrak{A}$ is complete it follows that $\mathfrak{B}$ is also complete, provided we regard an ordered system of subgroups with repetitions as complete if for every section of the system one of the following three possibilities is realized: 1) The first class of the section has a last subgroup and the second class a first subgroup, 2) the first class of the section has a last subgroup which is the intersection of the subgroups of the second class, 3) the second class of the section has a first subgroup which is the union of the subgroups of the first class.

To every jump B_α, $B_{\alpha+1}$ of $\mathfrak{B}$ there corresponds a jump A_α, $A_{\alpha+1}$ of $\mathfrak{A}$. Using the fact that A_α is normal in $A_{\alpha+1}$ and that

$$B_\alpha = B_{\alpha+1} \cap A_\alpha$$

and applying Zassenhaus' Lemma, we find that B_α is normal in $B_{\alpha+1}$ and that

$$B_{\alpha+1}/B_\alpha \simeq A_\alpha B_{\alpha+1}/A_\alpha.$$

However

$$A_\alpha B_{\alpha+1} \subseteq A_{\alpha+1},$$

so that the factor group $A_\alpha B_{\alpha+1}/A_\alpha$ is isomorphic to a subgroup of the factor group $A_{\alpha+1}/A_\alpha$. Finally, in view of the completeness of $\mathfrak{B}$, every collection of equal subgroups in the system has a first and a last subgroup;

we do not introduce new jumps, therefore, if we replace every such collection by a single subgroup; in other words, we have arrived at the required normal system of F.

This proves the subgroup theorem. In addition we note that *if* $\mathfrak{A}$ *is an ascending normal series, then the same is true for* $\mathfrak{B}$.

Generalizations of the Schreier and Jordan-Hölder Theorems. Two normal systems $\mathfrak{A}$ and $\mathfrak{B}$ of a group G are called *isomorphic* if a one-to-one correspondence can be established between their factors such that the corresponding factors are isomorphic. It is not assumed that the order types of $\mathfrak{A}$ and $\mathfrak{B}$, as ordered sets, are the same.

We cannot assert, in general, that every two composition systems of an arbitrary group are isomorphic—the additive group of the integers provides a counter-example. In this group the subgroup systems

$$\{1\} \supset \{2\} \supset \{4\} \supset \ldots \supset \{2^n\} \supset \ldots \supset 0,$$
$$\{1\} \supset \{3\} \supset \{9\} \supset \ldots \supset \{3^n\} \supset \ldots \supset 0$$

are descending principal series, but all the factors of the first series are cyclic groups of order two, and all the factors of the second series are cyclic groups of order three. A few results that generalize the Schreier and the Jordan-Hölder Theorems can, nevertheless, be proved.

Let $\mathfrak{A} = [A_\alpha]$, $0 \leqq \alpha \leqq \mu$ and $\mathfrak{B} = [B_\beta]$, $0 \leqq \beta \leqq \nu$ be two normal systems of a group G with an arbitrary operator domain. We put

$$A_{\alpha\beta} = A_\alpha (A_{\alpha+1} \cap B_\beta)$$

for all α for which $\alpha + 1$ exists and for all β, and

$$B_{\beta\alpha} = B_\beta (B_{\beta+1} \cap A_\alpha)$$

for all β for which $\beta + 1$ exists and for all α. Inserting all the $A_{\alpha,\beta}$ into $\mathfrak{A}$ and all the $B_{\beta,\alpha}$ into $\mathfrak{B}$, we obtain ordered systems of subgroups of G, possibly with repetitions; we denote them by $\overline{\mathfrak{A}}$ and $\overline{\mathfrak{B}}$.

Every jump in $\overline{\mathfrak{A}}$ has the form $A_{\alpha\beta}$, $A_{\alpha,\beta+1}$, where α is such that $\alpha + 1$ exists. If we associate it with the jump $B_{\beta\alpha}$, $B_{\beta,\alpha+1}$ of $\overline{\mathfrak{B}}$ we obtain a one-to-one correspondence between the jumps of the two systems. Zassenhaus' Lemma enables us to state that $A_{\alpha,\beta}$ is a normal subgroup of $A_{\alpha,\beta+1}$ and $B_{\beta,\alpha}$ a normal subgroup of $B_{\beta,\alpha+1}$ and that the corresponding factors are isomorphic:

$$A_{\alpha,\beta+1}/A_{\alpha\beta} \simeq B_{\beta,\alpha+1}/B_{\beta\alpha}.$$

The systems $\overline{\mathfrak{A}}$ and $\overline{\mathfrak{B}}$ need not, however, be complete in the sense of the above definition of completeness for subgroup systems with repetitions.

If we choose, for example, a section in $\overline{\mathfrak{A}}$, then it is easy to verify that the union of the first class of the section always belongs to $\overline{\mathfrak{A}}$. But the intersection of the second class need not belong to $\overline{\mathfrak{A}}$: if B_β is the intersections of the subgroups $B_{\beta'}$, $\beta' > \beta$, then $A_{\alpha+1} \cap B_\beta$ is the intersection of the subgroups $A_{\alpha+1} \cap B_{\beta'}$, but the product $A_\alpha (A_{\alpha+1} \cap B_\beta)$ may turn out to be smaller than the intersection of the products $A_\alpha (A_{\alpha+1} \cap B_{\beta'})$, $\beta' > \beta$.

Let us make the following assumption:

(C) *The normal systems $\mathfrak{A}$ and $\mathfrak{B}$ are such that the systems $\overline{\mathfrak{A}}$ and $\overline{\mathfrak{B}}$ contain the intersections of the second class for each of their sections, in other words, are such that $\overline{\mathfrak{A}}$ and $\overline{\mathfrak{B}}$ are complete.*

In that case every collection of equal subgroups of $\overline{\mathfrak{A}}$ (and of $\overline{\mathfrak{B}}$) has a first as well as a last subgroup. If we replace every such collection of equal subgroups by a single subgroup, we obtain systems without repetitions $\tilde{\mathfrak{A}}$ and $\tilde{\mathfrak{B}}$ containing the original systems $\mathfrak{A}$ and $\mathfrak{B}$ respectively. In the transition from $\overline{\mathfrak{A}}$ to $\tilde{\mathfrak{A}}$ and from $\overline{\mathfrak{B}}$ to $\tilde{\mathfrak{B}}$ no new jumps have appeared and no old ones have vanished, except those corresponding to factors E: and from the completeness of $\overline{\mathfrak{A}}$ and $\overline{\mathfrak{B}}$ there follows that of $\tilde{\mathfrak{A}}$ and $\tilde{\mathfrak{B}}$. Thus *$\tilde{\mathfrak{A}}$ and $\tilde{\mathfrak{B}}$ are isomorphic normal systems without repetitions, and are refinements of $\mathfrak{A}$ and $\mathfrak{B}$, respectively.*

We apply this method to prove the following theorem.

Any two ascending normal series of an arbitrary group G have isomorphic refinements, which are also ascending normal series. In particular, if G has ascending composition series, then all such series are isomorphic.

For if $\mathfrak{A}$ and $\mathfrak{B}$ are well-ordered ascending systems, then the same is true for $\overline{\mathfrak{A}}$ and $\overline{\mathfrak{B}}$, so that assumption (C) is satisfied. $\tilde{\mathfrak{A}}$ and $\tilde{\mathfrak{B}}$, as subsystems of $\overline{\mathfrak{A}}$ and $\overline{\mathfrak{B}}$, are also well-ordered.

If $\mathfrak{A}$ is an ascending invariant series of a group G and $\mathfrak{B}$ an arbitrary invariant system, then they have invariant refinements $\tilde{\mathfrak{A}}$ and $\tilde{\mathfrak{B}}$ such that the totality of factors of $\tilde{\mathfrak{B}}$ forms a part (not necessarily a proper part) of the totality of factors of $\tilde{\mathfrak{A}}$. In particular, if G has an ascending principal series $\mathfrak{A}$, then the totality of factors of any other principal systems of G forms part of the totality of factors of $\mathfrak{A}$.

Let us construct the systems $\overline{\mathfrak{A}}$ and $\overline{\mathfrak{B}}$ from $\mathfrak{A}$ and $\mathfrak{B}$. $\overline{\mathfrak{B}}$ is complete, because it is obtained from $\mathfrak{B}$ by completing every jump of some ascending well-ordered system of subgroups. However, $\overline{\mathfrak{A}}$ need not be complete, and we complete it to a system $\overline{\mathfrak{A}}'$ by adding the intersections of the second

classes of all sections; from the invariance of $\overline{\mathfrak{A}}$ there follows the invariance of $\overline{\mathfrak{A}}'$.[1] All the factors of $\overline{\mathfrak{A}}$ are preserved, but new jumps, and therefore new factors, may be added which do not correspond to any factors of $\overline{\mathfrak{B}}$. The transition from $\overline{\mathfrak{A}}'$ and $\overline{\mathfrak{B}}$ to invariant systems without repetitions $\widetilde{\mathfrak{A}}$ and $\widetilde{\mathfrak{B}}$ completes the proof of the theorem.

Let the group G have an ascending principal series $\mathfrak{A} = [A_n]$ with the order type of the natural numbers, that is, of the form

$$E = A_0 \subset A_1 \subset A_2 \subset \ldots \subset A_n \subset \ldots \subset A_\omega = G.$$

Then all principal systems of G are isomorphic to $\mathfrak{A}$.

For let $\mathfrak{B} = [B_\beta]$ be an arbitrary principal system of G. We construct the systems $\overline{\mathfrak{A}}$ and $\overline{\mathfrak{B}}$. Since $\mathfrak{A}$ is a principal system, and since we know that $\overline{\mathfrak{A}}$ contains the unions of the first class of all its sections, we can find for every n, $n \geqq 0$, an index β_n such that $A_{n,\beta_n} = A_n$, but $A_{n,\bar{\beta}} = A_{n+1}$ for all $\bar{\beta} > \beta_n$; in other words

$$A_{n+1} \cap B_{\beta_n} \subseteq A_n, \tag{1}$$

$$A_n (A_{n+1} \cap B_{\bar{\beta}}) = A_{n+1}, \quad \bar{\beta} > \beta_n. \tag{2}$$

Taking into account the remark in the proof of the preceding theorem, we can state that our theorem will be proved if we can establish the existence of the index $\beta_n + 1$ for every n. For in that case $\overline{\mathfrak{A}}$ is complete, and therefore in the transition to the system $\widetilde{\mathfrak{A}}$—in our case to $\mathfrak{A}$—no new factors can appear, so that the principal systems $\mathfrak{A}$ and $\mathfrak{B}$ turn out to be isomorphic.

Let us first prove the following lemma.

LEMMA. *If the indices β' and β'', $\beta' < \beta''$, are such that for a given n none of the indices β_i, $0 \leqq i \leqq n$, satisfies the inequality $\beta' \leqq \beta_i \leqq \beta''$, then*

$$A_{n+1} \cap B_{\beta'} = A_{n+1} \cap B_{\beta''}.$$

For if $n = 0$, then by (1) and (2)

$$A_1 \cap B_{\beta_0} = E, \quad A_1 \subseteq B_{\bar{\beta}} \text{ for } \bar{\beta} > \beta_0.$$

Therefore for $\beta'' < \beta_0$ we have

$$A_1 \cap B_{\beta'} = A_1 \cap B_{\beta''} = E,$$

[1] If we had considered not invariant, but only normal systems, then we would not be able to prove that $\overline{\mathfrak{A}}'$ is a normal system.

and for $\beta_0 < \beta'$

$$A_1 \cap B_{\beta'} = A_1 \cap B_{\beta''} = A_1.$$

Suppose the lemma already proved for $n - 1$. If $\beta'' < \beta_n$, then by (1)

$$A_{n+1} \cap B_{\beta'} \subseteq A_n, \quad A_{n+1} \cap B_{\beta''} \subseteq A_n,$$

and hence

$$A_{n+1} \cap B_{\beta'} = A_n \cap B_{\beta'}, \quad A_{n+1} \cap B_{\beta''} = A_n \cap B_{\beta''}.$$

The right-hand sides of these equations coincide, however, by the induction hypothesis and the condition of the lemma. If $\beta_n < \beta'$, then we choose an arbitrary element x of $A_{n+1} \cap B_{\beta''}$. By (2) it can be written in the form $x = yz$, where

$$y \in A_n, \ z \in (A_{n+1} \cap B_{\beta'}).$$

Hence it follows that

$$y = xz^{-1} \in B_{\beta''},$$

that is,

$$y \in (A_n \cap B_{\beta''}).$$

By the induction hypothesis

$$A_n \cap B_{\beta''} = A_n \cap B_{\beta'};$$

therefore $y \in B_{\beta'}$, and hence

$$x \in (A_{n+1} \cap B_{\beta'}),$$

and this is what we had to prove.

We now turn to the proof of the theorem. Suppose that for a given n the index $\beta_n + 1$ does not exist. In that case B_{β_n} is the intersection of all $B_{\beta'}$, $\beta' > \beta_n$, since otherwise their intersection could be inserted in $\mathfrak{B}$, in contradiction to the fact that it is a principal system. If β_k is the smallest of the indices β_i, $i < n$, that are greater than β_n (if such indices exist at all), then by the lemma the intersections $A_{n+1} \cap B_{\beta'}$ are equal for all β' such that $\beta_n < \beta' < \beta_k$ (or simply, for all β' with $\beta_n < \beta'$, if β_k does not exist). They are, then, also equal to the intersection of A_{n+1} with the intersection of all $B_{\beta'}$, that is, to the intersection $A_{n+1} \cap B_{\beta_n}$. But this leads to a contradiction to (1) and (2) and proves the theorem.

There are examples to show (see Kuroš [14]) that in the formulation of this theorem it is not sufficient to assume that $\mathfrak{A}$ is an arbitrary ascending principal series nor to replace the principal series and systems by composition series and systems. However, groups to which the theorem applies may have principal systems of very complicated structure. Let us consider, for

example, *the direct sum of a countable set of cyclic groups of order two.* This group obviously has an ascending principal series with the order type of the natural numbers. On the other hand, we can number the direct summands by means of the rational numbers and perform all possible sections in the system of rational numbers—omitting, in the case of a rational section, the corresponding rational number in the second class. If we take for every section the sum of the direct summands corresponding to the first class of the section and complete the system of subgroups so obtained, then we obtain a principal system with the cardinal number of the continuum, with the order type of a perfect everywhere-discontinuous set; and the jumps in the system correspond to rational sections.

CHAPTER XIV

SOLVABLE GROUPS

§ 57. Solvable and generalized solvable groups

We now pass on to the study of a very wide class of groups, which contains, in particular, all the abelian groups. Historically, the significance of this class of groups derives from its connection with the problems of the solution of equations by radicals.

A finite normal or invariant series of a group is called a *solvable series* if all its factors are abelian. A group G is called *solvable* if it satisfies one of the following conditions, whose equivalence will be proved below:

(1) G has a finite solvable normal series.

(2) G has a finite solvable invariant series.

(3) The derived chain of G (see § 14) terminates in the unit subgroup after a finite number of steps.

It is clear that (2) implies (1). Furthermore, (3) implies (2), because if the derived chain reaches the unit element after a finite number of steps, then it becomes the *derived series*, which is a finite solvable invariant series.

We shall now show that (1) implies (3). Let $K^{(i)}$ be the i-th derived group of G, and let G have a finite solvable normal series

$$G = H_0 \supset H_1 \supset H_2 \supset \ldots \supset H_n = E.$$

Since the factor group G/H_1 is commutative, we have $H_1 \supseteq K'$. Suppose $H_i \supseteq K^{(i)}$ to be already proved. Since H_i/H_{i+1} is commutative, H_{i+1} contains the derived group of H_i and, *a fortiori*, the derived group of $K^{(i)}$, that is, $H_{i+1} \supseteq K^{(i+1)}$. From $H_n = E$ it now follows that $K^{(n)} = E$.

Since a refinement of a solvable series is itself solvable, we obtain from Schreier's Theorem that *every normal series of a solvable group can be refined to a solvable series*, so that *every normal subgroup of a solvable group occurs in some solvable series.* It follows that *every factor group of a solvable group is itself solvable.* Furthermore, we can apply to a solvable series the theorem of § 16 which states that if a normal series is given in a group, then in any subgroup we can find a normal series whose factors are isomorphic to subgroups of the factors of the given series. So we see that *every subgroup of a solvable group is itself solvable.*

An extension G of a solvable group A by a solvable group B is itself a solvable group.

For if we take a solvable series of A and supplement it by means of the subgroups that correspond to the subgroups of a solvable series of B so as to form a normal series of G, then we obtain a solvable series of G.

It follows that *every group having a finite normal series with solvable factors is solvable.* In particular, *the direct product of a finite number of solvable groups is itself solvable.* The corresponding statement for the direct product of an infinite set of solvable groups does not hold.

Finally, we mention that simple non-abelian groups are the simplest examples of non-solvable groups.

Finite solvable groups. If a solvable group G is *finite*, then a solvable series of G can be refined to a composition series. *The composition factors of a finite solvable group are simple abelian groups, that is, cyclic groups of prime order.* This property of finite solvable groups can be taken as the definition of this class of groups. Furthermore, every solvable group having a composition series is finite, because every simple abelian group is finite.

Finite solvable groups, in contrast to finite abelian groups, form a very wide class of groups whose complete classification has not yet been achieved. Indeed, the following problem, which is equivalent to Burnside's problem on simple finite groups (see § 61), is still open: *Is every finite group of odd order solvable?*

Every finite p-group, for an arbitrary prime number p, is solvable.

For if G is a finite p-group, then we know from § 54 that its center Z is different from E. The factor group G/Z is also a finite p-group, but of smaller order. If we assume the theorem to be proved for p-groups whose order is less than that of G, then we obtain that G is an extension of the abelian group Z by the solvable group G/Z, and hence is itself solvable.

Finite solvable groups can also be defined in many other ways, apart from those indicated above. Let us discuss one of these methods (see Ore [9]).

We shall call a subgroup A of a group G *almost normal* if we can find normal subgroups N and N' in G, $N \supset N'$, such that

$$AN = G,\ A \cap N = N'. \tag{1}$$

If A is a normal subgroup of G, then it is almost normal: it is sufficient to take

$$N = G,\ N' = A.$$

A finite group is solvable if and only if it has the following property:

($\mathfrak{D}$) *If A and B are subgroups of G, $A \subset B$, and if A is a maximal proper subgroup of B, then A is almost normal in B.*

Suppose a group G to have the property ($\mathfrak{D}$). Then all the subgroups and all the factor groups of G also have the property ($\mathfrak{D}$).

For if A/H and B/H are subgroups of G/H, $A/H \subset B/H$, and if A/H is a maximal proper subgroup of B/H, then $A \subset B$, and A is a maximal proper subgroup of B. There then exist normal subgroups N and N' of B, with $N \supset N'$, satisfying the conditions

$$AN = B,\ A \cap N = N'.$$

In them we can substitute the normal subgroups HN and HN', and then

$$A/H \cdot HN/H = B/H,\ A/H \cap HN/H = HN'/H.$$

Hence it follows that all the factors of a composition series of G have the property ($\mathfrak{D}$). If at least one of these factors is not a cyclic group of prime order, then it must have a non-trivial subgroup and therefore, by ($\mathfrak{D}$), a non-trivial normal subgroup, and this is impossible.

This proves that G is solvable.

Suppose, on the other hand, that A and B are subgroups of a finite solvable group, $A \subset B$, and that A is a maximal proper subgroup of B. We denote by N' a maximal normal subgroup of B contained in A. Since B, as a subgroup of a solvable group, is itself solvable, its factor group $\overline{B} = B/N'$ is also solvable. It therefore has an abelian normal subgroup $\overline{N} = N/N'$—for example, the last term but one of a solvable invariant series of $\overline{B}$. It is clear that

$$AN = B. \tag{2}$$

Moreover, the intersection $A \cap N$ is normal in A, as the intersection of a subgroup with a normal subgroup, and it is also normal in N, because

$$A \cap N \supseteq N', \tag{3}$$

and N/N' is abelian. Therefore, by (2), $A \cap N$ is a normal subgroup of B, and now from (3), (2), and the fact that N' is a maximal normal subgroup of A we deduce that

$$A \cap N = N'.$$

This proves that A is almost normal in B, in other words, that G has the property $(\mathfrak{D})$.

Generalized solvable groups. The concept of a solvable series of a group is easily generalized to the concepts of a *solvable normal system* and of a *solvable invariant system*, that is, a normal or an invariant system with abelian factors. This leads to the following very broad generalizations of solvable groups.

A group G is called an *SN-group* if it has a solvable normal system, and an *SI-group* if it has a solvable invariant system. The problem whether these two classes of groups coincide is still open.

Other forms of the definition of solvable and finite solvable groups also lend themselves to corresponding generalizations, and the classes of groups so obtained cease to be identical. The class of SN-groups is the widest. We shall describe these classes of groups and some of their properties below, but for additional details we refer the reader to the paper by Kuroš and Černikov [1].

The definition of a solvable group by means of the derived series leads to the concept of an *SD-group*, that is, a group whose derived series, possibly continued transfinitely, contracts to the unit subgroup. SD-groups are SI-groups and therefore are SN-groups.

In § 36 we showed that free groups are SD-groups, and since every group can be represented as factor group of a free group, the factor group of SD-groups (and also of SI-groups and SN-groups) need not belong to the corresponding class. By contrast, the subgroups of SD-, SI-, and SN-groups have the corresponding property. This is obvious for SD-groups; and for SI-groups and SN-groups it follows from the subgroup theorem proved in the preceding section.

Narrower than the classes of SN- and SI-groups are those of $\overline{SN}$- and $\overline{SI}$-groups, that is, groups for which every composition (or principal) system is solvable. *These classes are also closed with respect to formation of factor groups.* Suppose, for example, that G is an $\overline{SI}$-group and that an arbitrary principal system in the factor group G/H is given. There corresponds to it an invariant system of G passing through H. Completing this to a principal system, bearing in mind that it must be solvable, and going over to the factor group G/H, we see that the given principal system of the factor group is solvable.

Closely related to $\overline{SI}$-groups, and possibly identical with them, are the groups studied in a paper by Schmidt [7], namely groups in which every factor group of every subgroup is an SI-group. Another class of groups

we could consider is the class of groups having property ($\mathfrak{D}$) (see above).

Finally, we introduce the classes of *SN*-groups* and *SI*-groups*. They are the groups that have a solvable ascending normal and invariant series, respectively.

The classes of SN- and SI*- groups are closed with respect to subgroups*; this follows from the theorem on subgroups (see § 56).

They are also closed with respect to factor groups. For suppose that in a group G having a solvable ascending normal (or invariant) series $\mathfrak{A}$ a normal subgroup H is given. To the series $\mathfrak{A}$ and the normal (and even invariant) series

$$E \subset H \subset G \tag{4}$$

we apply the theorem of § 56 on the existence of isomorphic refinements, which are themselves ascending normal (or invariant) series: we refine (4) to a solvable series. Hence there follows the existence of a solvable ascending normal (or invariant) series in G/H.

Every SI-group is an $\overline{SI}$-group.* For if $\mathfrak{A}$ is a solvable ascending invariant series of a group G, and $\mathfrak{B}$ an arbitrary invariant system of G, then by the theorem of § 56 there exist invariant refinements $\overline{\mathfrak{A}}$ and $\overline{\mathfrak{B}}$ of these systems such that the totality of factors of $\overline{\mathfrak{B}}$ is part of the totality of factors of $\overline{\mathfrak{A}}$. The system $\overline{\mathfrak{A}}$, as a refinement of a solvable series, is itself solvable, and therefore $\overline{\mathfrak{B}}$ is also solvable. Hence it follows that all principal systems of G are solvable.

Similarly, we can show that *every SN*-group is an $\overline{SN}$-group.* Again, whether these two classes of groups are identical is an open problem.

Finally, by a repetition of the arguments we have used to prove that finite solvable groups have the property ($\mathfrak{D}$), we can show that *every SI*-group has the property* ($\mathfrak{D}$).

§ 58. Local theorems. Locally solvable groups

The following local theorem of Mal'cev holds in generalized solvable groups (see Mal'cev [3], Kuroš and Černikov [1]).

Every group having one of the properties SN, SI, $\overline{SN}$, or $\overline{SI}$ locally is itself an SN-, SI-, $\overline{SN}$-, or $\overline{SI}$-group.

We shall deal with each of the four statements separately.

Proof of the local theorem for SN-groups. Suppose that L is a local system of subgroups of a group G and that all the subgroups A^{α}, A^{β}, ...

of the system are SN-groups. In every subgroup A^α of L we label a definite solvable normal system $\mathfrak{S}^\alpha$.

Let a and b be any two elements of G. For every α for which A^α contains both these elements there exists a largest subgroup in $\mathfrak{S}^\alpha$ that fails to contain at least one of the elements a, b; we denote this subgroup by $C^\alpha_{a,b}$. If $\overline{C}^\alpha_{a,b}$ is the smallest subgroup of $\mathfrak{S}^\alpha$ that contains both a and b, then the subgroups $C^\alpha_{a,b}$, $\overline{C}^\alpha_{a,b}$ form a jump in $\mathfrak{S}^\alpha$ with an abelian factor, so that *the commutator* $[a, b]$ *belongs to* $C^\alpha_{a,b}$.

All the subgroups A^α of L containing a and b belong to one of the following three classes: the corresponding subgroup $C^\alpha_{a,b}$ either contains a but not b, or contains b but not a, or contains neither a nor b. *At least one of these three classes is a local system of subgroups of* G.

For suppose that for each of the three classes we can find a "contradictory" element in G, not contained in any subgroup of this class, or a pair of "contradictory" subgroups, belonging to the class but not contained in any third subgroup of the class. By the definition of a local system of subgroups, we can find a subgroup A^α in L containing a and b as well as these "contradictory" elements and subgroups for all three classes. However, the subgroup A^α must belong to one of the three classes in question, and this leads to a contradiction.

Every local system of subgroups obtained in this way will be said to be *linked with the pair of elements* (a, b); there will be one, two, or three such local systems.

We now choose two pairs of elements, (c, d) and (c', d'). Every subgroup A^α of L containing all these elements belongs to at least one of the following two classes: either

$$C^\alpha_{c,d} \subseteq C^\alpha_{c',d'},$$

or else

$$C^\alpha_{c,d} \supseteq C^\alpha_{c',d'}.$$

As above we can show that *at least one of these two classes is a local system of subgroups of* G. This will be a local system *linked with the set of pairs* (c, d), (c', d'), and there are one or two of them.

We define the *intersection* of several local systems as the system of subgroups belonging to every one of the given local systems. If a finite number of pairs (a_i, b_i), $i = 1, 2, \ldots, n$ is given, and a finite number of sets of pairs (c_j, d_j), (c_j', d_j'), $j = 1, 2, \ldots, m$, then *we can select in at least one way, from all the local systems linked with each of these pairs and sets of*

pairs, one system each such that their intersection is also a local system of subgroups of G.

For suppose that for each of these intersections—and there is only a finite number of them—we can find a "contradictory" element or pair of elements, in the above-defined sense. We also choose "contradictory" elements or pairs of subgroups for all these classes with respect to each pair (a_i, b_i) and each set of pairs (c_i, d_i), (c_i', d_i') which are not local systems linked with these pairs or sets of pairs. However, in L there exists a subgroup A^α containing all "contradictory" elements and subgroups enumerated in this paragraph as well as all elements of the given pairs and sets of pairs. For obviously each of these pairs or sets of pairs A^α will belong to one of the local systems linked with that pair or set of pairs and will therefore belong to the intersection of all these local systems. However, this contradicts the fact that A^α contains an element or pair of subgroups "contradictory" to the intersection in question.

On the basis of this result we can show that *for every pair* (a, b) *and every set of pairs* (c, d), (c', d') *we can choose at least one local system of G linked with it*—denoted by $L_{(a,b)}$ and $L_{(c,d),\,(c',d')}$ respectively—*such that the intersection of any finite number of these local systems is itself a local system of subgroups of G.*

For the proof, we shall regard the set $\mathfrak{M}$ of all pairs and sets of pairs as well-ordered and shall proceed by induction with respect to this set $\mathfrak{M}$. Suppose that the α-th element of $\mathfrak{M}$ is taken $(\alpha > 1)$ and that for all the preceding elements we have *labelled* one of the local systems linked with it so as to satisfy the following conditions: For any finite number of labelled systems $L', L'', \ldots, L^{(k)}$ and any finite number of elements of $\mathfrak{M}$ standing, for example, in the α'-th, α''-th, $\ldots$, $\alpha^{(l)}$-th places we can choose for these latter elements local systems linked with them,

$$L_0^{(\alpha')}, L_0^{(\alpha'')}, \ldots, L_0^{(\alpha^{(l)})}$$

such that the intersection of the local systems

$$L', L'', \ldots, L^{(k)}, L_0^{(\alpha')}, L_0^{(\alpha'')}, \ldots, L_0^{(\alpha^{(l)})}$$

is itself a local system of subgroups of G. Then we can also label for the α-th element of $\mathfrak{M}$ one of the finite number of local systems linked with it such that the property of labelled local systems just indicated remains valid. For if we can find for every local system linked with the α-th element a "contradictory" finite collection of local systems and elements

of $\mathfrak{M}$, then taking the union of all these collections and including the α-th element itself, we arrive at a contradiction to the induction hypothesis.

The set of all local systems $L_{(a,\,b)}$ and $L_{(c,\,d),\,(c',\,d')}$ will be denoted by $\mathfrak{S}$.

We now proceed to the construction of a solvable normal system of G. We choose an arbitrary pair of elements (a, b) and define a subgroup $H_{a,b}$ of G as follows:

1. We take the intersection of the local system $L_{(a,\,b)}$ and an arbitrary finite set of other local systems of $\mathfrak{S}$; this is, as we know, a local system.

2. We take the intersection of the subgroups $C^{\alpha}_{a,\,b}$ for all those A^{α} that belong to the local system constructed under 1.

3. We take the union of all the intersections described under 2. that are obtained for the fixed pair (a, b), but for the various local systems constructed under 1., and we denote this union by $H_{a,b}$.

$H_{a,b}$ is actually a subgroup, because any two intersections of the form described under 2. are contained in a third intersection of the same form.

The subgroup $H_{a,b}$ either contains only one of the elements a, b or neither; however, it always contains their commutator $[a, b]$. For this is precisely a property of the subgroup $C^{\alpha}_{a,\,b}$, for all A^{α} that belong to the local system

The set $\mathfrak{H}$ of subgroups $H_{a,b}$, constructed for all pairs (a, b), is ordered by set-theoretical inclusion. For let us choose subgroups $H_{(a,\,b)}$ and $H_{(c,\,d)}$. By definition of the local system $L_{(a,\,b),\,(c,\,d)}$, only one of the two possible inclusions $C^{\alpha}_{a,\,b} \subseteq C^{\alpha}_{c,\,d}$ or $C^{\alpha}_{a,\,b} \supseteq C^{\alpha}_{c,\,d}$ can hold for all A^{α} occurring in the system; suppose it is the first. However, since the intersections described under point 2. of the definition of $H_{a,b}$ can only increase if we add the system $L_{(a,\,b)\,(c,\,d)}$ to the local systems described under 1., we find that

$$H_{a,\,b} \subseteq H_{c,\,d}.$$

Omitting all repetitions from the ordered system of subgroups $\mathfrak{H}$ and completing it by the unions and intersections of all its subsets, we obtain a well-ordered system of subgroups $\overline{\mathfrak{H}}$.

The subgroup E belongs to $\overline{\mathfrak{H}}$. For if a is an element of G other than the unit element, then the subgroup $H_{1,a}$, which certainly contains the unit element, cannot contain a. Hence the intersection of all the subgroups of $\mathfrak{H}$ is E.

However, we cannot show that G itself belongs to $\overline{\mathfrak{H}}$, since the union G' of all subgroups of $\mathfrak{H}$ may be different from G. Nevertheless if we take two elements a, b, of G, then we know that their commutator belong to $H_{a,b}$

and hence to G'. For the proof of the theorem it only remains, therefore, to show that *the complete system* $\overline{\mathfrak{H}}$ *is a solvable normal system of* G'.

The system $\overline{\mathfrak{H}}$ *is normal.* For let $\overline{H}_\beta$, $\overline{H}_{\beta+1}$ be an arbitrary jump in it. If the elements a, b are such that

$$a \in \overline{H}_\beta, \qquad b \in \overline{H}_{\beta+1}, \qquad b \notin \overline{H}_\beta,$$

then $H_{a,b} \subseteq \overline{H}_\beta$, since otherwise the subgroup $H_{a,b}$, which belongs to $\overline{\mathfrak{H}}$, would contain $\overline{H}_{\beta+1}$, that is, would contain both a and b. However, since $[a, b]$ is contained in $H_{a,b}$, it belongs to $\overline{H}_\beta$ and so, as $a \in \overline{H}_\beta$, the element $b^{-1}ab$ also lies in $\overline{H}_\beta$. This proves that $\overline{H}_\beta$ is a normal subgroup of $\overline{H}_{\beta+1}$.

The system $\overline{\mathfrak{H}}$ *is solvable.* For let $\overline{H}_\beta$, $\overline{H}_{\beta+1}$ be a jump in the system with a non-abelian factor. This means that we can find elements a, b in $\overline{H}_{\beta+1}$ such that they and their commutator both lie outside $\overline{H}_\beta$. But this is impossible, because $H_{a,b}$ contains $[a, b]$ and, moreover, cannot contain both a and b; in other words, $H_{a,b}$ is itself contained in $\overline{H}_\beta$, so that $[a, b] \in \overline{H}_\beta$. This completes the proof of the theorem.

Proof of the local theorem for SI-groups. This can be conducted by the same method. We only have to show that *every subgroup* $H_{a,b}$ *is normal in* G.

Let c be an arbitrary element of $H_{a,b}$, and let d be an arbitrary element of G. The definition of $H_{a,b}$ shows that c is contained in the intersection of the subgroups $C^{\alpha}_{a,b}$, taken for all A^α that form the intersection of the local system $L_{(a,b)}$ with a certain finite number of other local systems of the set $\mathfrak{S}$. We know that we can assume here that the system $L_{(a,b),(c,d)}$ belongs to these local systems. Therefore all these subgroups A^α contain d, and since $C^{\alpha}_{a,b}$ is now a normal subgroup of A^α, all the subgroups $C^{\alpha}_{a,b}$ in question, and therefore their intersection, contain the element $d^{-1}cd$. This element belongs, then, to $H_{a,b}$, and this is what we had to prove.

Proof of the local theorem for $\overline{SI}$*-groups.* Let L be a local system of subgroups of a group G and suppose that all the subgroups A^α of the system are $\overline{SI}$-groups. Since every invariant system can be refined to a principal system, it is sufficient to prove the following statement:

If B_1 *and* B_2 *are normal subgroups of our group* G, *if* B_1 *is contained in* B_2, *and if the factor group* B_2/B_1 *is non-commutative, then between* B_1 *and* B_2 *there can be inserted a normal subgroup* C *of* G, *distinct from* B_1 *and* B_2.

From the fact that B_2/B_1 is non-commutative it follows that there are two elements x and y in B_2 such that B_1 contains neither these elements

themselves nor their commutator $[x, y]$. If A^α is an arbitrary subgroup in the local system L containing x and y, then the intersections

$$B_1^\alpha = A^\alpha \cap B_1, \qquad B_2^\alpha = A^\alpha \cap B_2$$

are normal in A^α; moreover B_1^α is contained in B_2^α and is distinct from it, since the elements x, y, and $[x, y]$ belong to B_2^α but not to B_1^α.

Since A^α is an $\overline{SI}$-group, its invariant system

$$E \subseteq B_1^\alpha \subset B_2^\alpha \subseteq A^\alpha$$

can be refined to a solvable principal system. We take one of these refinements. We can find in it a jump C^α, $\overline{C}^\alpha$ such that $\overline{C}^\alpha$ contains both elements x and y and C^α contains no more than one of them; but C^α contains their commutator $[x, y]$, because $\overline{C}^\alpha / C^\alpha$ is commutative. Thus

$$B_1^\alpha \subset C^\alpha \subset \overline{C}^\alpha \subseteq B_2^\alpha.$$

We shall assume that for every A^α of L containing x and y a normal subgroup C^α is constructed in this way. Then all these subgroups A^α can be divided into the following three classes: the corresponding normal subgroup C^α either contains x but not y, or contains y but not x, or contains neither x nor y. As in the proof of the preceding theorem, we can show that *at least one of these three classes is a local system of subgroups of* G. We select one of these local systems, denote it by L', and use in what follows only the subgroups A^α belonging to L'.

We denote by C the set of all elements z of G with the following property: in the local system L' we can find a subgroup A^α such that for every subgroup $A^{\alpha'}$ of L' containing A^α the element z belongs to the normal subgroup $C^{\alpha'}$.

The set C is a subgroup of G. For if z_1 and z_2 are elements of C, then there are subgroups A^{α_1} and A^{α_2} in L' such that z_i, $i = 1, 2$, is contained in C^α for every subgroup A^α containing A^{α_i}. However, in L' there is a subgroup A^{α_3}, containing both A^{α_1} and A^{α_2}. Thus, for every subgroup A^α in L' containing A^{α_3}, the normal subgroup C^α contains both z_1, z_2, and hence their product and their inverses.

The subgroup C is normal in G. For let $z \in C$, $g \in G$. If A^α is a subgroup in L' such that for every subgroup $A^{\alpha'}$ containing A^α the element z belongs to $C^{\alpha'}$, and if A^{α_1} is a subgroup in L' containing A^α and g, then for every subgroup A^{α_2} containing A^{α_1} the normal subgroup C^{α_2} contains not only z but also $g^{-1}zg$, so that $g^{-1}zg \in C$.

The normal subgroup C lies between B_1 and B_2. For if b is an element of B_1 and if it is contained in a subgroup A^α of L' and hence in all subgroups $A^{\alpha'}$ containing A^α, then it must belong to $B_1^{\alpha'}$ for all these α' and, therefore, to $C^{\alpha'}$. This shows that $b \in C$. On the other hand, if z belongs to C, then there exists a subgroup A^α such that $z \in C^\alpha \subset B_2^\alpha$, so that $z \in B_2$.

The normal subgroup C is distinct from B_1 and B_2. To prove this, we have to consider separately every one of the three cases that can arise in the choice of the local system L'. If this system consists of subgroups A^α of the first class, that is, of subgroups for which the corresponding normal subgroup C^α contains x but not y, then C also contains x and hence is distinct from B_1, but does not contain y and hence is distinct from B_2. A similar argument applies to the case in which L' consists of subgroups A^α of the second class. But if L' consists of subgroups of the third class—that is, of subgroups for which the corresponding C^α contains neither x nor y but does contain their commutator $[x, y]$—then the normal subgroup C also contains neither x nor y and hence is distinct from B_2, but does contain $[x, y]$ and hence is distinct from B_1. This completes the proof of the theorem.

Proof of the local theorem for $\overline{SN}$-groups. This merely requires a combination of the methods used in the proof of the preceding theorems and will be omitted.

The problem whether the local theorem holds for SN^*-groups is still open.

For SI^*-groups and SD-groups the local theorems do not hold. This is shown by examples of locally finite p-groups without abelian normal subgroups (Schmidt [7]) and of locally finite p-groups coinciding with their derived group (Ado [1], Schmidt [7]).

For solvable groups the local theorem, obviously, cannot hold. This leads to the following important class of generalized solvable groups: a group G is called *locally solvable* if it has a local system of solvable subgroups. Since every subgroup of a solvable group is solvable this is equivalent to the postulate that every finitely generated subgroup of G is solvable.[1]

It is obvious that locally solvable groups belong to every class of generalized solvable groups for which the local theorem holds. Generally speaking, the classes of SN^*-, $\overline{SN}$-, and $\overline{SI}$-groups and of locally solvable groups, and also the groups with the property $(\mathfrak{D})$ and the groups studied in the paper by Schmidt [7] are very close to one another, and it would be interesting to clarify precisely the relations among them.

[1] In the definition of locally solvable groups local finiteness is not assumed.

§ 59. Solvable groups with finiteness conditions

New links appear between the classes of generalized solvable groups investigated above if it is assumed in addition that the groups are subject to finiteness conditions (see § 53) of one kind or another. We mention some results of this type.

Under the condition of local finiteness, all classes of generalized solvable groups for which the local theorem holds coincide with the class of locally solvable groups and are therefore identical.

For if G is a locally finite SN-group, then all its finite subgroups are solvable, and it is therefore locally solvable.

The Burnside problem on periodic groups is not yet solved even for SN-groups. Only the following theorem has been proved so far (Černikov [4], Baer [24]; for the proof, see Schmidt [7]).

Every periodic SN^*-group is locally finite.

This theorem follows immediately from the fact that a periodic abelian group is locally finite, that an extension of a locally finite group by a locally finite group is itself locally finite (see § 53), and that the union of an ascending sequence of locally finite groups is itself locally finite.

From this theorem it follows that *every periodic solvable group is locally finite* and therefore that *every periodic locally solvable group is locally finite.*

We shall now prove the following theorem (Černikov [7]).

Every SI-group (in particular, every solvable group) G having a finite number of classes of conjugate elements is finite.

For it is obvious that no group with a finite number of classes of conjugate elements can have an infinite invariant system, so that G must be solvable. Let

$$E \subset H_1 \subset \ldots \subset H_{k-1} \subset H_k = G \tag{1}$$

be an arbitrary solvable normal series of G. The factor G/H_{k-1}, as a factor group of a group with a finite number of classes of conjugate elements, has itself a finite number of classes of conjugate elements. Since it is, moreover, abelian we see that G/H_{k-1} *is a finite group.*

Let us show that H_{k-1} *has a finite number of classes of conjugate elements.* If this were not so, then we could find in H_{k-1} an infinite set of elements

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

no two of which are conjugate in H_{k-1}, whereas they are all conjugate in G

and hence lie in one class. Therefore there are elements x_i in G such that

$$x_i^{-1} a_i x_i = a_1, \qquad i = 2, 3, \ldots. \tag{2}$$

Since G/H_{k-1} is finite, we can find indices i and j, $i \neq j$, such that

$$x_i H_{k-1} = x_j H_{k-1},$$

and hence

$$x_j = x_i h_{k-1}, \qquad h_{k-1} \in H_{k-1}. \tag{3}$$

From (2) and (3) we deduce that

$$a_i = (x_i h_{k-1} x_i^{-1})^{-1} a_j (x_i h_{k-1} x_i^{-1}),$$

and since the element $x_i h_{k-1} x_i^{-1}$ lies in the normal subgroup H_{k-1}, a_i, and a_j turn out to be conjugate, contrary to assumption.

Now we can prove that H_{k-1}/H_{k-2} is finite and, continuing the process, that all factors of (1) are finite. Hence G is finite, and the theorem is proved.

The following theorem of Cernikov [4, 5] on *solvable groups with minimal condition for subgroups* completely reduces the classification of these groups to that of finite solvable groups.

Every SN-group with minimal condition for subgroups is solvable. A group G is a solvable group with minimal condition for subgroups if and only if it is an extension of a complete abelian group with minimal condition for subgroups by a finite solvable group.

Proof (see Schmidt [7]). Let G be an SN-group with minimal condition for subgroups. By the minimal condition every solvable normal system of G must be ascendingly well-ordered, so that G is an SN^*-group. Again by the minimal condition G is periodic and, as a periodic SN^*-group, G is even locally finite. However, we have shown above that in the locally finite case every SN-group is an SI-group, so that G is an SI-group and therefore, again by the minimal condition, is even an SI^*-group.

By the minimal condition, G has a minimal subgroup F of finite index containing no subgroup of finite index. F is the only subgroup of this kind, since the intersection of two subgroups of finite index has itself finite index. Therefore F is a normal subgroup of G. Let us show that *the center Z of F is different from E.*

As a subgroup of an SI^*-group, F is itself an SI^*-group and therefore has an abelian normal subgroup A other than E. It follows from the classification of abelian groups with minimal condition given in § 53 that A con-

tains only a finite number of elements of any given order and therefore, since A is a normal subgroup, that the normalizer in F of every element of A has finite index in F, so that it must be equal to F. Hence it follows that A lies in the center of F, $A \subseteq Z$, and so $Z \neq E$.

We shall now show that Z is equal to F. Suppose that $Z \neq F$. Then F/Z as a factor group of an SI^*-group is itself an SI^*-group. Furthermore it satisfies the minimal condition and, like F, contains no proper subgroup of finite index. The arguments of the preceding paragraph are therefore applicable to F/Z, so that F/Z must have a non-trivial center Z'/Z, $Z' \neq Z$. If z' is an arbitrary element of Z', then every element z'' conjugate to z' in F is contained in the coset $z'Z$, that is, has the form

$$z'' = z'z, \quad z \in Z.$$

Since the elements z' and z'' have the same order and

$$zz' = z'z,$$

the order of z must divide the order of z'. There can only be a finite number of such elements z in the abelian group Z with minimal condition, so that z' has only a finite number of conjugates in F. It follows that the normalizer of z' in F has finite index in F and is therefore equal to F, so that $z' \in Z$. This contradiction to the inequality $Z' \neq Z$ shows that $Z = F$.

Thus F has turned out to be an abelian normal subgroup of G. As an abelian group with minimal condition containing no proper subgroup of finite index, F is complete and, by § 53, is the direct product of a finite number of groups of type p^∞ for certain prime numbers p.

Furthermore, the factor group G/F is finite and at the same time is an SI^*-group, that is, a finite solvable group. Therefore G, as an extension of an abelian group by a solvable group, is itself solvable.

To complete the proof, we mention that an extension of an arbitrary abelian group with minimal condition by a finite solvable group is itself solvable and (see § 53) satisfies the minimal condition for subgroups.

From the theorem of Černikov it follows, in particular, that *every solvable group with minimal condition for subgroups is countable.*

The following statement is obvious: A solvable group satisfies the minimal condition for subgroups if and only if all the factors in its solvable normal series are abelian groups with minimal condition.

We mention, further (see Schmidt [7], Černikov [21]), that for periodic solvable groups and for some more general classes of groups the minimal

condition for abelian subgroups implies the minimal condition for all subgroups. On the other hand (see Čarin [1]), for periodic solvable groups the minimal condition for normal subgroups does not imply the minimal condition for all subgroups.

For *solvable groups with maximal condition for subgroups* the results so far obtained are less complete. These groups are studied in papers by Hirsch [1, 2, 4, 6, 7] and Zappa [2, 4]. Mal'cev [10] has proved that for solvable groups the maximal condition for abelian subgroups implies the maximal condition for all subgroups. We mention the following result (Hirsch [1]).

If a solvable group G has a solvable normal series in which all factors are finitely generated abelian groups, then it satisfies the maximal condition for subgroups. Conversely, if a group G satisfies the maximal condition for subgroups, then all factors in all solvable normal series of G are finitely generated; that is, these series can be refined to normal series with cyclic factors.

For suppose that every factor in the solvable series of G

$$G = G_0 \supset G_1 \supset \ldots \supset G_{n-1} \supset G_n = E \tag{4}$$

has a finite number of generators. We show, first of all, that G is a finitely generated group. This statement is true for the group $G_{n-1} = G_{n-1}/E$. If we have already proved that G_i is a finitely generated group, then we prove it for G_{i-1} in the following way: We take a finite system of generators in the factor group G_{i-1}/G_i and choose a representative for each one in the corresponding cosets of G_i. The finite system so obtained, together with a system of generators of G_i, generates the whole group G_{i-1}. This proves that all the groups G_i, and among them $G_0 = G$, are finitely generated.

If H is an arbitrary subgroup of G, then H has a normal series whose factors are isomorphic to subgroups of some of the factors in (4), so that, by § 20, they are themselves finitely generated abelian groups. Hence it follows that every subgroup of G is also finitely generated, so that by what we have proved in § 53 every ascending chain of subgroups breaks off.

The converse statement is clear: If the ascending chains of subgroups of a solvable group break off, then it follows that all subgroups of the group are finitely generated; therefore all the factor groups of the latter and, among them, all the factors of an arbitrary solvable series are also finitely generated. Every one of these factors therefore has a finite normal series with cyclic factors. The last part of the theorem follows from this.

This result and the above-mentioned analogous result for solvable groups with minimal condition show that it is appropriate to study special classes of solvable groups defined by restrictions of one kind or another imposed on the factors of the solvable series of the groups. For example, Mal'cev [10] has obtained a number of results relating to solvable groups in which all the factors of the solvable series are abelian groups of finite rank and also results relating to narrower classes of solvable groups; see also Smirnov [1].

§ 60. Sylow Π-subgroups of solvable groups

Let G be a finite group of order n, and let n be written as the product of two co-prime factors

$$n = kl, \quad (k, l) = 1.$$

We denote by Π the set of all the prime numbers by which k is divisible. It is clear that the order of every Sylow Π-subgroup of G is a divisor of k. It is not clear, however, that it has to be equal to k; and in general G need not contain subgroups of order k. We shall show below that in the case of a finite *solvable* group we have another situation: *All Sylow* Π*-subgroups of a finite solvable group are of order* k *and are conjugate.*

First we wish to prove the following theorem of Hall (see P. Hall [1]; other proofs are in the book by Zassenhaus [2] and in papers by Ore [9] and Goheen [1]).

HALL'S FIRST THEOREM. *If* k *divides the order* n *of a finite solvable group* G *and if*

$$n = kl, \quad (k, l) = 1, \tag{1}$$

then G *has subgroups of order* k*, and all these subgroups are conjugate.*[1]

We shall give yet another formulation of Hall's Theorem. First we introduce the following definition.

[1] P. Hall [4] and Čunihin [1] have proved that the converse is also true, even in the following form: *If a finite group* G *has subgroups of order* k *for all divisors* k *of its order* n *for which* (1) *holds and for which the corresponding complement* l *is a power of a prime number, then* G *is solvable.*

The proof of this theorem is based on the following *Theorem of Burnside*, which is a special case of it: *Every finite group whose order is divisible by only two distinct prime numbers is solvable.* The proof of this last theorem uses a method that falls outside the scope of the present book, namely the theory of characters of finite groups.

Let Π be a set of some (not necessarily all) prime numbers that occur in the order n of a finite group G. A *Sylow Π-basis* $\mathfrak{S}$ of G is a collection of Sylow p-subgroups P_p of G, one for each p of Π, satisfying the following condition: If

$$P_{p_1}, P_{p_2}, \ldots, P_{p_r}$$

are some of the subgroups occurring in $\mathfrak{S}$, then the order of every element in the subgroup

$$\{P_{p_1}, P_{p_2}, \ldots, P_{p_r}\},$$

generated by them is a product of non-negative powers of the prime numbers $p_1, p_2, \ldots, p_r$.

If the set Π consists of all the prime divisors of the order n of G, then a Sylow Π-basis is called a *complete Sylow basis* of G. The subgroups forming a complete Sylow basis generate the whole group G.

Two Sylow Π-bases $\mathfrak{S}_1$ and $\mathfrak{S}_2$ of G are called *conjugate* if there is an element in G that transforms all the subgroups of $\mathfrak{S}_1$ into the corresponding subgroups of $\mathfrak{S}_2$.

If Π is an arbitrary set of prime numbers and Π_0 the subset consisting of all those prime numbers of Π that occur in the order of a finite group G, then we shall understand by a Sylow Π-basis simply a Sylow Π_0-basis of G.

Then the following theorem (P. Hall [6]) holds:

HALL'S SECOND THEOREM. *Every finite solvable group has a complete Sylow basis and all these bases are conjugate.*[1]

We shall deduce both theorems of Hall from some more general theorems. Let Π be an arbitrary non-empty set of prime numbers. Following S. A. Čunihin we shall call a finite group G *Π-separable* if it has a normal series in which the order of every factor is divisible by not more than one prime number in Π. In particular, if Π consists of all the prime numbers or at least of all those that occur in the order of G, then a Π-separable group is solvable, because it has a normal series in which all the factors are p-groups. Conversely, every solvable group is Π-separable for such a choice of Π. In the other extreme case, when Π consists of one prime number only, every finite group G is Π-separable.

From the subgroup theorem of § 16 it follows that *every subgroup of a Π-separable group is itself Π-separable.*

[1] Hall has also proved the following converse theorem: *If a finite group has a complete Sylow basis, then it is solvable.*

Now the following theorem (Čunihin [4, 6]) holds.

ČUNIHIN'S THEOREM: *If k is a divisor of the order n of a finite Π-separable group G such that*

$$n = kl, \quad (k, l) = 1,$$

and if all the prime divisors of k occur in Π, then G has a subgroup of order k, and all these subgroups are conjugate in G.

If the set Π consists of all the prime numbers, then this theorem turns into Hall's First Theorem and, if Π consists of a single prime number p, it turns into the fundamental statement of Sylow's Theorem, which was proved in § 54.

We shall prove the following theorem (Gol'berg [3]), which is even more general.

GOL'BERG'S THEOREM. *If G is a finite Π-separable group and Π' an arbitrary subset of Π, then G has Sylow Π'-bases, and all these bases are conjugate.*

This theorem turns into Hall's Second Theorem if Π consists of all the prime divisors of the order of G and $\Pi' = \Pi$. Let us show that *it also implies Čunihin's Theorem.*

Let k be a number as indicated in Čunihin's Theorem. If Π' is the set of all the prime divisors of k, then by Gol'berg's Theorem G has a Sylow Π'-basis $\mathfrak{S}'$. The subgroup A of G generated by all the subgroups in $\mathfrak{S}'$ has order k: for the order of A is obviously divisible by k, but the order of every element of A itself is a divisor of k. Now if A_1 and A_2 are any two subgroups of order k of the Π-separable group G, then they are Π'-separable (see the Subgroup Theorem of § 16) and therefore solvable. By Hall's Second Theorem, which follows, as we have pointed out above, from Gol'berg's Theorem, A_1 and A_2 have complete Sylow bases $\mathfrak{S}_1'$ and $\mathfrak{S}_2'$. These will be Sylow Π'-bases for G; by Gol'berg's Theorem they are conjugate; and therefore the subgroups A_1 and A_2 generated by them are also conjugate.

Proof of Gol'berg's Theorem. Without loss of generality we can assume that all the prime numbers of Π divide the order of the finite Π-separable group G, and we shall prove the theorem by induction over the order of the group. Let the subset Π' consist of the prime numbers

$$p_1, p_2, \ldots, p_k, \quad k \geqq 1.$$

If $k = 1$, then all parts of the theorem follow from Sylow's Theorem; we therefore put $k > 1$.

In this case Π contains not fewer than two prime numbers; therefore the definition of a Π-separable group shows that G has a *non-trivial* normal subgroup H whose index in G is divisible by not more than one prime number of Π. If this index is not divisible by any prime number of Π', then a Sylow Π'-basis of H, which exists by the induction hypothesis, is also a Sylow Π'-basis of G. On the other hand, every Sylow Π'-basis of G is contained in H and therefore, again by the induction hypothesis, all these bases are conjugate in H.

Now let the index of the normal subgroup H of G be divisible by a prime number p_1 of Π'. We assume that $p_1^{\alpha_1}$ and $p_1^{\alpha_1'}$ are the highest powers of p_1 that occur in the order of G and H, respectively:

$$\alpha_1 > \alpha_1' \geqq 0.$$

By assumption, H has a Sylow Π'-basis

$$P_1', P_2, \ldots, P_k, \tag{2}$$

where P_i, $i = 2, 3, \ldots, k$ is a Sylow p_i-subgroup of G and where P_1' is of order $p_1^{\alpha_1'}$. We denote by $N(G)$ and $N(H)$ the normalizers of the set-theoretical union of the subgroups (2) in G and H, respectively. As H is normal in G and all Sylow Π'-bases of H are conjugate, the indices of these normalizers in G and H must be equal; let them be divisible by p_1^{β}, $\beta \geqq 0$.

The intersection $P_1' \cap N(H)$ is a Sylow p_1-subgroup of $N(H)$—otherwise P_1' would not be a Sylow p_1-subgroup of H—and it is therefore of order $p_1^{\alpha_1'-\beta}$. We supplement this intersection to a Sylow p_1-subgroup P_1'' of $N(G)$; it is of order $p_1^{\alpha_1-\beta}$. Since

$$P_1'P_1'' = P_1''P_1',$$

the subgroup $P_1 = P_1'P_1''$ is a p_1-subgroup. Its order is equal to

$$p_1^{\alpha_1'+(\alpha_1-\beta)-(\alpha_1'-\beta)} = p_1^{\alpha_1},$$

so that it is a Sylow p_1-subgroup of G. Finally, since $P_i P_1'' = P_1'' P_i$, $i = 2, 3, \ldots, k$, the system of subgroups

$$P_1, P_2, \ldots, P_k \tag{3}$$

is a Sylow Π'-basis of G.

Now let two Sylow Π'-bases of G be given, say (3) and

$$Q_1, Q_2, \ldots, Q_k. \tag{4}$$

The intersections $P_1 \cap H$ and $Q_1 \cap H$ are Sylow p_1-subgroups of H; hence

$$P_1 \cap H, \; P_2, \ldots, P_k, \qquad Q_1 \cap H, \; Q_2, \ldots, Q_k$$

are Sylow Π'-bases of H, as one can easily verify. By assumption they are conjugate in H. Suppose that under the transformation by an element x the second of these bases goes over into the first. Then, under the transformation by the same element, (4) turns into a Sylow Π'-basis of G

$$R_1 = x^{-1} Q_1 x, \; P_2, \ldots, P_k. \tag{5}$$

It remains to prove that (3) and (5) are conjugate bases. Let

$$A = \{P_1, P_2, \ldots, P_k\}, \; B = \{R_1, P_2, \ldots, P_k\}.$$

From

$$x^{-1}(Q_1 \cap H)x = P_1 \cap H$$

follows

$$R_1 \cap H = P_1 \cap H,$$

and since $P_i \subset H$, $i = 2, 3, \ldots, k$, we have

$$A \cap H = B \cap H.$$

We denote this intersection by H'; it is a normal subgroup of A and of B, and hence of $\{A, B\}$. The Sylow p_1-subgroups P_1 and R_1 are conjugate in $\{A, B\}$, therefore the subgroups $A = \{H', P_1\}$ and $B = \{H', R_1\}$ are also conjugate. Thus, under the transformation the basis (5) goes over into a Sylow Π'-basis of A which is, however, conjugate to the basis (3)—at least if A is a proper subgroup of G.

But if $A = G$, then also $B = G$. Clearly this is only possible when $\Pi' = \Pi$ and Π consists of all prime divisors of the order of G. We put for $i = 2, 3, \ldots, k$:

$$A_i = \{P_1, P_2, \ldots, P_{i-1}, P_{i+1}, \ldots, P_k\},$$
$$B_i = \{R_1, P_2, \ldots, P_{i-1}, P_{i+1}, \ldots, P_k\}.$$

By what has been proved above, A_i and B_i are conjugate in G. Since now $G = B = B_i P_i$, we can find an element x_i in P_i

$$x_i \in P_i \tag{6}$$

such that

$$x_i^{-1} B_i x_i = A_i. \tag{7}$$

Let us show that for every j, $j = 2, 3, \ldots, k$, $j \neq i$,

$$x_i^{-1} P_j x_i = P_j. \tag{8}$$

By (6) we have

$$x_i^{-1} P_j x_i \subset \{P_i, P_j\}$$

and by (7)

$$x_i^{-1} P_j x_i \subset A_i.$$

Therefore

$$x_i^{-1} P_j x_i \subseteq \{P_i, P_j\} \cap A_i = P_j$$

by reference to the definition of a Sylow basis. Hence (8) follows.

The element

$$x = x_2 x_3 \ldots x_k$$

carries the basis (5) *into* (3). For it follows from (6) and (8) that

$$x^{-1} P_i x = P_i, \; i = 2, 3, \ldots, k.$$

On the other hand, (6) and (7) give for $i = 2, 3, \ldots, k$:

$$x^{-1} R_1 x = (x_{i+1} \ldots x_k)^{-1} x_i^{-1} (x_2 \ldots x_{i-1})^{-1} R_1 (x_2 \ldots x_{i-1}) x_i (x_{i+1} \ldots x_k) \subset$$
$$\subset (x_{i+1} \ldots x_k)^{-1} x_i^{-1} B_i x_i (x_{i+1} \ldots x_k) = (x_{i+1} \ldots x_k)^{-1} A_i (x_{i+1} \ldots x_k) = A_i.$$

Therefore $x^{-1} R_1 x$ lies in the intersection of all A_i, $i = 2, 3, \ldots, k$, that is, in P_1, and hence

$$x^{-1} R_1 x = P_1.$$

This completes the proof.

P. Hall [1] has also proved the following theorem.

If the order of the finite solvable group G has the form

$$n = kl, \quad (k, l) = 1,$$

then every subgroup of G whose order divides k is contained in a subgroup of order k.

We shall prove the theorem by induction on the order of the group. Let A be a subgroup of G whose order k_0 divides k. In G we choose a non-trivial normal subgroup H, whose order n' we write in the form

$$n' = k'l',$$

where k' and l' divide k and l, respectively; and we assume that

$$l' < l. \tag{9}$$

The order of the factor group G/H is

$$\frac{n}{n'} = \frac{k}{k'} \cdot \frac{l}{l'}.$$

The order of its subgroup AH/H divides k/k' so that, by the induction hypothesis, AH/H is contained in a subgroup F/H of order k/k'. Therefore the subgroup F of G has the order kl' and is, by (9), different from G. Applying the induction hypothesis once more, this time to F, we see, since $A \subset F$ and the order of F is divisible by k, that A is contained in a subgroup of order k.

But suppose that we cannot find a normal subgroup H of G with the property (9), so that the order of every non-trivial normal subgroup is divisible by l. We now denote by H the smallest term other than E in a principal series of G. H must be abelian and its order is a power of a prime number—otherwise H would not be a minimal normal subgroup of G. We know that this order is divisible by l and hence it is simply equal to l.

The subgroup AH now is of order $k_0 l$, and $(k_0, l) = 1$. Furthermore, by Hall's First Theorem proved earlier in this section, G has a subgroup B of order k. Since

$$\{AH, B\} = HB = G,$$

the intersection

$$AH \cap B = A'$$

is a subgroup of order k_0. Applying Hall's Theorem again, but to the subgroup AH, we find that A and A' are conjugate

$$x^{-1}A'x = A.$$

Then $x^{-1}Bx$ is a subgroup of order k containing A.

This completes the proof. The corresponding theorem for Π-separable groups has not yet been obtained.

From the theorem just proved the statement made in the first paragraph of the present section follows immediately.

The transition to *infinite* groups has been made in papers by Baer [25] and Gol'berg [2], where Hall's Theorems proved in this section are extended to locally normal and locally solvable groups. For this purpose either the methods explained in § 55, or closely related methods, are used.

In the problem of conjugacy of Sylow Π-subgroups Kasačkov [1, 2] has gone a little further. He has proved the local theorem for the property of conjugacy of all Sylow Π-subgroups of a group (for given Π) provided only that at least one finite class of conjugate subgroups occurs among them. It follows that *if a locally finite and locally solvable group has a finite class of conjugate Sylow Π-subgroups, then all Sylow Π-subgroups of the group are conjugate.*

Schur's Theorem. In the theory of finite groups the following theorem of Schur (see Zassenhaus [2]) often turns out to be useful.

Schur's Theorem. *If the finite groups A and B have co-prime orders, then every extension of A by means of B is a split extension.*

Proof. Let the orders of A and B be k and l, respectively, $(k, l)=1$, and let G be an extension of A by B. We have to prove that G contains a subgroup of order l. The proof will be by induction with respect to k.

Let p be one of the prime divisors of k, P a Sylow p-subgroup of G, and N its normalizer in G. It is clear that all the Sylow p-subgroups of G, and among them P, are contained in A. The intersection $N \cap A$ is a normal subgroup of N, and its index in N is l, because the indices of N in G and of $N \cap A$ in A are both equal to the number of Sylow p-subgroups of G. Therefore the group N/P contains the normal subgroup $(N \cap A)/P$ of index l. Applying the induction hypothesis—the order of $(N \cap A)/P$ is less than k—we find in N/P a subgroup H/P of order l.

We denote by Z the center of the p-group P; we know from § 54 that it is different from E. The group H/Z contains the normal subgroup P/Z of index l. Applying the induction hypothesis once more—the order of

P/Z is less than k—we find in H/Z a subgroup F/Z of order l.

We cannot apply the induction hypothesis again, because the original group A may be an abelian p-group. We therefore make use of results of § 48. The extension F of the abelian p-group Z by the group F/Z of order l is given by a factor system $m_{\alpha,\beta}$ and a system of automorphisms. We put

$$c_\beta = \prod_{\alpha \in F/Z} m_{\alpha,\beta}.$$

In equation (2) of § 48 we take the product of each side with respect to α, keeping β and γ fixed. Since Z is a commutative group, we arrive at the equation

$$m^l_{\beta,\gamma} = c^{-1}_{\beta\gamma} c_\gamma c^\gamma_\beta ; \tag{10}$$

we have to bear in mind that the element $\alpha\beta$ ranges over the whole group Z as α does.

We denote by k' the order of Z. Since $(k', l) = 1$, there exists a number l' satisfying the congruence

$$ll' \equiv 1 \pmod{k'}.$$

Raising both sides of (10) to the power l' we find, again on account of Z being a commutative group:

$$m_{\beta,\gamma} = (c^{l'}_{\beta\gamma})^{-1} c^{l'}_\gamma (c^{l'}_\beta)^\gamma.$$

Comparing this with equation (8) of § 48 we see that the extension F of Z is equivalent to an extension with unit factors, that is, with a splitting extension (see § 52). Thus we have shown that F, and therefore G also, has a subgroup of order l. This completes the proof of the theorem.

The special case of Schur's Theorem in which B is solvable could also be deduced from Čunihin's Theorem—G is in this case a Π-separable group—if we understand by Π the set of all prime divisors of the order l of B. In this case we even find that *all subgroups of G of order l are conjugate.* The conjugacy of these subgroups has also been proved by Zassenhaus [2] under the assumption that A is solvable. The problem whether this statement is true in general has not yet been solved.

§ 61. Finite semi-simple groups

A finite group is called *semi-simple* if it does not contain any solvable normal subgroups other than E. Since every solvable group has an abelian

characteristic subgroup different from the unit element—for example, the last term but one of the derived series—a finite semi-simple group can also be defined as a group that does not contain any abelian normal subgroup other than E.

Fitting [6] has proved the following theorem.

Every finite group G is an extension of a solvable group by a semi-simple group.

For let A and B be solvable normal subgroups of a group G. Then *their product AB is also a solvable normal subgroup.* For

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

The group on the right-hand side is solvable; therefore AB, as an extension of the solvable group A by the solvable group AB/A, is itself solvable (see § 57).

Since by assumption G is finite, it has a maximal solvable normal subgroup H; the argument above proves that it is unique. The factor group G/H is now semi-simple: if it contained a non-trivial solvable normal subgroup F/H, then the normal subgroup F of G, as an extension of the solvable group H by the solvable group F/H would be solvable, in contradiction to the maximal property of H.

This proves the theorem. Let us keep in mind that the maximal solvable normal subgroup of the group is uniquely determined and that every extension of a solvable group A by a semi-simple group B obviously has A as its maximal solvable normal subgroup. *Therefore we obtain every finite group once and only once if we let A range over all finite solvable groups, B over all finite semi-simple groups, and then take all non-equivalent extensions of A by B.*

In his paper Fitting [6] has shown that the survey of all finite semi-simple groups can be completely reduced to the classification of the non-commutative *simple* groups and their groups of automorphisms. Gol'berg [1] has extended Fitting's results to the infinite case, which requires some changes in the definition of a semi-simple group. We shall confine ourselves to an exposition of Fitting's results for finite semi-simple groups.

Let us first consider a certain other class of groups, which occurs rather often in applications even outside the limits of group theory. We shall not assume the groups to be finite, and moreover, we shall admit an arbitrary operator domain.

A group G is called *completely reducible* if it can be decomposed into the

direct product of a finite number of *simple* groups (in the case of operator groups: simple with respect to the given operator domain).

Every completely reducible group has a principal series. For if

$$G = A_1 \times A_2 \times \ldots \times A_n \tag{1}$$

is a completely reducible group and if all the A_i are simple groups, then the series

$$E \subset A_1 \subset (A_1 \times A_2) \subset \ldots \subset G$$

is a principal (and even a composition) series of G.

We can therefore apply the Krull-Schmidt Theorem (§ 47) to completely reducible groups and see that any two direct decompositions of a completely reducible group in the form (1) are centrally isomorphic. Moreover, if G is a group *without center*, which is equivalent to the assumption that all the direct factors A_i, $i = 1, 2, \ldots, n$ in (1) are non-commutative, then G *has a unique direct decomposition in the form* (1).

Every (admissible) normal subgroup B of a completely reducible group G is itself completely reducible and is a direct factor of G.

We shall begin with the proof of the second part. If (1) is the decomposition of G into the direct product of simple groups, then we shall call A_i a direct factor of the first kind if it is contained in the product of B and $A_1 \times \ldots \times A_{i-1}$, and otherwise a factor of the second kind. If A_i is a factor of the second kind, then it forms a direct product with $B(A_1 \times \ldots \times A_{i-1})$; for from the fact that A_i is simple it follows in this case that the intersection of A_i with the product above is E. It is easy to see now that B and all the factors of the second kind in (1) form a direct product which, because all the factors of the first kind in (1) are contained in G, coincides with G.

We obtain a direct decomposition of G in which B is one of the direct factors. To prove the first part of the theorem, we take the refinement of this decomposition that arises when B is replaced by its decomposition into a direct product of indecomposable groups. This refinement is centrally isomorphic with (1), so that B itself decomposes into the direct product of simple groups. This completes the proof.

A finite completely reducible group G without center is semi-simple.

For if G had a solvable normal subgroup B, then by the preceding theorem it would be completely reducible and therefore abelian. Moreover, it would be a direct factor of G; but this is impossible, because G has no center.

If A and B are completely reducible normal subgroups without center in an arbitrary group G, then their product AB is also completely reducible and has no center.

For if

$$D = A \cap B,$$

then D is a normal subgroup of G, and also of A, and therefore

$$A = D \times A', \tag{2}$$

because A is completely reducible.

Transforming this equation by an arbitrary element g of G, we obtain

$$A = D \times (g^{-1} A' g). \tag{3}$$

The equations (2) and (3) show, by the lemma of § 42, that A' and $g^{-1}A'g$ are centrally isomorphic in A, and since A is a group without center,

$$A' = g^{-1} A' g.$$

This shows that A' is a normal subgroup of G and is, moreover, completely reducible and without center. Since

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

and

$$A' \cap B = E$$

we have

$$AB = A' \times B,$$

so that AB is completely reducible and without center.

It follows from this theorem that *every finite group has a unique maximal completely reducible normal subgroup without center.* In general, this may, of course, be the unit subgroup E. However, the following theorem holds:

If G is a finite semi-simple group different from E, then its maximal completely reducible normal subgroup H (which has no center, because G is semi-simple) *is also different from E.*

First we prove a lemma.

LEMMA. *Every normal subgroup A of a finite semi-simple group G is itself semi-simple.*

For otherwise A would have a maximal solvable normal subgroup other than E which, as a characteristic subgroup of A, would be normal in G, in contradiction to the assumption that G is semi-simple.

We now turn to the proof of the theorem, which will be by induction on the order of G. If the finite semi-simple group G other than E has the smallest possible order then, by the lemma, it is simple and therefore coincides with its maximal completely reducible normal subgroup. We can therefore assume that the theorem is proved for all finite semi-simple groups other than E whose order is less than the order of G. If G is simple, then the theorem is true by the same considerations as above. If not, then G has a non-trivial normal subgroup A which is finite, different from E and, by the lemma, semi-simple. By the induction hypothesis A has a maximal completely reducible normal subgroup B other than E. As a characteristic subgroup of A, the subgroup B is normal in G; therefore G has a completely reducible normal subgroup other than E, and this is what we had to show.

We can show even more: *if G is a finite semi-simple group other than E, then the centralizer C of its maximal completely reducible normal subgroup H is equal to E.*

For C is a normal subgroup of G (see § 11) and so, by the lemma, semi-simple. Moreover, $C \cap H = E$, because this intersection is the center of H; therefore

$$\{C, H\} = C \times H.$$

If C is not E, then by the preceding theorem its maximal completely reducible normal subgroup H' is also different from E. But then it follows that G has a completely reducible normal subgroup $H' \times H$ that is not contained in H, in contradiction to the maximal property. Thus $C = E$, which is what we had to prove.

After these preliminary considerations we can go over to a *survey of the semi-simple groups.* Let G be an arbitrary finite semi-simple group, H its maximal completely reducible normal subgroup, and Γ the group of automorphisms of H. Since H is a group without center, it is isomorphic to its group of inner automorphisms, so that we can assume that *H is contained in Γ.*

Transforming H by an arbitrary element x of G, we obtain an automorphism φ_x of H. The mapping $x \to \varphi_x$ of G into Γ is a homomorphism, and even an isomorphism, because the centralizer of H in G is E. Thus, *G is isomorphic to a subgroup of Γ, and this subgroup obviously contains H.*

Conversely, let H be an arbitrary finite completely reducible group without center and Γ its group of automorphisms, so that by identifying H with its group of inner automorphisms we can assume that H is contained in Γ as a normal subgroup. Further, let F be an arbitrary subgroup of Γ containing H. *Then F is a semi-simple group and H its maximal completely reducible normal subgroup.*

For suppose that an element γ of Γ is permutable, *quâ* automorphism of H, with an arbitrary inner automorphism of H, so that for arbitrary x, y of H

$$y^{-1}(x\gamma)y = (y^{-1}xy)\gamma = (y\gamma)^{-1}(x\gamma)(y\gamma).$$

Hence

$$(x\gamma)[y(y\gamma)^{-1}] = [y(y\gamma)^{-1}](x\gamma).$$

Since the element $x\gamma$ ranges over the whole group H as x does, we see that $y(y\gamma)^{-1}$ belongs to the center of H, so that it is the unit element, and hence

$$y = y\gamma$$

for an arbitrary y of H. The automorphism γ therefore turns out to be the identity. Thus, the centralizer of H in Γ is E.

Let K be a solvable normal subgroup of F. Then $H \cap K$ is a solvable normal subgroup of H and, since H is semi-simple, this intersection is E. Thus the normal subgroups H and K of F form a direct product, and therefore K is part of the centralizer of H in Γ and, by what we have proved above, K is E. This proves that F is semi-simple.

Finally, if H is contained in a larger completely reducible normal subgroup $\overline{H}$ of F, then we know that H is a direct factor of the completely reducible group $\overline{H}$,

$$\overline{H} = H \times H^*.$$

The subgroup H^* is therefore contained in the centralizer of H in Γ; in other words, H^* is E and $\overline{H} = H$. This proves the last part of the theorem.

Under the same assumptions on H and Γ as in the preceding theorem we can show that *if F_1 and F_2 are two isomorphic subgroups of Γ containing H, then they are conjugate in Γ.*

In order to make the proof of this theorem perfectly clear, we shall dispense with the assumption that the elements of H are identical with the inner automorphisms corresponding to them. The inner automorphism induced by an element x of H will be denoted by $\bar{x}$ and the whole group of inner automorphisms of H by $\overline{H}$. Thus, $\overline{H}$ is a normal subgroup of Γ.

Further, we denote by $\overline{\Gamma}$ the group of automorphisms of $\overline{H}$. The isomorphism of H and $\overline{H}$, of course, implies the isomorphism of Γ and $\overline{\Gamma}$: if $\gamma \in \Gamma$, then there corresponds to γ an element γ' of $\overline{\Gamma}$ such that for every x of H

$$\bar{x}\gamma' = \overline{x\gamma}. \tag{4}$$

Let us show that for every γ of Γ

$$\gamma' = \overline{\gamma}, \tag{5}$$

where $\overline{\gamma}$ is the automorphism of $\overline{H}$ that is induced when $\overline{H}$, as a normal subgroup of Γ, is transformed by the element γ.

For an arbitrary y of H we have

$$y(\gamma^{-1}\bar{x}\gamma) = [x^{-1}(y\gamma^{-1})x]\gamma = (x\gamma)^{-1}y(x\gamma),$$

that is,

$$\gamma^{-1}\bar{x}\gamma = \overline{x\gamma}.$$

Hence by (4),

$$\bar{x}\gamma' = \gamma^{-1}\bar{x}\gamma,$$

and since $\bar{x}$ is an arbitrary element of $\overline{H}$, equation (5) is proved. We denote the isomorphic mapping $\gamma \to \overline{\gamma}$ by φ, so that $\gamma\varphi = \overline{\gamma} = \gamma'$.

The subgroups F_1 and F_2 which occur in the formulation of the theorem contain the subgroup $\overline{H}$, and by the preceding theorem $\overline{H}$ is the maximal completely reducible normal subgroup in each of them. Hence it follows that the isomorphic mapping θ of F_1 onto F_2, which exists by assumption, induces an automorphism $\overline{\gamma}$ in $\overline{H}$, so that for all $\bar{x}$ of $\overline{H}$

$$\bar{x}\theta = \overline{x\gamma}. \tag{6}$$

It is clear that $\overline{\gamma}$ is an element of $\overline{\Gamma}$.

The image of F_1 and of F_2 under the isomorphism φ will be denoted by $\overline{F}_1$ and $\overline{F}_2$, respectively. The mapping

$$\overline{f}_1 \to \overline{f_1\theta}$$

is an isomorphism between $\overline{F}_1$ and $\overline{F}_2$. We know that $\overline{f}_1$ is the following automorphism of $\overline{H}$:

$$\bar{x} \to f_1^{-1}\bar{x}f_1, \quad \bar{x} \in \overline{H}. \tag{7}$$

Similarly $\overline{f_1\theta}$ is the automorphism

$$\bar{x} \to (f_1\theta)^{-1}\,\bar{x}\,(f_1\theta), \quad \bar{x} \in \overline{H},$$

or since $\bar{x}\bar{\gamma} = \bar{x}\theta$ ranges over the whole group $\overline{H}$ as $\bar{x}$ does, we have by (6):

$$\bar{x}\bar{\gamma} = \bar{x}\theta \to (f\theta)^{-1}\,(\bar{x}\theta)\,(f_1\theta) = (f_1^{-1}\bar{x}f_1)\,\theta = (f_1^{-1}\bar{x}f_1)\,\bar{\gamma}.$$

However by (7) the automorphism $\bar{\gamma}^{-1}\bar{f}_1\bar{\gamma}$ of $\overline{H}$ also carries every element $\bar{x}\bar{\gamma}$ into the element $(f_1^{-1}\bar{x}f_1)\,\bar{\gamma}$:

$$(x\gamma)\,(\bar{\gamma}^{-1}f_1\gamma) = x\,(f_1\gamma) = (f_1^{-1}xf_1)\,\gamma.$$

This proves the equation

$$\overline{f_1\theta} = \bar{\gamma}^{-1}\bar{f}_1\bar{\gamma}$$

for all $\bar{f}_1$ of $\overline{F}_1$ and shows that $\overline{F}_1$ and $\overline{F}_2$ are conjugate in $\overline{\Gamma}$. Hence it follows that F_1 and F_2 are conjugate in Γ, and this is what we had to show.

The theorem just proved leads to the following results:

We obtain every finite semi-simple group, and each of them once only, if we

1) *take all finite completely reducible groups without center,*
2) *embed every completely reducible group without center H in its group of automorphisms Γ, identifying it with its group of inner automorphisms,*
3) *separate all the subgroups of Γ containing H into classes of conjugate subgroups, and*
4) *choose one representative from each of these classes.*

So we have reduced the survey of the finite semi-simple groups to the survey of the finite completely reducible groups without center and their groups of automorphisms. We have also shown above that the survey of the completely reducible groups without center is reduced, in turn, to the survey of the simple groups. Fitting [6] (see also Gol'berg [1]) has shown that also the group of automorphisms of a completely reducible group without center

$$G = A_1 \times A_2 \times \ldots \times A_n,$$

where all the A_i are simple groups, can be constructed by a perfectly lucid method by means of the groups of automorphisms of $A_1, \ldots, A_n$. We

must emphasize, however, that *the problem of a classification of all non-commutative simple finite groups* is very difficult indeed and far from an exhaustive solution. In § 9 we became acquainted with an infinite sequence of such groups, namely the alternating groups of degree n for $n \geqq 5$. Some similar sequences are known, and also a few isolated simple finite groups that do not belong to these collections.[v]

All non-commutative simple finite groups that have been found so far are of even order. The problem *whether simple finite groups of odd composite order exist* is known as Burnside's problem. Since all the composition factors of a group of odd order are themselves of odd order, this problem, is equivalent, as we remarked in § 57, to the problem whether every finite group of odd order is solvable. So far, it is known (Frobenius, Burnside, Turkin) that *a finite group whose order is odd and consists of not more than seven prime factors is, in fact, solvable.*

We list a few other theorems (essentially due to Frobenius and Burnside) which connect the problem of non-simplicity of a finite group (not necessarily of odd order) with the properties of its order and other properties of the group. The proofs of some of these theorems require the theory of representations and of characters of a group and therefore cannot be given in the present book.

A finite group whose order is composed of powers of not more than two distinct prime numbers is solvable.

A finite group whose order is not divisible by the square of any prime number is solvable.

If the number of elements in some class of conjugates of a finite group is a power of a prime number, then the group is not simple.

If a Sylow p-subgroup of a finite group is contained in the center of its normalizer, then the group is not simple.

There exists a large number of generalizations of these theorems, and numerous other theorems of this type. A number of similar "criteria of non-simplicity" have been published, in particular, by Turkin, Kulakov, Čunihin, Dietzmann, Dyubyuk, Széle, Szélpál, Szep, Rédei.

CHAPTER XV

NILPOTENT GROUPS

§ 62. Nilpotent and finite nilpotent groups

Solvable groups form such a wide generalization of abelian groups that only very few non-trivial properties of the latter can be carried over to solvable groups. More interesting in this respect is a class of groups intermediate between that of abelian and solvable groups. The present chapter is devoted to the study of this class of groups and its generalizations.

Let

$$E = A_0 \subset A_1 \subset A_2 \subset \ldots \subset A_i \subset \ldots \subset A_n = G. \tag{1}$$

be an invariant series of a group G. We shall call it a *central series* if for $i = 0, 1, \ldots, n-1$, A_{i+1}/A_i lies in the center of G/A_i; in other words, if the commutator group $[A_{i+1}, G]$ (see § 14) lies in A_i,

$$[A_{i+1}, G] \subseteq A_i, \; i = 0, 1, \ldots, n-1. \tag{2}$$

Note that the invariance of (1) need not have been postulated, because it follows from (2) for all i that

$$[A_i, G] \subseteq A_i,$$

which is equivalent to the fact that A_i is normal in G.

A group G having at least one central series is called *nilpotent*. It is clear that every abelian group is nilpotent. Moreover, every nilpotent group is solvable, because a central series is, of course, a solvable series.

These three classes of groups are distinct, even in the finite case. For there are solvable groups without center, for example the symmetric group of degree 3, whereas in a nilpotent group the center contains the subgroup A_1 of the central series (1) and is therefore different from E. On the other hand, as we shall show below, every finite p-group is nilpotent, although it need not be abelian.

Every subgroup and every factor group of a nilpotent group is nilpotent.

For let H be a subgroup of a nilpotent group with a central series (1). If

$$B_i = A_i \cap H, \qquad i = 0, 1, \ldots, n, \tag{3}$$

then by (2) we have for $i = 0, 1, \ldots, n-1$,

$$[B_{i+1}, H] \subseteq [A_{i+1}, G] \cap H \subseteq A_i \cap H = B_i.$$

After omission of repetitions the subgroups (3) therefore form a central series of H.

Further, let φ be a homomorphic mapping of a nilpotent group G with central series (1) onto a group $\bar{G}$. We denote by $\bar{A}_i$ the image of A_i under this homomorphism, $i = 0, 1, \ldots, n$. Let $\bar{a}_{i+1}$ and $\bar{g}$ be elements of $\bar{A}_{i+1}$ and $\bar{G}$ respectively, $i = 0, 1, \ldots, n-1$, and let a_{i+1} and g be inverse images under φ of $\bar{a}_{i+1}$ and $\bar{g}$ in A_{i+1} and G,

$$a_{i+1}\varphi = \bar{a}_{i+1}, \quad g\varphi = \bar{g}.$$

Since by (2)

$$[a_{i+1}, g] \in A_i,$$

we have

$$[\bar{a}_{i+1}, \bar{g}] = [a_{i+1}, g]\varphi \in \bar{A}_i.$$

After omission of repetitions the subgroups $\bar{A}_i$, $i = 0, 1, \ldots, n$ therefore form a central series of $\bar{G}$.

The direct product of a finite number of nilpotent groups is nilpotent.

For let

$$G = \prod_{k=1}^{s} G_k,$$

where all the G_k are nilpotent. We choose a central series in each of these groups and assume that the lengths of these series are equal, admitting, if necessary, series with repetitions. Let

$$E = A_{k0} \subseteq A_{k1} \subseteq \ldots \subseteq A_{ki} \subseteq \ldots \subseteq A_{kn} = G_k$$

be the central series of G_k, $k = 1, 2, \ldots, l$. Then the subgroups

$$B_i = \prod_{k=1}^{s} A_{ki}, \quad i = 0, 1, \ldots, n,$$

form a central series of G.

Note that an extension of a nilpotent group by a nilpotent group need not be nilpotent, for otherwise all solvable groups would turn out to be nilpotent.

In § 14 we defined the concept of the lower central chain of an arbitrary group G: this is the chain of subgroups

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_k \ldots,$$

where

$$G_{k+1} = [G_k, G], \quad k = 0, 1, 2, \ldots .$$

Let us construct this chain in a nilpotent group G with central series (1). By (2),

$$G_1 = [G, G] = [A_n, G] \subseteq A_{n-1}.$$

Suppose we have already proved that $G_k \subseteq A_{n-k}$. Then

$$G_{k+1} = [G_k, G] \subseteq [A_{n-k}, G] \subseteq A_{n-k-1}.$$

Hence it follows that

$$G_n \subseteq A_0 = E,$$

or $G_n = E$.

This proves that in a nilpotent group the lower central chain leads to the unit subgroup in a finite number of steps; in other words, it becomes the *lower central series*, and *the length of this series is not greater than the length of any other central series of the group*. The lower central series obviously satisfies the above definition of a central series, so that the existence of a finite lower central series can be taken as the definition of a nilpotent group.

In every group G we can also construct the *upper central chain*: this is the sequence of subgroups

$$E = Z_0 \subseteq Z_1 \subseteq Z_2 \subseteq \ldots \subseteq Z_k \subseteq \ldots$$

such that Z_1 is the center of G, Z_2/Z_1 the center of G/Z_1, and more generally, Z_{k+1}/Z_k the center of G/Z_k. It is easy to see that this chain consists of characteristic subgroups; in general, it can be continued transfinitely, becoming stationary but not necessarily leading up to G itself.

Let us construct the upper central chain of a nilpotent group G with central series (1). Since, by (2), $[A_1, G] = E$, we have $A_1 \subseteq Z_1$. Suppose we have already proved that $A_k \subseteq Z_k$. Then, by (2),

$$[A_{k+1}, G] \subseteq A_k \subseteq Z_k.$$

This shows that in the natural homomorphic mapping of G onto G/Z_k the subgroup A_{k+1} is mapped into the center of this factor group, and therefore $A_{k+1} \subseteq Z_{k+1}$. Hence it follows that

$$A_n = G \subseteq Z_n,$$

or $Z_n = G$.

This proves that in a nilpotent group the upper central chain leads to the group itself in a finite number of steps; in other words, it becomes the *upper central series*, and *the length of this series does not exceed the length of any central series of the group*. The existence of an upper central series can also be taken as the definition of a nilpotent group.

From what we have shown above it follows that *in a nilpotent group the lower and the upper central series have one and the same length*, which is the minimal length of all the central series of the group. This length is called the *class* of the nilpotent group. In particular, nilpotent groups of class 1 are abelian groups, and nilpotent groups of class 2 have been introduced in § 14.

Let G be a nilpotent group whose class does not exceed k. Then the k-th term G_k of the lower central chain of the group is E. In other words, the (identical) relation

$$[\ldots [[x_1, x_2], x_3], \ldots, x_{k+1}] = 1$$

holds identically in G. Therefore, by § 37, G is a factor group of a certain reduced free group, corresponding to this identical relation. It is easy to see that this is the factor group of a free group F with respect to the k-th term F_k of its lower central chain.

The factor group F/F_k is itself a nilpotent group of class k; we call it the *free nilpotent group of class k*. The number of free generators of F we call the *rank* of F/F_k. This is an invariant of the group, by the theorem of Baer proved in § 37.

Thus, every nilpotent group whose class does not exceed k is a factor group of a free nilpotent group of class k. A nilpotent group with n generators is a factor group of the free nilpotent group of rank n. For $k = 1$ this is the familiar theorem that every abelian group is a factor group of a free abelian group.

Some theorems on the automorphisms of free nilpotent groups are proved in a paper by Mal'cev [9]. Golovin [2-5] has introduced and studied the *k-th nilpotent product of groups*, $k = 1, 2, \ldots$. This construction stands in the same relation to free nilpotent groups of class k as does the direct product to free abelian groups, or the free product to free groups. A number

of properties of direct and free products can also be proved for nilpotent products; in particular, this construction, considered as an operation in the set of all groups, is associative. Other examples of constructions with these properties have been given by Lyapin [7].[W]

Finite nilpotent groups. We shall now indicate a number of properties of nilpotent groups which, in the case of finite nilpotent groups, are equivalent to their definition.

Every subgroup of a nilpotent group can be included in a normal series of the group; in other words, every such subgroup is accessible.

For let G be a nilpotent group,

$$E = A_0 \subset A_1 \subset A_2 \subset \ldots \subset A_n = G$$

a central series of G, and H a proper subgroup of G. There exists an index i, $i < n$, such that

$$A_i \subseteq H, \quad A_{i+1} \not\subseteq H.$$

However, by (2), the commutator of an arbitrary element of A_{i+1} with an arbitrary element of H is contained in A_i, that is, in H. Therefore the normalizer H_1 of H in G contains A_{i+1} and is different from H. If H_1 is different from G, then by the same argument its normalizer H_2 is strictly greater than H_1 and in any case contains A_{i+2}. Continuing the process, we arrive at G after not more than $n - i$ steps. The subgroups

$$E \subset H \subset H_1 \subset H_2 \subset \ldots \subset G$$

therefore form a normal series of G.

The problem whether the property just proved can be taken as definition of a nilpotent group has not yet been solved.

From this theorem it follows that *every proper subgroup of a nilpotent group is distinct from its normalizer.* Groups with this last property are said to satisfy the *normalizer condition.*

If the normalizer condition holds in a group G, then every Sylow p-subgroup of G for every p is a normal subgroup of G.

For we have shown in § 54 that the normalizer of a Sylow subgroup is its own normalizer. In our case the normalizers of Sylow subgroups must therefore be equal to G, so that all Sylow subgroups are normal in G.

Thus, again by § 54, *a group G in which the normalizer condition holds has a unique Sylow p-subgroup for every prime number p. These Sylow*

subgroups, taken for all p, form a direct product in G which contains precisely the elements of finite order in G. (We know that every finite cyclic group can be decomposed into the direct product of primary cyclic groups.)

If we apply the above results to finite groups, we see that *every finite nilpotent group can be decomposed into the direct product of p-groups.*

The converse statement is also true, and this lends particular interest to finite nilpotent or—as they used to be called—finite *special* groups.

Every finite group that can be decomposed into the direct product of p-groups is nilpotent.

We have shown above that the direct product of a finite number of nilpotent groups is itself nilpotent; it is therefore sufficient to prove the following theorem; this in turn implies the fact, proved in § 57, that a finite p-group is solvable.

Every finite p-group is nilpotent.

For a finite p-group G has a non-trivial center Z_1, as we proved in § 54. The factor group G/Z_1 again is a finite p-group, its center Z_2/Z_1 is again non-trivial, and so Z_2 is strictly greater than Z_1. Continuing the process, we construct the upper central series of G; that is, we prove the nilpotency of the group.

We have found several properties of finite groups each of which can be taken as definition of a finite nilpotent group; for example, the existence of a central series, the normalizer condition, the decomposition into the direct product of p-groups. Finite nilpotent groups admit many other equivalent definitions. We mention a few of them, but by no means do we aim at an exhaustive statement of everything that can be said in this connection.

A finite group is nilpotent if and only if all its maximal (proper) subgroups are normal.

For a finite nilpotent group satisfies the normalizer condition, and its maximal subgroups must therefore be normal in the group. Suppose, conversely, that all maximal subgroups of a group G are normal. Let P be a Sylow p-subgroup of G for some p and N its normalizer. If N is different from G, then we denote by A one of the maximal subgroups of G containing N. Since the theorem on the conjugacy of Sylow p-subgroups holds in G, every subgroup containing N, including A, must be its own normalizer, by § 54. However, this contradicts the fact that A is normal in G. Thus N coincides with G; that is, P is a normal subgroup of G. But the fact that the Sylow p-subgroups are normal for all p implies the nilpotency of a finite group.

We now define a new characteristic subgroup of an arbitrary group G. The Φ-*subgroup* (or Frattini subgroup) of a group G is the intersection of all the maximal subgroups of G, provided G has maximal subgroups; otherwise G shall be regarded as its own Φ-subgroup.

The following theorem holds (Neumann [5], Zassenhaus [2]).

The Φ-subgroup of a group G consists precisely of those elements x of G that can be omitted from every system of generators G in which they occur; that is, if $G = \{M, x\}$, then $G = \{M\}$.

For if an element x does not belong to the Φ-subgroup, then there is some maximal subgroup A in which it is not contained, so that $\{x, A\} = G$, although $\{A\} = A \neq G$. Suppose, conversely, that there exists a set M such that

$$G = \{M, x\} \tag{4}$$

but $G \neq \{M\}$. Among the subgroups containing M but not x, we denote a maximal one by A (see § 7). A is a maximal proper subgroup of G, because every larger subgroup must contain x and therefore, by (4), must coincide with G. Thus x is not contained in the maximal subgroup A and therefore does not belong to the Φ-subgroup.

From this theorem it follows that *if the Φ-subgroup of a group G is finite, or even finitely generated,* (as it is, for example, in the case of finite groups), *then every set M that, in conjunction with the Φ-subgroup, generates the whole group G, is itself a system of generators of G.* An example of such an M is a system of representatives of the cosets of the Φ-subgroup in G.

Now we can point out yet another method of defining a finite nilpotent group (Wielandt [2]).

A finite group G is nilpotent if and only if its derived group is contained in its Φ-subgroup, in other words, if every set M that, in conjunction with the derived group, generates the whole group G, generates G by itself.

For if the derived group is contained in the Φ-subgroup Φ of G, then G/Φ is abelian. All subgroups of G containing Φ and, in particular, all maximal subgroups of G are therefore normal in G, and hence G is nilpotent.

Conversely, if G is nilpotent, then every maximal subgroup A is normal in G. The factor group G/A contains no proper subgroups, so that it is a cyclic group of prime order and hence abelian. Thus A contains the derived group of G, so that the derived group is contained in the intersection of all maximal subgroups, that is, in the Φ-subgroup.

As the reader can easily verify, the proof of the statement that *the derived group of a nilpotent group is contained in its Φ-subgroup* does not require the finiteness of the group. A generalization of the above theorem to the case of finitely generated groups can be found in a paper by Baer [24]; see also Hirsch [2, 4].

§ 63. Generalized nilpotent groups

The definition of a nilpotent group given in the preceding section lends itself to natural generalizations. But on transition to infinite groups the various forms of the definition of a finite nilpotent group lead to classes of groups which, in general, no longer coincide. We shall now consider some of these classes of groups, referring the reader for further details to the paper by Kuroš and Černikov [1]. Other classes of generalized nilpotent groups are studied by Kontorovič [8].

A generalization of the concept of a central series is that of a *central system*: this is an invariant system $\mathfrak{A} = [A_\alpha]$ of a group G (see § 56) such that we have for every jump $A_\alpha, A_{\alpha+1}$ in the system

$$[A_{\alpha+1}, G] \subseteq A_\alpha,$$

in other words, that $A_{\alpha+1}/A_\alpha$ is contained in the center of G/A_α.

A *Z-group* or *group with property Z* is a group that has at least one central system. This generalization of the concept of a nilpotent group is very wide—by Magnus' Theorem (see § 36) all free groups are Z-groups.

Mal'cev [3] has proved that the local theorem holds for the property Z:

Every group that has the property Z locally is a Z-group.

The proof of this theorem is conducted on the same lines as the proof of the local theorem for the property SN (see § 58), and we only point out the changes that now have to be brought in. The subgroup $C^{\alpha}_{a,b}$ must now be defined as the largest subgroup of the system $\mathfrak{C}^\alpha$ containing neither of the elements a and b other than 1; therefore, in particular, it is not necessary to consider local systems linked with one pair (a, b). The subgroup $H_{a,b}$ also contains neither a nor b, but it does contain their commutator. The proof that the system $\mathfrak{H}$, supplemented if necessary by the group G itself, is a central system of G now proceeds without difficulty.

A much narrower class of groups is that of the *ZA-groups*, that is, groups having an ascending well-ordered central system or, as we shall say, an *ascending central series*. Many properties of nilpotent groups can easily be

transferred to this class of groups. Thus, by an almost verbatim repetition of the arguments of the preceding section and an occasional simple transfinite induction the reader can prove the following statements.

Every subgroup and every factor group of a ZA-group is itself a ZA-group.

A group is a ZA-group if and only if its upper central chain, possibly continued transfinitely, leads up to the group G.

Every ZA-group satisfies the normalizer condition.

The local theorem for ZA-groups does not hold; this is shown by the existence of locally finite p-groups without center. However, the following theorem is true (Černikov [20]).

Every group whose countable subgroups are all ZA-groups is itself a ZA-group.

First we prove the following lemma:

Lemma. *A group G is a ZA-group if and only if for every element a of G and every sequence of elements $x_1, x_2, \ldots, x_k, \ldots$ we can find an index k such that*

$$[\ldots[[a, x_1], x_2], \ldots, x_k] = 1.$$

For let G be a ZA-group with an ascending central series

$$E = A_0 \subset A_1 \subset \ldots \subset A_\alpha \subset \ldots \subset A_\mu = G \tag{1}$$

and let a and $x_1, x_2, \ldots, x_k, \ldots$ be elements of G. If none of the elements

$$a_k = [\ldots[[a, x_1], x_2], \ldots, x_k], \quad k = 1, 2, \ldots, \tag{2}$$

is the unit element, then we can find an index α, $\alpha \geqq 0$, such that A_α contains none of the elements a_k, whereas $A_{\alpha+1}$ contains at least one of the elements, say a_l.[1] But then, by the definition of a central system,

$$a_{l+1} = [a_l, x_{l+1}] \in A_\alpha,$$

and we have arrived at a contradiction to the choice of α.

For the proof of the converse part of the lemma we show, to begin with, that if for arbitrary elements a and $x_1, x_2, \ldots, x_k, \ldots$ in G at least one of the elements (2) is the unit element, then *this also holds in the factor group*

[1] It follows from the definition of a normal system that for a limit number α the subgroup A_α in (1) is the union of the preceding subgroups.

of the center Z of G. Let aZ and $x_1Z, x_2Z, \ldots, x_kZ, \ldots$ be elements of G/Z. If the elements a_k of G are defined as in (2), then by assumption there is an index k such that $a_k = 1$. Therefore

$$Z = a_kZ = [\ldots[[aZ, x_1Z], x_2Z], \ldots, x_kZ],$$

and this is what we had to prove.

We now show that if for arbitrary elements a and $x_1, x_2, \ldots, x_k, \ldots$ in G at least one of the elements (2) is equal to 1, then G *has a non-trivial center.* For if an element a of G does not lie in the center, then we can find an element x_1 such that the commutator $a_1 = [a, x_1]$ is not the unit element. If a_1 does not lie in the center then we can find an element x_2 such that $a_2 = [a_1, x_2]$ is again not the unit element. This process cannot be continued *ad infinitum*, because that would contradict the assumption made about G; hence some a_k will be an element other than 1 of the center.

The converse part of the lemma follows from what we have proved in the two preceding paragraphs, because the ascending central chain of G must lead to the group itself.

The proof of the theorem is now easy. If G is not a ZA-group, then, by the lemma, we can find elements a and $x_1, x_2, \ldots, x_k, \ldots$ in G such that none of the elements (2) is the unit element. The subgroup $\{a, x_1, x_2, \ldots, x_k, \ldots\}$ is countable but, again by the lemma, it is not a ZA-group. This proves the theorem.

ZA-groups will play an important rôle in what follows. By way of contrast, the class of groups that have a descending well-ordered central system are of very little interest and will not be considered here.

N-groups. We now turn to a study of the groups in which the normalizer condition holds or, concisely, *N-groups*. We have mentioned above that *every ZA-group is an N-group*. It is still an open question whether the converse is true.

A group G is an N-group if and only if through each subgroup of G there passes an ascending normal series.

For if A is a subgroup of an N-group G, then we can construct an ascending normal series $[A_\alpha]$ by putting $A_0 = E$, $A_1 = A$ and then choosing A_α as follows: if α is not a limit number, we take the normalizer of $A_{\alpha-1}$, but if α is a limit number, we take the union of all A_β, for $\beta < \alpha$. This system obviously leads to G itself. Conversely, if every subgroup of a group G occurs in some ascending normal series, then every proper

subgroup is normal in some larger subgroup and is therefore distinct from its normalizer.

Using these results it is easy to prove that *every subgroup and every factor group of an $\mathfrak{N}$-group is itself an $\mathfrak{N}$-group.* Thus, if A is a subgroup of an $\mathfrak{N}$-group G containing, in turn, a subgroup B, then the intersection with A of an ascending normal series of G passing through B gives an ascending normal series for A, after omission of repetitions. This shows that A is an N-group.

A natural generalization of the concept of an $\mathfrak{N}$-group is that of an $\tilde{\mathfrak{N}}$-*group*: this is a group in which for every subgroup there is some normal system passing through it. It can be shown, just as above for $\mathfrak{N}$-groups, that *every subgroup and every factor group of an $\tilde{\mathfrak{N}}$-group is itself an $\tilde{\mathfrak{N}}$-group.*

Note that not every Z-group is an $\tilde{N}$-group; otherwise all free groups would be $\tilde{N}$-groups, and hence also all their factor groups, that is, all groups whatsoever, and this is clearly not the case. Whether every $\tilde{\mathfrak{N}}$-group has the property Z is an open question.

The following theorem indicates another form of the definition of an $\tilde{N}$-group.

A group G is an $\tilde{N}$-group if and only if in every subgroup B of G every maximal proper subgroup A of B is normal in B.

For we know that B is itself an $\tilde{N}$-group, so that some normal system of B passes through A. But since there are no subgroups between A and B, these two subgroups form a jump in the normal system, and A is therefore normal in B.

For the proof of the converse we take an arbitrary subgroup A of B and show that it occurs in some normal system. For this purpose we refine the system of subgroups

$$E \subset A \subset G,$$

which need not, of course, be a normal system, to an ordered system of subgroups that admits no further refinements. The new system is obviously complete. Furthermore, no intermediate subgroup can be inserted at any jump of the system; hence it follows from the condition of the theorem that at every jump the first subgroup is normal in the second, in other words, the system of subgroups we have constructed turns out to be a normal system.

Baer [24] has proved the local theorem for $\tilde{\mathfrak{N}}$-groups.

Every group having the property $\tilde{\mathfrak{N}}$ locally is an $\tilde{\mathfrak{N}}$-group.

Let a group G have a local system consisting of subgroups U^a with the property $\tilde{N}$, and let A and B be subgroups of G, $A \subset B$, such that there is no subgroup between A and B. If A is not normal in B, then we can find elements $a \in A$ and $b \in B$, $b \notin A$, such that

$$c = b^{-1}ab \notin A,$$

although, of course, $c \in B$. It follows that $\{A, c\} \neq A$, and therefore $\{A, c\} = B$. Hence there exists a finite system of elements $a_1, a_2, \ldots, a_n$ of A such that b can be expressed in terms of these elements and c. In the given local system we can find a subgroup U containing a, all the elements $a_1, a_2, \ldots, a_n$, and c. Therefore $b \in U$, but

$$b \notin V = U \cap A.$$

If we denote by W a maximal one among the subgroups of U containing V but not b, then there are no subgroups between W and $\{W, b\}$. Since U is an $\tilde{N}$-group, it follows that W is normal in $\{W, b\}$, and since

$$a \in V \subseteq W,$$

we find that

$$c = b^{-1}ab \in W.$$

But the element b, which, as we know, can be expressed in terms of $a_1, a_2, \ldots, a_n$, and c, must be contained in W, in contradiction to the assumption. This proves the theorem.

Locally nilpotent groups. We call a group G *locally nilpotent* if it has a local system consisting of nilpotent groups. Since every subgroup of a nilpotent group is itself nilpotent, this definition is equivalent to saying that every finitely generated subgroup of G is nilpotent.

Every subgroup and every factor group of a locally nilpotent group is itself locally nilpotent. This follows from the corresponding statements for nilpotent groups.

All locally nilpotent groups of course belong to every class of generalized nilpotent groups for which the local theorem holds, that is, to the Z-groups and the $\tilde{N}$-groups. Recalling the definition of a Z-group, we see that *a locally nilpotent group that is not a cyclic group of prime order cannot be simple.*

Mal'cev [6] has proved the following theorem.

Every ZA-group is locally nilpotent.

For let G be a ZA-group with an ascending central series

$$E = Z_0 \subset Z_1 \subset \ldots \subset Z_\alpha = G. \tag{3}$$

We call the ordinal number α the *length* of this central series and we assume that the theorem is proved for all ZA-groups having an ascending central series of smaller length; for $\alpha = 1$, that is, for abelian groups, the theorem is clearly true. In G we choose a finite system of elements

$$a_1, a_2, \ldots, a_n. \tag{4}$$

If α is a limit number, then the elements (4) lie in some subgroup Z_β, $\beta < \alpha$; and since this subgroup has an ascending central series of length β and since $\beta < \alpha$, $\{a_1, a_2, \ldots, a_n\}$ is nilpotent by induction hypothesis.

If α is not a limit number, then there is a limit number β and a natural number k for which

$$\alpha = \beta + k.$$

We take all possible sequences of commutators of the form

$$[\ldots[[a_{i_1}, a_{i_2}], a_{i_3}], \ldots, a_{i_{k+1}}]$$

for distinct choices of $k+1$ elements of (4). Only a finite number of such commutators exist, they all lie in Z_β and, since β is a limit number, they lie in some subgroup Z_γ, $\gamma < \beta$. Let

$$H = \{Z_\gamma, a_1, a_2, \ldots, a_n\}.$$

We can construct an ascending central series in H as follows. The beginning of the chain will be the segment of (3) up to and including Z_γ. Then follows $Z'_{\gamma+1}$, corresponding to the center of H/Z_γ, then $Z_{\gamma+2}$, corresponding to the center of $H/Z'_{\gamma+1}$, and so on. Since $Z'_{\gamma+1}$ is known to contain all sequences of commutators of k elements of (4), we find that $Z'_{\gamma+2}$ contains all sequences of commutators of $k-1$ elements of (4), and so on. Therefore this ascending central chain leads to H in not more than k steps, that is, it becomes an ascending central series whose length does not exceed $\gamma + k$. Since β is a limit number and $\gamma < \beta$, $\gamma + k$ is strictly less than β and *a fortiori* less than α. Hence, by induction hypothesis, $\{a_1, a_2, \ldots, a_n\}$ is a nilpotent subgroup. This completes the proof.

On the basis of this result Plotkin [2] has proved the following theorem.

THEOREM. *Every N-group is locally nilpotent.*

The proof[1] requires the following lemmas.

LEMMA 1 (Schmidt [6]). *If a normal subgroup H of an N-group G has a non-trivial center Z and if G/H is cyclic, then G itself has a non-trivial center.*

By assumption, G contains an element a such that

$$G = \{H, a\}.$$

The center Z is characteristic in H and is therefore normal in G. Moreover, $\{Z, a\}$ as a subgroup of an N-group is itself an N-group, so that either $Z \subset \{a\}$ or $\{a\}$ differs from its normalizer in $\{Z, a\}$. Every element of $\{Z, a\}$ has the form za^k, $z \in Z$, and therefore in both cases the normalizer of $\{a\}$ in $\{Z, a\}$ contains an element z of Z other than 1. If the commutator $[z, a]$ is the unit element then z, lying in the center of H, is permutable with a and so belongs to the center of G. But if $[z, a]$ is not the unit element, then it lies in the center Z of H and in $\{a\}$—in the latter because of the choice of z—and then $[z, a]$ is contained in the center of G.

LEMMA 2. *If a normal subgroup H of an N-group G has an ascending central series and if G/H is cyclic, then G itself is a ZA-group.*

By Lemma 1, G has a non-trivial center Z_1. Suppose that we have already constructed the terms Z_α of the upper central series for all α less than β. If β is a limit number, then we take Z_β to be the union of all Z_α, $\alpha < \beta$. But if $\beta - 1$ exists, then the group

$$HZ_{\beta-1}/Z_{\beta-1} \simeq H/(H \cap Z_{\beta-1})$$

as a factor group of the ZA-group H has a non-trivial center, the group $G/Z_{\beta-1}$ is an extension of it by a cyclic group and therefore, again by Lemma 1, the center of $G/Z_{\beta-1}$ is non-trivial. We denote its inverse image in G by Z_β. Hence the upper central chain of G cannot become stationary before G itself is reached.

LEMMA 3. *If a and x are elements of an N-group G and if*

$$x_1 = x, \quad x_{i+1} = [x_i, a], \quad i = 1, 2, \ldots,$$

[1] A simpler proof is given in Hirsch [10].

then there exists an index k such that $x_k = 1$.

For let $A_1 = \{a\}$. By the definition of an $\mathfrak{N}$-group, an ascending normal series of G passes through A_1

$$E = A_0 \subset A_1 \subset A_2 \subset \ldots \subset A_\alpha \subset \ldots \subset G. \tag{5}$$

Suppose that all the elements x_i are different from the unit element. Let A_{α_i} be the least subgroup of (5) containing x_i, $i = 1, 2, \ldots$. The index α_i cannot be a limit number. Nor can it be 1, because we would then have $x_{i+1} = 1$, in contradiction to our assumption. Hence it follows that $\alpha_i - 1$ exists and is different from zero, and therefore

$$a \in A_{\alpha_i - 1}.$$

Since (5) is a normal series, we also have

$$x_i^{-1} a^{-1} x_i \in A_{\alpha_i - 1},$$

and therefore also

$$x_i^{-1} a^{-1} x_i \cdot a = x_{i+1} \in A_{\alpha_i - 1}.$$

This shows that the indices α_i form a strictly decreasing sequence

$$\alpha_1 > \alpha_2 > \ldots > \alpha_i > \ldots;$$

but this contradicts the fact that (5) is well-ordered.

Lemma 4. *If H is a locally nilpotent normal subgroup of an $\mathfrak{N}$-group G and*

$$G = \{H, a\}$$

then G is also locally nilpotent.

Every finite system of elements of G can be expressed in terms of a and a finite number of elements of H; therefore it is sufficient to prove the nilpotency of a subgroup of G generated by an arbitrary system of elements of the form

$$a,\ h',\ h'',\ \ldots,\ h^{(n)},\quad h^{(k)} \in H,\quad k = 1, 2, \ldots, n. \tag{6}$$

We denote by F the subgroup generated by the elements

$$h^{(k)} = h_1^{(k)},\quad k = 1, 2, \ldots, n, \tag{7}$$

and all the elements

$$h_{i+1}^{(k)} = [h_i^{(k)}, a], \quad i = 1, 2, \ldots, \quad k = 1, 2, \ldots, n. \tag{8}$$

All the elements (7) and (8) lie in H and by Lemma 3, only a finite number of them are different from the unit element; therefore F is nilpotent. Moreover, F is a normal subgroup of $\bar{F}$ generated by the elements (6), because

$$a^{-1} h_i^{(k)} a = h_i^{(k)} h_{i+1}^{(k)}.$$

The factor group $\bar{F}/F$ is cyclic; therefore by Lemma 2, $\bar{F}$ is a ZA-group. Finally, by making use of the fact that $\bar{F}$ is finitely generated and that a ZA-group is locally nilpotent, as we have proved above, we find that $\bar{F}$ is nilpotent.

We now come to the proof of the theorem.

Proof of the Theorem. In the N-group G we can construct an ascending normal series

$$E = H_0 \subset H_1 \subset H_2 \subset \ldots \subset H_\alpha \subset \ldots \subset H_\gamma = G, \tag{9}$$

such that

$$H_{\alpha+1} = \{H_\alpha, a_\alpha\}, \quad 0 \leqq \alpha < \gamma, \tag{10}$$

where a_α is an element of the normalizer of H_α in G that is not in H_α. If G is not locally nilpotent, then let H_α be the first subgroup in (9) that is not locally nilpotent. Now α cannot be a limit number, because the union of an ascending sequence of locally nilpotent groups is itself locally nilpotent. But $H_{\alpha-1}$ is locally nilpotent and, by Lemma 4, we have reached a contradiction. This completes the proof.

In connection with this theorem we mention that papers of Černikov [4] and Schmidt [6] contain examples of locally nilpotent groups in which the normalizer condition does not hold.[y]

§ 64. Connections with solvable groups. S-groups. Finiteness conditions

All nilpotent groups are, as we know, solvable. Similarly, we can indicate for every class of generalized nilpotent groups at least one class of generalized solvable groups containing it.

The following statements are obvious: *Every Z-group is an SI-group, every locally nilpotent group is locally solvable, and every ZA-group belongs to the class of SI^*-groups.*

For ZA-groups there is yet another class of generalized solvable groups containing it (see Baer [30]; for the proof see Černikov [3]).

Every ZA-group G is an SD-group.

For if G is abelian, then there is nothing to prove. But if G is non-commutative, then we shall use the following lemma.

Grün's Lemma (Grün [1]). *If a group G has a center Z other than E and if the center of G/Z is also different from E, then there exists a homomorphic mapping of G onto a subgroup of Z other than E.*

For the assumptions of the lemma show that in the ascending central chain of G the subgroup Z_2 is distinct from $Z_1 = Z$. We take an element a in Z_2, outside Z, and associate with every element x of G the commutator $[a, x]$. From the fact that a occurs in Z_2, which corresponds to the center of G/Z, it follows that $[a, x] \in Z$, and from $a \notin Z$ follows the existence of an x_0 such that $[a, x_0] \neq 1$. This non-trivial mapping of G into Z is a homomorphism. This follows from the equation

$$[a, x] \cdot [a, y] = [a, xy].$$

Because of $[x, a^{-1}] \in Z$ we have

$$[a,\ x] \cdot [a,\ y] = a^{-1}x^{-1}ax \cdot a^{-1}y^{-1}ay = \\ = a^{-1}y^{-1}(x^{-1}axa^{-1})\,ay = [a,\ xy].$$

From the lemma it follows that a non-commutative ZA-group G has a non-trivial abelian factor group and is therefore distinct from its derived group. Since every subgroup of a ZA-group is itself a ZA-group, the theorem is proved.

Finally we prove the following theorems.

Every $\widetilde{N}$-group is an $\widetilde{SN}$-group.

For an arbitrary normal system of an $\widetilde{N}$-group G can be refined to a well-ordered system of subgroups in which no intermediate group can be inserted at any jump. By the property $\widetilde{N}$ the first subgroup of every jump is therefore normal in the second; in other words, it turns out to be a normal system and all its factors are obviously cyclic of prime order.

Every N-group is an SN^*-group.

For at the end of the preceding section we constructed an ascending

normal series (9) with the property (10) in an arbitrary N-group G. The factors of this series are obviously cyclic.

Groups having an invariant system with cyclic factors. Obviously, every abelian group has an ascending invariant series with cyclic factors. Using this fact, we can show that *every ZA-group also has an ascending invariant series with cyclic factors, and every Z-group has an invariant system with cyclic factors.*

If G is a Z-group with a central system $\mathfrak{A} = [A_\alpha]$, then, as we have mentioned above, at every jump A_α, $A_{\alpha+1}$ of the system we can insert an ascending series with cyclic factors. All the terms of this series are normal in G, since the factor $A_{\alpha+1}/A_\alpha$ lies in the center of G/A_α.

The converse does not hold, even for finite groups. For example, the symmetric group of degree 3 has a principal series with cyclic factors but is not nilpotent. We therefore have a class of groups between solvable and nilpotent groups.[1]

The following theorem (Černikov [7]) is known in the case of finite groups as *Wendt's Theorem.*

The derived group of every group having an invariant system with cyclic factors is a Z-group.

Let G have an invariant system $\mathfrak{A} = [A_\alpha]$ with cyclic factors; since all the subgroups of a cyclic group are characteristic, we can assume that all the factors of $\mathfrak{A}$ are finite. Let K be the derived group of G. The intersections

$$B_\alpha = A_\alpha \cap K$$

form an invariant system $\mathfrak{B}$ of K, after omission of repetitions, again with finite cyclic factors. Let $B_\alpha, B_{\alpha+1}$ be a jump of $\mathfrak{B}$ and let $B_{\alpha+1}/B_\alpha$ be a cyclic group of order n consisting of the elements $c^i B_\alpha$, where $c \in B_{\alpha+1}$, $i = 0, 1, \ldots, n-1$. If x and y are arbitrary elements of G, then since B_α and $B_{\alpha+1}$ are normal subgroups of G there exist exponents k and l such that

$$(xB_\alpha)(cB_\alpha)(xB_\alpha)^{-1} = c^k B_\alpha,$$
$$(yB_\alpha)(cB_\alpha)(yB_\alpha)^{-1} = c^l B_\alpha.$$

Hence

$$(xyB_\alpha)(cB_\alpha)(xyB_\alpha)^{-1} = (yxB_\alpha)(cB_\alpha)(yxB_\alpha)^{-1} = c^{kl} B_\alpha,$$

so that $[x, y]B_\alpha$ is permutable with cB_α. This shows that the factor group

[1] They are called *supersolvable* groups. [*Trans.*]

B_{a+1}/B_a lies in the center of K/B_a—in other words, that $\mathfrak{B}$ is a central system of K. This proves the theorem.

Now we can indicate, at any rate for finite groups, the correct position of groups having an invariant series with cyclic factors. We know that every solvable group has an invariant series with abelian factors. Conversely, every group having an invariant series with arbitrary *nilpotent* factors is solvable. This allows us to classify solvable groups with respect to the minimal length of their invariant series with nilpotent factors. If this length does not exceed 2, that is, if the group is an extension of a nilpotent group by a nilpotent group, then we shall call it *metanilpotent.*

Wendt's theorem shows that *every finite group having an invariant series with cyclic factors is metanilpotent.*

Finally we mention, without proof, the following theorem about the classes of groups we have studied (Baer [24]; see also Kuroš and Černikov [1]).

Every $\bar{N}$-group having an invariant system with cyclic factors or an ascending invariant series with cyclic factors is a Z-group or a ZA-group, respectively.

S-groups. So far we have not attempted to extend to infinite groups one of the most important among the definitions of a finite nilpotent group, namely the representation of these groups as a direct product of p-groups. This can be done in the following way.

Let us call a group G an *S-group* if it has a unique Sylow p-subgroup for every prime number p, in other words, if the set of all the elements of finite order in the group forms a subgroup which is the direct product of p-groups. We call this subgroup the *periodic part* of G.

The class of S-groups is very wide. They comprise, in particular, all the p-groups, which themselves constitute a very complicated class of groups. Every torsion-free group also satisfies the definition of an S-group. We shall therefore only be interested in relations between S-groups and the classes of generalized nilpotent groups introduced in the preceding section.

First of all, we mention the following obvious property of S-groups which will be used in the sequel: *Every subgroup of an S-group is itself an S-group.* Conversely, *if a group G has a local system $\mathfrak{A} = [A_a]$ consisting of S-groups, then it is itself an S-group.* For we obtain the unique Sylow p-subgroup of G if we form the union of the elements of the Sylow p-subgroups of all A_a.

In § 62 we have already shown that all N-groups, and therefore all nilpotent groups, are S-groups. Since the local theorem holds for the property S we arrive at a more general result: *Every locally nilpotent group is an S-group.*

On the other hand, not every Z-group is an S-group (see Mal'cev [7]). The corresponding problem for $\tilde{N}$-groups is still open; some partial results are contained in a paper by Baer [24].

Imposition of finiteness conditions. When finiteness conditions of one kind or another are imposed, then additional connections appear, of course, between the classes of generalized nilpotent groups. For example, the following theorem holds.

For locally finite groups the following properties are equivalent: Z, $\tilde{N}$, S, *and local nilpotency.*

For if G is a locally finite group with the property Z, $\tilde{N}$, or S, then all its finite subgroups have the same property—that is, by § 62, are nilpotent—so that G itself is locally nilpotent. Conversely, if a locally finite group G is locally nilpotent, then all its finite subgroups have each of the properties Z, $\tilde{N}$, and S, and then the local theorems for these properties imply that G itself is a Z-, $\tilde{N}$-, and S-group.

We mention that it follows from the local finiteness of periodic locally solvable groups, which was established in § 59, that *every periodic locally nilpotent group is locally finite.* Restricting this result successively we find that *periodic N-groups, periodic ZA-groups, and periodic nilpotent groups are locally finite.*

Now we subject the groups under consideration to the *minimal condition for subgroups.* Under this condition property $\tilde{N}$ obviously turns into property N, and Z into ZA; therefore, as we have just mentioned, the periodicity of a group, which is a consequence of the minimal condition, turns into local finiteness in these two cases. Therefore the theorem that was proved above for locally finite groups leads to the following result (Černikov [37]).

In groups with minimal condition for subgroups, the following properties are equivalent: 1) ZA, 2) N, *and* 3) *the combination of local finiteness and* S.

Groups for which this theorem gives three equivalent definitions are periodic and have the property S, so that they are direct products of p-groups. Let us define a *Černikov p-group* as a group satisfying any one of the following equivalent definitions:

(1) p-groups with minimal condition for subgroups having an ascending central series;

(2) p-groups satisfying the minimal condition for subgroups and the normalizer condition;

(3) locally finite p-groups with minimal condition for subgroups.

For Černikov p-groups we can give a number of other definitions and, indeed, the possibility of looking at them from various points of view makes them particularly interesting. Thus, for Černikov p-groups we can also take either of the following two definitions:

(4) solvable p-groups with minimal condition for subgroups;

(5) p-groups with minimal condition for subgroups having a complete abelian normal subgroup of finite index.

(4) *follows from* (1): We mentioned at the beginning of this section that every ZA-group is an SI-group, so that under the minimal condition for subgroups it is, by Černikov's Theorem of § 59, solvable. (3) *follows from* (4), because, as we have proved in § 59, an arbitrary periodic solvable group is locally finite. Finally, the *equivalence of* (4) *and* (5) follows immediately from the same theorem of Černikov.

The definition (5) is interesting in that it reduces the classification of all Černikov p-groups to that of finite p-groups: on account of the classification of abelian groups with minimal condition given in § 53 they are precisely all the possible extensions of a direct product of a finite number of groups of type p^∞ by a finite p-group. We note that the complete abelian normal subgroup of finite index in a Černikov p-group is uniquely determined (see the proof of Černikov's Theorem in § 59). We also note that in definition (5) the postulate that the abelian normal subgroup of finite index shall be complete can be omitted, because by § 53 every abelian group with minimal condition has a complete characteristic subgroup of finite index.

Finally, we mention, without proof, four theorems that permit us to give other definitions of Černikov p-groups.

A p-group having an ascending central series is a Černikov p-group if and only if all the factors of its upper central series satisfy the minimal condition (Muhammedžan [2]).

A locally finite p-group is a Černikov p-group if and only if it satisfies the minimal condition for abelian subgroups (Schmidt [6], Černikov [20]).

Locally finite p-groups of finite special rank (see § 53) *are Černikov p-groups and conversely* (Myagkova [1]).

A p-group is isomorphic to a group of matrices over a field of characteristic zero if and only if it is a Černikov p-group. (Mal'cev [2]).

Other finiteness conditions do not lead to such a complete theory; we only mention a few results.

Under the maximal condition for subgroups every locally nilpotent group is nilpotent, because the maximal condition implies that the number of

generators is finite. Because of Plotkin's theorem of the preceding section, this result contains the theorem of Hirsch [5]: *Every N-group satisfying the maximal condition for subgroups is nilpotent.*

In papers by Myagkova [1] and Mal'cev [10] some other finiteness conditions are given under which locally nilpotent groups are nilpotent.

Finally we mention the following theorem (Baer [32]; the proof below is due to Fedorov). This theorem shows that in the case of nilpotent groups the maximal condition for subgroups can be replaced by a much simpler condition.

If in a nilpotent group G the factor group of the derived group is finitely generated, then all factors of the lower central series of G are finitely generated, and G itself satisfies the maximal condition for subgroups.

We shall prove the theorem by induction over the class of the nilpotent group G; for abelian groups, the theorem is obvious. Let

$$G = G_0 \supset G_1 \supset \ldots \supset G_{k-1} \supset G_k \supset G_{k+1} = E \tag{1}$$

be the lower central series of G. The factor group G/G_k occurs in the lower central series

$$G/G_k \supset G_1/G_k \supset \ldots \supset G_{k-1}/G_k \supset G_k/G_k = E,$$

so that, by the induction hypothesis, the theorem is true for G/G_k. It follows that G/G_k has a finite system of generators

$$x_1 G_k,\ x_2 G_k,\ \ldots,\ x_m G_k.$$

Also all the factor groups of (1), except (possibly) the last, are finitely generated; in particular, G_{k-1}/G_k has a finite system of generators

$$y_1 G_k,\ y_2 G_k,\ \ldots,\ y_n G_k.$$

We know, moreover, that G_k lies in the center of G and is generated by all the possible commutators of the form $[x, y]$, where $x \in G$, $y \in G_{k-1}$. However, the element x can be written as a word v in the elements $x_1, x_2, \ldots, x_m$, multiplied by an element of G_k, that is, an element of the center; similarly y can be written as a word w in the elements $y_1, y_2, \ldots, y_n$, also multiplied by an element of the center. Therefore the commutator $[x, y]$ is equal to the commutator of v and w. But this can be written as a product of powers of the commutators $[x_i, y_j]$, $i = 1, 2, \ldots, m$, $j = 1, 2, \ldots, n$: we need

only use the commutator properties (1) to (4) of § 14 and take into account that every commutator of an element of G with an element of G_{k-1} lies in the center of G. This proves that G_k is also finitely generated. Thus, all the factors of (1) are finitely generated, and since the nilpotent group G is solvable and since (1) is a solvable series of G, we see by Hirsch's Theorem of § 59 that G satisfies the maximal condition for subgroups.[1]

The paper by Baer [32] also contains a number of other results closely related to the one just proved or generalizations of it.

§ 65. Complete nilpotent groups

As we know, complete abelian groups play a very important rôle in the theory of abelian groups: an exhaustive classification of them has been given in § 23. The definition of a complete group can easily be extended, as follows, to non-commutative groups: A group G is called *complete* if, for any element a of G and an arbitrary natural number n, the equation

$$x^n = a$$

has at least one solution in G or, in other words, if every root of every element of G belongs to G.

The structure of a complete group may be very complicated. However, it is natural to expect that complete nilpotent groups, which are very closely related to complete abelian groups, may form the object of a rather far-reaching theory. Such a theory has been developed by Černikov [10, 13] and will be expounded in the present section. It turns out to be convenient not to confine ourselves to complete nilpotent groups but to study at once arbitrary complete ZA-groups; some of the results to be obtained here cannot, however, be extended to arbitrary complete locally nilpotent groups.

We shall call a group G *Černikov complete* if for every natural number n it is generated by the n-th powers of all its elements. Of course, *every complete group is Černikov complete*. The converse, which is obvious for abelian groups, does not hold in general; it will be proved for ZA-groups after some preliminary considerations. To avoid cumbersome formulations in deriving this result we shall understand by a complete group one that is Černikov complete.

[1] Other proofs of this theorem are contained in papers by P. Hall [12] and Jennings [2].

A ZA-group is complete if and only if it contains no proper subgroup of finite index.

For if a complete group G, which need not even be a ZA-group, had a proper subgroup of finite index, then it would also have a proper normal subgroup of finite index. However, a complete group cannot have non-trivial finite factor groups, because the homomorphic image of a complete group is itself a complete group and a finite group other than E can never be complete—it is sufficient to take for n the order of the group.

Conversely, let G be a ZA-group containing no proper subgroup of finite index and let n be an arbitrary natural number. We denote by H the subgroup generated by the n-th powers of all the elements of G. We have to show that $G = H$. If this is not so, then we consider the factor group G/H, H being normal in G. Either it is abelian or, as a ZA-group, it has a non-trivial abelian factor group by Grün's Lemma of § 64. In both cases we can find in G a non-trivial abelian factor group with elements of bounded orders. Prüfer's First Theorem (§ 24) shows that such an abelian group is a direct product of cyclic groups and therefore has a proper subgroup of finite index which corresponds to a proper subgroup of finite index in G, in contradiction to the assumption. This proves the theorem.

The periodic part of a complete ZA-group G is contained in the center of the group.

Let

$$E = Z_0 \subset Z_1 \subset \ldots \subset Z_\alpha \subset Z_{\alpha+1} \subset \ldots \subset Z_\gamma = G$$

be the upper central series of G and let a be an element of G of finite order other than the unit element,

$$a^n = 1. \tag{1}$$

There exists an α such that

$$a \notin Z_\alpha, \qquad a \in Z_{\alpha+1}.$$

We have to show that $\alpha = 0$.

Let $\alpha = 1$. We show that x^n is permutable with a, where x is an arbitrary element of G. The subgroup $H = \{a, x\}$ is nilpotent and, as $a \in Z_2$, its class does not exceed two. If this subgroup is abelian, then there is nothing to prove. Otherwise, let

$$E \subset Z' \subset H$$

be its upper central series. The subgroup $\{Z', x\}$ is normal in H, so that x is permutable with all its conjugates in H. Hence

$$x(a^{-1}xa)(a^{-2}xa^2)\dots(a^{-n+1}xa^{n-1}) = x^n[x,\ a][x,\ a^2]\dots[x,\ a^{n-1}].$$

The left-hand side of this equation is permutable with x. Transformation by a does not change it, because of (1), so that it is an element of the center Z' of H. The commutators on the right-hand side also lie in Z'; therefore $x^n \in Z'$. Hence a is permutable with x^n for an arbitrary x in G, and as G is a complete group, every element of G can be written as a product of n-th powers of certain of its elements; therefore a turns out to lie in the center of G, in contradiction to the assumption $\alpha = 1$.

Let β be an arbitrary ordinal number greater than 1. Suppose we have already proved that the inequality $1 \leqq \alpha < \beta$ is impossible. We put $\alpha = \beta$. Then $a \in Z_{\beta+1}$, and therefore the commutator $[x, a]$ for an arbitrary x of G is contained in Z_β. However

$$[x,\ a] = (x^{-1}a^{-1}x)\,a.$$

On the right we have the product of two factors of finite order; therefore $[x, a]$ also belongs to the periodic part of G—that is, it has finite order. It follows from the induction hypothesis that this commutator, as an element of Z_β, must even belong to the center Z_1 of G. As the element x was arbitrary we see that, in fact, $a \in Z_2$, in contradiction to the assumption $\beta > 1$.

This proves the theorem. We deduce from it that *every periodic complete ZA-group is abelian.* Some generalizations of this last result can be found in a paper by Muhammedžan [2]. The result cannot, however, be extended to arbitrary periodic complete locally nilpotent groups; Černikov [10] has constructed an example of a non-commutative complete locally finite p-group.

If the periodic part F of a complete ZA-group G is finite, then $F = E$; in other words, G is torsion-free. Moreover, in this case G has an ascending central series in which all the factors are complete abelian torsion-free groups. We can even assume that all these factors are of rank 1.

We have seen above that F is contained in the center Z of G. If G is abelian, then everything is proved, because the periodic part of a complete abelian group is either E or infinite, and a complete abelian torsion-free group is a direct product of groups isomorphic to the additive group of the rational numbers (see § 23). Otherwise, by Grün's Lemma (§ 64), Z contains a non-trivial subgroup onto which G can be mapped homomorphically.

This is the homomorphic image of a complete group and is therefore itself complete. We denote by L_1 an arbitrary complete subgroup of Z; we can, of course, assume that it has rank 1. As a subgroup of the center, L_1 is normal in G. Further,

$$L_1 \cap F = E;$$

this follows from what we have shown above about the periodic part of a complete abelian group. Finally, the periodic part of G/L_1 is FL_1/L_1 and is therefore finite. For if an element aL_1 has finite order n in G/L_1, then $a^n \in L_1$. As L_1 is a complete abelian group, we can find in it an element b such that $a^n = b^n$; and since b lies in the center, $(ab^{-1})^n = 1$—that is, $ab^{-1} \in F$; therefore

$$aL_1 = (ab^{-1})L_1 \in FL_1/L_1.$$

Suppose we have already constructed in G a strictly increasing chain of normal subgroups

$$L_1 \subset L_2 \subset \ldots \subset L_\alpha \subset \ldots, \tag{2}$$

where α is less than an ordinal number β, such that for all α:

$$L_\alpha \cap F = E,$$

the periodic part of G/L_α is FL_α/L_α, and the factor $L_{\alpha+1}/L_\alpha$ lies in the center of G/L_α and is a complete abelian torsion-free group. If β is a limit number, then we take as L_β the union of all L_α, $\alpha < \beta$. This is a normal subgroup of G, and its intersection with F is E. Let us find the periodic part of G/L_β. If a coset aL_β has finite order n in G/L_β, so that $a^n \in L_\beta$, then there exists an α less than β such that $a^n \in L_\alpha$. Therefore, by the induction hypothesis, the coset aL_α is contained in the factor group FL_α/L_α; that is,

$$aL_\alpha = cL_\alpha, \qquad c \in F;$$

and then

$$aL_\beta = cL_\beta,$$

or $aL_\beta \in FL_\beta/L_\beta$.

But if $\beta - 1$ exists, then $G/L_{\beta-1}$ satisfies all the conditions to which the original group G was subject. We can therefore find in its center a non-trivial complete normal subgroup $L_\beta/L_{\beta-1}$, whose intersection with the periodic part $FL_{\beta-1}/L_{\beta-1}$ of $G/L_{\beta-1}$ is the unit subgroup. Hence

$$L_\beta \cap FL_{\beta-1} = L_{\beta-1},$$

and since by assumption

$$L_{\beta-1} \cap F = E,$$

then

$$L_\beta \cap F = E$$

also holds. Further, the periodic part of the factor group

$$(G/L_{\beta-1})/(L_\beta/L_{\beta-1})$$

coincides with

$$(FL_{\beta-1}/L_{\beta-1}) \cdot (L_\beta/L_{\beta-1})/(L_\beta/L_{\beta-1}),$$

and hence it follows that the periodic part of G/L_β is FL_β/L_β. Finally, we mention that $L_\beta/L_{\beta-1}$ can be chosen such that its rank is 1.

Thus, the strictly increasing chain (2) can be continued as long as L_α does not coincide with G. However, for $F \neq E$, this can never happen, since the intersection of F with an arbitrary L_α is E. We have thus proved that $F = E$. The ascending chain (2), brought up to G itself, now turns into the required ascending central series of G. The last part of the theorem follows from the remarks made in the course of the proof.

Next we shall prove a theorem which would not be true under the definition of completeness with which we began the section.

The periodic part F of a complete ZA-group G is itself Černikov complete.

If F has a proper subgroup F_0 of finite index, then the latter, as a subgroup of the center, is normal in G. The factor group G/F_0 is complete and is a ZA-group, but its periodic part F/F_0 is finite and is not E, in contradiction to what we have shown above. Hence F cannot have a proper subgroup of finite index and, being an abelian group, is therefore complete; this follows from the first theorem of this section. This proves the theorem.

On the basis of this and the preceding results we can now prove the following theorem.

Every complete ZA-group G has an ascending central series

$$E \subseteq L_0 \subset L_1 \subset \ldots \subset L_\alpha \subset \ldots \subset L_\gamma = G, \tag{3}$$

where L_0 is a periodic complete abelian group, possibly equal to E, and all the subsequent factors are complete abelian torsion-free groups. We can even assume that all these factors are of rank 1.

For we can take as L_0 the periodic part of G. As we have proved, it lies in the center and is complete. Its factor group is a complete torsion-free ZA-group, so that it only remains to apply the above theorem.

We next prove the following theorem.

If a ZA-group G is complete in the sense of Černikov, then it is also complete in the sense of the original definition in this section.

Let a be an element of G and let n be a natural number. We have to show that the equation

$$x^n = a$$

has at least one solution in G. We construct in G an ascending central series (3) in accordance with the preceding theorem. There exists an α such that

$$a \notin L_\alpha, \qquad a \in L_{\alpha+1}.$$

Since $L_{\alpha+1}/L_\alpha$ is a complete abelian group, there exists an element x_1 in $L_{\alpha+1}$ such that

$$aL_\alpha = (x_1 L_\alpha)^n,$$

and hence

$$a = x_1^n a_1, \qquad a_1 \in L_\alpha. \tag{4}$$

There exists an index α_1, $\alpha_1 < \alpha$, such that

$$a_1 \notin L_{\alpha_1}, \qquad a_1 \in L_{\alpha_1+1}.$$

We know that $L_{\alpha_1+1}/L_{\alpha_1}$ is a complete abelian group and that it lies in the center of G/L_{α_1}. Therefore there exists an element x_2 in L_{α_1+1} such that

$$a_1 L_{\alpha_1} = (x_2 L_{\alpha_1})^n.$$

Hence, by (4),

$$aL_{\alpha_1} = (x_1 L_{\alpha_1})^n (x_2 L_{\alpha_1})^n = (x_1 x_2)^n L_{\alpha_1},$$

and therefore

$$a = (x_1 x_2)^n a_2, \qquad a_2 \in L_{\alpha_1}.$$

Suppose we have already found a decreasing finite set of indices

$$\alpha > \alpha_1 > \alpha_2 > \ldots > \alpha_{k-1},$$

with

$$a = (x_1 x_2 \ldots x_k)^n a_k, \qquad a_k \in L_{\alpha_{k-1}}.$$

Then there exists an index α_k, $\alpha_k < \alpha_{k-1}$, such that

$$a_k \notin L_{\alpha_k}, \qquad a_k \in L_{\alpha_{k+1}}.$$

Repeating the preceding arguments we find that

$$a = (x_1 x_2 \dots x_k x_{k+1})^n a_{k+1}, \qquad a_{k+1} \in L_{\alpha_k}.$$

After a finite number of steps we come to an equation

$$a = (x_1 x_2 \dots x_l)^n a_l,$$

where $a_l \in L_0$ or, in case $L_0 = E$, $a_l \in L_1$. In the complete abelian group L_0 (or L_1) there exists an element x_{l+1} such that

$$a_l = x_{l+1}^n$$

and, as x_{l+1} lies in the center of G,

$$a = (x_1 x_2 \dots x_l x_{l+1})^n,$$

and this is what we had to prove.

From now on we shall again interpret the completeness of a group as the unlimited possibility of extracting roots of all the elements of the group.

The following principal theorem describes the structure of complete ZA-groups rather well; in the commutative case it turns into the classification of complete abelian groups with which we are acquainted.

Principal Theorem. *In every complete ZA-group G we can find a system of subgroups*

$$A_0, A_1, A_2, \dots, A_\alpha, \dots, \alpha < \gamma \tag{5}$$

with the following properties:

(1) *Every A_α, $0 \leqq \alpha < \gamma$ is either a group of type p^∞ for some prime number p or a group isomorphic to the additive group of all rational numbers.*

(2) *The subgroup B_β, $0 \leqq \beta < \gamma$, generated by all subgroups A_α, $0 \leqq \alpha < \beta$, is normal in G.*

(3) *For all β, $0 < \beta < \gamma$,*

$$B_\beta \cap A_\beta = E.$$

(4) $B_\gamma = G$.

Conversely, every group G having a system of subgroups (5) *with the properties* (1)-(4) *is a complete ZA-group.*

Proof. Let G be a complete ZA-group. We have shown above that it has an ascending central series

$$E \subseteq L_0 \subset L_1 \subset \ldots \subset L_\alpha \subset \ldots \subset L_\gamma = G$$

such that L_0 is a periodic complete abelian group and all factors $L_{\alpha+1}/L_\alpha$, $\alpha = 0, 1, \ldots$, are complete abelian torsion-free groups of rank 1. If L_0 is different from E, then it is the direct product of groups of type p^∞ for some prime numbers p; let these be $A_0, A_1, \ldots, A_\alpha, \ldots$, where α is less than a certain ordinal number δ. Thus, condition (3) is satisfied for $0 < \beta < \delta$. Moreover, as L_0 lies in the center of G, condition (2) is satisfied for $0 < \beta \leqq \delta$.

We know, further, that L_α, $\alpha \geqq 0$, is a normal subgroup of G and therefore of $L_{\alpha+1}$. Let us show that $L_{\alpha+1}$ is a splitting extension of L_α.

Let x_1 be an arbitrary element of $L_{\alpha+1}$, outside L_α. We define elements x_k, $k = 2, 3, \ldots$, by induction: the element x_k is one of the solutions of the equation

$$x^k = x_{k-1};$$

x_k exists, because G is complete. As the coset $x_1 L_\alpha$ has infinite order in $L_{\alpha+1}/L_\alpha$, the order of x_1 is also infinite and

$$\{x_1\} \cap L_\alpha = E.$$

Thus, x_1 is contained in some subgroup isomorphic to the additive group of rational numbers (see § 7); we denote it by A_α'.

From the equation

$$(x_k L_\alpha)^k = x_{k-1} L_\alpha$$

it follows that the elements $x_k L_\alpha$, $k = 1, 2, \ldots$ generate in $L_{\alpha+1}/L_\alpha$ a subgroup isomorphic to the additive group of rational numbers, that is, isomorphic to $L_{\alpha+1}/L_\alpha$ itself. However, the abelian group $L_{\alpha+1}/L_\alpha$, being indecomposable into a direct sum, cannot contain proper complete subgroups. This shows that every coset of L_α in $L_{\alpha+1}$ contains one and only one element of A_α', and this implies what we had to prove.

We know that

$$B_\delta = \{A_\alpha,\ 0 \leqq \alpha < \delta\} = L_0.$$

By induction over β it is easy to establish that

$$\{L_0;\ A_\alpha',\ 0 \leqq \alpha < \beta\} = L_\beta,\ 0 \leqq \beta \leqq \gamma.$$

Therefore, all the conditions of the first half of the theorem are satisfied if we take for (5) the system of subgroups

$$A_\alpha,\ 0 \leqq \alpha < \delta;\ A_\alpha',\ 0 \leqq \alpha < \gamma.$$

We now proceed to the proof of the second half of the theorem. First we prove a lemma.

LEMMA. *If a group A, isomorphic to a group of type p^∞ or to the additive group of rational numbers, is a normal subgroup of a group G that has no proper subgroup of finite index, then A is contained in the center of G.*

To begin with, let A be a group of type p^∞, and let a be an arbitrary element of A. The subgroup $\{a\}$ is cyclic of prime-power order, say p^n. A has only one subgroup of this order, so that $\{a\}$ is characteristic in A and therefore normal in G. Thus, a has a finite number of conjugates in G and since, by assumption, G has no proper subgroup of finite index, a lies in the center of G.

Let A be now isomorphic to the additive group of rational numbers. We know from § 21 that the group of automorphisms Γ of A is isomorphic to the multiplicative group of non-zero rational numbers, so that it is the direct product of cyclic groups (see § 17). Every subgroup of Γ is also a direct product of cyclic groups (see § 24) and therefore cannot be complete.

The transformation of A by an arbitrary element of G induces an automorphism in A. We obtain a homomorphic mapping of G into a subgroup Γ' of Γ. As G, by assumption, contains no proper subgroups of finite index, there are no such subgroups in Γ' either. The abelian group Γ' is therefore complete and, by what we have shown above, $\Gamma' = E$. This shows that A lies in the center of G and completes the proof of the lemma.

Now let G be a group having a system of subgroups (5) with conditions (1)-(4). We shall show that G has no proper subgroup of finite index. It is clear that there are no such subgroups in $B_1 = A_0$, which is a complete abelian group. Suppose we have already proved that subgroups of finite index do not exist in any of the subgroups B_α, $0 < \alpha < \beta$. If β is a limit number, then there are no such subgroups in B_β, because B_β is the union of all B_α, $\alpha < \beta$, and the intersection of a subgroup of finite index in B_β with an arbitrary B_α would give a subgroup of finite index in B_α, that is, would be equal to B_α.

Suppose now that $\beta - 1$ exists. If B_β contains a subgroup H of finite index, then as above, $H \supset B_{\beta-1}$, so that $H/B_{\beta-1}$ is a subgroup of finite index in

$$B_{\beta}/B_{\beta-1} \simeq A_{\beta-1};$$

but this is impossible.

This shows that there are no subgroups of finite index in any subgroup B_β, and among them, in $B_\gamma = G$. Therefore, there are no such subgroups in any factor group G/B_β, $0 < \beta < \gamma$. Hence it follows from the lemma that $B_1 = A_0$, as a normal subgroup of G, lies in the center of G and that for $0 < \beta < \gamma$ the subgroup $B_{\beta+1}/B_\beta$, which is isomorphic to A_β and normal in G/B_β, lies in the center of G/B_β. Therefore

$$E \subset B_1 \subset \ldots \subset B_\beta \subset \ldots \subset B_\gamma = G$$

is an ascending central series of G, so that G turns out to be a ZA-group. From the fact that G has no proper subgroups of finite index it now follows, by the first theorem of the present section, that G is complete. This concludes the proof of the theorem.

In papers by Černikov [10, 13, 19] the reader can find a number of other properties of complete ZA-groups. See also Čarin [3].

§ 66. Groups with unique extraction of roots

Whenever we deal with locally finite groups or p-groups or groups with minimal condition for subgroups we remain within the domain of periodic groups. The other extreme case, namely that of torsion-free groups, is also very interesting.

Arbitrary non-commutative torsion-free groups of course form an immensely wide class of groups. A narrower class is the class of *groups in which the extraction of roots is unique*, or briefly, *R-groups*. They are the groups in which for every element a and every natural number n the equation

$$x^n = a$$

has not more than one solution; in other words, for every pair of elements x and y and every natural number n it follows from $x^n = y^n$ that $x = y$.

It is obvious that every R-group is torsion-free and that all abelian torsion-free groups are R-groups. It is also easy to verify that every free group is an *R-group*. But *not every torsion-free group is an R-group*: the group with the generators a, b and the defining relation $a^2 = b^2$, which is the free product of two infinite cyclic groups with an amalgamated subgroup, is torsion-free, by § 35, but is not an R-group.

R-groups are studied in papers by Kontorovič [5, 7]; see also Plotkin [1, 3]. We shall indicate only some of the main properties of these groups, following the paper by Kontorovič [5].

In the theory of R-groups the concept of a *serving subgroup* plays an important rôle; it is carried over from the theory of abelian groups (see §§ 25, 30), but here it is more often known under another name: a subgroup A of an R-group G is called an *isolated subgroup* of G if for every element a of A and every natural number n the solution of the equation

$$x^n = a,$$

if it exists in G, belongs to A.

The group G itself and its unit subgroup are isolated in G. Since the extraction of roots is unique, *the intersection of an arbitrary set of isolated subgroups of an R-group is itself isolated.* Hence there exists a unique minimal isolated subgroup of an R-group G containing a given set of elements M; this group is called the *isolated closure* or *isolator* of M in G and is denoted by $I(M)$.

It is obvious that a normal subgroup H of an R-group G is isolated if and only if the factor group G/H is torsion-free. Note that this factor group need not be an R-group.

If H is an isolated normal subgroup of an R-group G and if the factor group G/H is an R-group, then in the natural one-to-one correspondence between all the subgroups of G/H and all the subgroups of G containing H isolated subgroups correspond to one another.

For let A be an isolated subgroup of G containing H. If

$$(gH)^n = aH,\ g \in G,\ a \in A,$$

then $g^n = ah \in A$, and since A is isolated, we have $g \in A$, so that gH is an element of A/H. Conversely, let A/H be an isolated subgroup of G/H. If

$$g^n = a,\ g \in G,\ a \in A,$$

then

$$(gH)^n = aH,$$

and since A/H is isolated, gH is an element of A/H, so that $g \in A$.

The centralizer of an arbitrary set of elements of an R-group is an isolated subgroup.

For let M be a set of elements of an R-group G and let x be such that x^n belongs to the centralizer of M, so that for every a of M

$$a^{-1}x^n a = x^n.$$

Hence

$$(a^{-1}xa)^n = x^n,$$

and therefore, by the definition of an R-group,

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

so that x itself belongs to the centralizer of M.

It follows that *the center of an R-group is isolated.* Of course, we do not claim that the center of an R-group differs from the unit subgroup.

In every R-group G the equation

$$a^k b^l = b^l a^k,$$

where a and b are any two elements of G, implies that

$$ab = ba.$$

It is sufficient to consider the case when one of the exponents, for example l, is equal to 1, that is, $a^k b = ba^k$. Then

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

Hence, by the definition of an R-group,

$$b^{-1}ab = a,$$

and this is what we had to prove.

The following theorem holds.

A torsion-free group is an R-group if and only if the factor group of its center is an R-group.

For we already know that the center Z of an R-group G is isolated, so that G/Z is torsion-free. Let

$$(xZ)^n = (yZ)^n, \quad x, y \in G.$$

Hence

$$x^n = y^n z, \quad z \in Z. \tag{1}$$

This equation shows that x^n and y^n are permutable and, by what we have proved above, x and y are also permutable. From (1) we now obtain

$$(y^{-1}x)^n = z,$$

and as Z is isolated,

$$y^{-1}x \in Z,$$

and hence

$$xZ = yZ.$$

Conversely, let the factor group of the center Z of a torsion-free group G be an R-group. If

$$x^n = y^n, \tag{2}$$

where x, y are elements of G, then

$$(xZ)^n = (yZ)^n.$$

But since G/Z is an R-group

$$xZ = yZ$$

or $x = yz$, $z \in Z$. Raising this to the n-th power we obtain

$$x^n = y^n z^n.$$

By (2) we have $z^n = 1$, and since G is torsion-free, $z = 1$, and therefore $x = y$.

On the basis of these results it is easy to prove the following theorem.

All the terms of the upper central chain

$$E = Z_0 \subseteq Z_1 \subseteq Z_2 \subseteq \ldots \subseteq Z_\alpha \subseteq \ldots$$

of an R-group G are isolated in G, all the factors $Z_\alpha/Z_{\alpha-1}$ of this chain are abelian torsion-free groups, and all the factor groups G/Z_α are R-groups.

For since Z_1 is the center of G, the factor $Z_1/Z_0 = Z_1$ is abelian and torsion-free, Z_1 is isolated in G, and the factor group G/Z_1 is an R-group.

Suppose the theorem already proved for all indices α less than β. If the number $\beta - 1$ exists, then $G/Z_{\beta-1}$ is an R-group. Therefore its center $Z_\beta/Z_{\beta-1}$ is an abelian torsion-free group; the factor group of the center, isomorphic to G/Z_β, is an R-group; and from the fact that the center $Z_\beta/Z_{\beta-1}$ of $G/Z_{\beta-1}$ is isolated it follows, on the basis of the above theorem

on the correspondence between isolated subgroups of a group and its factor group, that Z_β is isolated in G.

But if β is a limit number, then Z_β is the union of an ascending sequence of isolated subgroups and is therefore isolated. Moreover, if

$$(xZ_\beta)^n = (yZ_\beta)^n, \quad x, y \in G,$$

then $x^n = y^n z$, where $z \in Z_\beta$, and therefore $z \in Z_\alpha$, $\alpha < \beta$. Hence

$$(xZ_\alpha)^n = (yZ_\alpha)^n,$$

and since G/Z_α is, by hypothesis, an R-group, then $xZ_\alpha = yZ_\alpha$ and *a fortiori* $xZ_\beta = yZ_\beta$. This proves that G/Z_β is an R-group.

We mention that *the derived group of an R-group need not be isolated.* For example, let us consider the group G with the generators a, b, c and the defining relations

$$ac = ca, \quad bc = cb, \quad [a, b] = c^2.$$

The center of the group is the cyclic subgroup $\{c\}$, so that the factor group of the center is an abelian torsion-free group, that is, an R-group; therefore by the above theorem G itself is an R-group. But the factor group of its derived group contains an element of order 2; therefore the derived group is not isolated.

The following property of R-groups could also be taken as their definition, provided the concept of an isolated subgroup is duly extended to arbitrary torsion-free groups.

The isolator of an arbitrary element other than the unit element of an R-group is an abelian torsion-free group of rank 1 *and is the isolator of each of its elements other than* 1. *The isolators of any two elements of an R-group either are identical or else intersect in the unit element.*

For in every torsion-free group G an arbitrary element x, $x \neq 1$, generates an infinite cyclic subgroup which is an abelian torsion-free group of rank 1. Since the union of an ascending sequence of abelian torsion-free groups of rank 1 is a group of the same kind, x is contained in at least one subgroup A that is a maximal abelian torsion-free subgroup of G of rank 1. If G is now an R-group, then A is contained in the isolator $I(x)$ of x: for an arbitrary a of A the cyclic subgroups $\{x\}$ and $\{a\}$ have an intersection other than E, but clearly $\{x\} \subset I(x)$.

But suppose that x is contained in two distinct maximal abelian torsion-free subgroups of rank 1, A and B; the intersection of these two subgroups is therefore not E. Let a and b be arbitrary elements, other than 1, of A and B, respectively. Since certain powers of these elements are equal and therefore permutable, a and b are themselves permutable, by a property of R-groups proved above. Thus, $\{A, B\}$ is an abelian torsion-free group. However, in such a group distinct maximal subgroups of rank 1 cannot have an intersection other than E (see § 30). Hence all the parts of the theorem follow easily.

The significance of R-groups for the theory of nilpotent groups lies in the following theorem (Mal'cev [6]; Černikov [19]; the proof below is in a paper by Sesekin [1]).

Every nilpotent torsion-free group is an R-group.

For abelian torsion-free groups there is nothing to prove; we can therefore conduct the proof by induction over the class of the nilpotent group. Let G be a group of class k, $k > 1$, with the upper central series

$$E = Z_0 \subset Z_1 \subset \ldots \subset Z_{k-1} \subset Z_k = G$$

and let x and y be two elements of G such that

$$x^n = y^n, \; n > 0. \tag{3}$$

The subgroup $H = \{Z_{k-1}, x\}$ is normal in G, because G/Z_{k-1} is abelian; furthermore, it is nilpotent and its class is not greater than $k-1$: in § 11 we proved that in a non-commutative group the factor group of the center cannot be cyclic. Therefore H is an R-group. Now by (3)

$$x^n = y^{-1}x^n y = (y^{-1}xy)^n,$$

but as both x and $y^{-1}xy$ belong to the R-group H, we have $x = y^{-1}xy$, or $xy = yx$. Therefore (3) can be rewritten in the form

$$(xy^{-1})^n = 1;$$

but since G is torsion-free, $x = y$. This proves the theorem.

The local theorem for the property of being an R-group obviously holds; therefore we can even assert that every locally nilpotent torsion-free group is an R-group.

§ 67. Locally nilpotent torsion-free groups

From the theorem at the end of the preceding section it follows that all the properties that have been established above for R-groups are true, in particular, for arbitrary locally nilpotent torsion-free groups. These latter groups, however, admit of a much deeper analysis. This analysis is, as yet, far from complete, and in this section we shall mention only some results on which further investigations may be based.

We know from § 25 that the isolator of a subgroup A of an abelian torsion-free group G, that is, the serving subgroup of G generated by A, consists of all the elements of G a positive power of which occurs in A. Let us show that arbitrary locally nilpotent torsion-free groups have the same property. The following lemma holds (Mal'cev [5]; the proof is due to Fedorov).

LEMMA. *Let G be a nilpotent torsion-free group having a finite system of generators*

$$x_1, x_2, \ldots, x_s \tag{1}$$

and let D be a subgroup of G such that some positive power n_i of every element x_i of (1), $i = 1, 2, \ldots, s$ lies in D. Then D is of finite index in G, so that a positive power of every element of G lies in D.

We shall prove the lemma by induction over the class of G. Let

$$G = G_0 \supset G_1 \supset \ldots \supset G_{k-1} \supset G_k \supset G_{k+1} = E$$

be the lower central series of G. By the last theorem of § 64, G_k is finitely generated. In addition to the lemma we shall prove the following statement.

G_k has a finite system of generators such that some positive power of every element of G_k lies in D.

For groups of class 1, that is, for abelian groups, all the statements are obvious. Suppose they are already proved for groups of class k. Then DG_k/G_k has finite index in G/G_k, therefore DG_k has finite index in G. Moreover, G_{k-1}/G_k has a finite system of generators

$$y_1 G_k, \; y_2 G_k, \ldots, \; y_t G_k,$$

such that

$$(y_j G_k)^{m_j} \in DG_k/G_k, \quad j = 1, 2, \ldots, t. \tag{2}$$

As in the proof of the last theorem of § 64, we can now show that the elements $[x_i, y_j]$, $i = 1, 2, \ldots, s$, $j = 1, 2, \ldots, t$, form a system of generators for G_k. By the commutator properties (1)-(4) of § 14,

$$[x_i, y_j]^{n_i m_j} = [x_i^{n_i}, y_j^{m_j}]. \tag{3}$$

However, the element $x_i^{n_i}$ lies in D, and by (2) the element $y_j^{m_j}$ differs from an element of D by a factor lying in the center of G. This proves that the right-hand side of (3) is contained in D. We have therefore found in G_k a finite system of generators such that some positive power of every element of the system lies in D.

Hence it follows, since G_k is abelian, that the intersection $D \cap G_k$ has finite index in G_k. By the isomorphism

$$G_k/(D \cap G_k) \simeq DG_k/D$$

D has finite index in DG_k, and since we have already shown that GD_k has finite index in G we have proved all the statements of the lemma.

In a locally nilpotent torsion-free group G the isolator $I(A)$ of an arbitrary subgroup A consists precisely of those elements of G some positive power of which belongs to A.

It is clear that $x^n \in A$ implies $x \in I(A)$. Further, let

$$x^n \in A, \quad y^m \in A.$$

The subgroup $H = \{x, y\}$ of G is a nilpotent group with two generators; therefore, by the lemma, some positive power of every element of H, and in particular of xy, belongs to the intersection $A \cap H$, that is, to A. Hence it follows that all the elements of G some positive power of which lie in A form a subgroup. This subgroup is obviously isolated and therefore it is $I(A)$.

Another proof of this theorem occurs in a paper by Plotkin [3].

We next prove the following theorem (Gluškov [1]; see also Plotkin [1], Smirnov [1]).

In a locally nilpotent torsion-free group the normalizer of an isolated subgroup is isolated.

First of all, we consider a *nilpotent* torsion-free group G with a central series

$$E = Z_0 \subset Z_1 \subset \ldots \subset Z_k \subset Z_{k+1} \subset \ldots \subset Z_n = G.$$

Let A be an isolated subgroup of G, N its normalizer, and x an element such that

$$x^m \in N \text{ but } x \notin N. \tag{4}$$

The subgroup $x^{-1}Ax$ does not lie within A, because then (4) could not hold; we can therefore find an element a in A such that

$$x^{-1}ax \notin A. \tag{5}$$

Let

$$a \in Z_{k+1}, \quad a \notin Z_k. \tag{6}$$

Moreover, we shall assume that a is chosen such that the suffix k, $1 \leqq k < n$, is as small as possible, so that

$$x^{-1}(A \cap Z_k)x \subset A. \tag{7}$$

We can assume also that

$$x(A \cap Z_k)x^{-1} \subset A, \tag{8}$$

otherwise we replace x by x^{-1}—it follows from (4) that $x^{-m} \in N$.

We put

$$[a, x] = y_1, \quad [y_i, x] = y_{i+1}, \quad i = 1, 2, \ldots.$$

By (6),

$$y_i \in Z_k, \; i = 1, 2, \ldots, \tag{9}$$

and the definition of a central series implies that

$$y_{k+1} = y_{k+2} = \ldots = 1. \tag{10}$$

Since

$$x^{-1}ax = ay_1, \tag{11}$$

we have, by (5),

$$y_1 \notin A. \tag{12}$$

We also note that

$$x^{-1}y_i x = y_i y_{i+1}, \quad i = 1, 2, \ldots. \tag{13}$$

The letter z with subscripts shall be used to denote products of elements y_i. By (9) every such product lies in Z_k; if it also lies in A, then

by (7) and (8) its images under the transformations by x and x^{-1} also belong to A. We shall denote by z' or $z^{(1)}$ the product obtained from z by increasing by 1 the indices of all the factors y_i occurring in z. Furthermore, we put $z^{(s)} = (z^{(s-1)})'$, where $z^{(0)} = z$.

Let us show that for all $i \geqq 1$ we can find z_i such that

$$x^{-i}ax^i = az_i, \tag{14}$$

and

$$z_i = z_{i-1}y_1z'_{i-1}. \tag{15}$$

for $i > 1$. Clearly $z_1 = y_1$, and by (11) and (13) we have

$$x^{-2}ax^2 = x^{-1}axx^{-1}y_1x = ay_1y_1y_2,$$

so that $z_2 = z_1y_1z_1'$. Suppose (14) and (15) have already been proved for all $i < j$. Then for any i with $1 < i < j$,

$$x^{-i}ax^i = x^{-1}az_{i-1}x = ay_1 \cdot x^{-1}z_{i-1}x,$$

so that $z_i = y_1x^{-1}z_{i-1}x$, or

$$x^{-1}z_{i-1}x = y_1^{-1}z_i. \tag{16}$$

Hence by (13) we have, for $s = 1, 2, \ldots,$

$$x^{-1}z_{i-1}^{(s)}x = y_{s+1}^{-1}z_i^{(s)}. \tag{17}$$

and therefore, by (15), (11), (13), (16), and (17),

$$x^{-j}ax^j = x^{-1}az_{j-1}x = x^{-1}ax \cdot x^{-1}z_{j-2}x \cdot x^{-1}y_1x \cdot x^{-1}z'_{j-2}x =$$
$$= ay_1 \cdot y_1^{-1}z_{j-1} \cdot y_1y_2 \cdot y_2^{-1}z'_{j-1} = az_{j-1}y_1z'_{j-1}.$$

Hence (14) and (15) follow for j. The equation (15), of course, implies for $s = 1, 2, \ldots$ that

$$z_i^{(s)} = z_{i-1}^{(s)}y_{s+1}z_{i-1}^{(s+1)}. \tag{18}$$

From (4) and (14) it follows that

$$z_m \in A, \tag{19}$$

that is, by (15),

$$z_{m-1} y_1 z'_{m-1} \in A.$$

Therefore by (7), (16), (13), and (17),

$$x^{-1}(z_{m-1} y_1 z'_{m-1})\, x = x^{-1} z_{m-1} x \cdot x^{-1} y_1 x \cdot x^{-1} z'_{m-1} x =$$
$$= y_1^{-1} z_m y_1 z'_m \in A.$$

As $y_1^{-1} = x^{-1} a^{-1} x a$, we have, by (7) and (8),

$$z_m y_1 z'_m y_1^{-1} \in A$$

or by (19),

$$y_1 z'_m y_1^{-1} \in A,$$

and hence, again by (7) and (8), we have:

$$z_m' \in A.$$

Repeating these arguments with y_2 in place of y_1, we find that

$$z_m'' \in A.$$

In general,

$$z_m^{(i)} \in A, \; i = 1, 2, \ldots, k-1. \tag{20}$$

But the product $z_m^{(k-1)}$ is simply some positive power of y_k. Since A is an isolated group, it follows now that y_k is an element of A.

Suppose we have already proved that $y_k, y_{k-1}, \ldots, y_{i+1}$ lie in A, so that every product of the form $z^{(i)}$ is contained in A. By (20),

$$z_m^{(i-1)} \in A,$$

or, by (18),

$$z_{m-1}^{(i-1)} y_i z_{m-1}^{(i)} \in A.$$

The last factor on the left lies in A; therefore

$$z_{m-1}^{(i-1)} y_i \in A$$

or, by (7) and (8),

$$y_i z_{m-1}^{(i-1)} \in A.$$

Suppose we have already proved that

$$y_i^t z_{m-t}^{(i-1)} \in A. \tag{21}$$

Then, by (18)

$$y_i^t z_{m-t-1}^{(i-1)} y_i z_{m-t-1}^{(i)} \in A.$$

The last factor on the left lies in A; hence, if we again transform the remaining product by y_i^{-1} we find that

$$y_i^{t+1} z_{m-t-1}^{(i-1)} \in A.$$

Therefore, (21) holds for all t. For $t = m-1$ we get

$$y_i^{m-1} z_1^{(i-1)} \in A.$$

However $z_1^{(i-1)} = y_i$, because $z_1 = y_1$. Thus $y_i^m \in A$, and since A is isolated,

$$y_i \in A.$$

This proves that all the elements y_i, and y_1 in particular, lie in A; but this is in contradiction with formula (12).

We now turn to the case of a locally nilpotent torsion-free group G. Let A be an isolated subgroup of G, let N be its normalizer, and let $x^m \in N$, $x \notin N$. As above, we find an element a of A such that

$$x^{-1} a x \notin A. \tag{22}$$

The subgroup

$$H = \{a, x\}$$

is nilpotent and

$$A' = A \cap H$$

is isolated in H. Let N' be the normalizer of A' in H. By (22) $x \notin N'$. Furthermore it is clear that

$$x^{-m} A' x^m \subseteq A'.$$

If this were a strict inclusion, then we would have

$$x^m A' x^{-m} \supset A',$$

or

$$x^m A' x^{-m} \not\subset A,$$

although $x^{-m} \in N$. Therefore $x^{-m} \in N'$; but this leads to a contradiction to the above case of a nilpotent group.

This completes the proof. The theorem implies the following result (Plotkin [1], [3]).

If A and B are subgroups of a locally nilpotent group G and if A is normal in B, then the isolator $I(A)$ is normal in $I(B)$.

Clearly, $I(A) \subseteq I(B)$. Further, under an inner automorphism of a group the isolator of a subgroup goes over into the isolator of the image of the subgroup. Hence for an arbitrary element b of B

$$b^{-1} I(A) b = I(b^{-1} A b) = I(A);$$

that is, the whole subgroup B is contained in the normalizer of $I(A)$ in G. We have shown above that this normalizer is isolated; therefore it also contains $I(B)$, so that $I(A)$ is normal in $I(B)$.

We mention that Gluškov [4] has studied locally nilpotent torsion-free groups with chain conditions for isolated subgroups.

Completions of locally nilpotent torsion-free groups. The significance of complete groups in the theory of abelian groups has become manifest in many theorems of § 23. We recall the theorem that every abelian group *can be embedded* in a complete abelian group, that there exists a *minimal* complete abelian group containing a given abelian group G, and that it is *unique*—in other words, that there exists an isomorphism (extending the identity automorphism of G) between any two minimal complete abelian groups containing G.

The theorem on the embedding in a complete group can easily be extended to arbitrary groups (see B. H. Neumann [7]).

Every group G is contained in a complete group.

For let a be an arbitrary element of G and let k be an arbitrary natural number. Furthermore, let $B = \{b\}$ be a cyclic group, infinite if a is of infinite order, or of finite order nk if a has finite order n. Then the free product of G and B with an amalgamated subgroup $\{a\} = \{b^k\}$ (see § 35) and with

$$a = b^k$$

contains G as well as a solution of the equation $x^k = a$; it is not excluded that the equation may already have a solution in G itself.

Under the assumption that the set of pairs (a, k) is well-ordered, where $a \in G$ and where k is a natural number, we can transfinitely construct an ascending sequence of groups containing G, by applying the above construction successively to every pair (a, k) and, for limit numbers, by taking the union of the groups previously constructed. In this way we arrive at a group G_1, containing G, which contains every root of every element of G. Applying the same construction to G_1 we obtain a group G_2, and so on. The union of the ascending sequence of groups G_n, $n = 0, 1, 2, \ldots$, with $G_0 = G$, is obviously complete.

This proves the theorem. At the same time we see that, in general, we cannot expect the uniqueness of a minimal complete group containing G: the construction described in the proof, when applied to an abelian group G, yields an embedding of G in a very non-commutative complete group.

Are all the above properties of complete abelian groups preserved if we go from abelian groups not directly to arbitrary groups, but only to nilpotent groups?

In general, this is not the case: from Černikov's Theorem of § 65, to the effect that the periodic part of a complete ZA-group lies in the center of the group, it follows that a non-commutative periodic nilpotent group cannot be embedded in a complete nilpotent group. However, Mal'cev [6] has proved that the situation is entirely different if we confine ourselves to *torsion-free* nilpotent or even locally nilpotent groups. If G is a complete locally nilpotent torsion-free group, then obviously *the complete subgroups of G and they only are isolated in G*. Owing to this circumstance, some of the results obtained above can be re-phrased in the case of complete groups. Thus:

If G is a complete locally nilpotent torsion-free group, then the intersection of an arbitrary set of complete subgroups of G is itself complete; the normalizer of a complete subgroup of G is itself complete; all the terms of the upper central chain

$$E \subseteq Z_1 \subseteq Z_2 \subseteq \ldots \subseteq Z_\alpha \subseteq \ldots$$

of G are complete subgroups, all the factors of the chain are complete abelian torsion-free groups, and all the factor groups G/Z_α are complete locally nilpotent torsion-free groups.

Some of the statements of the last theorem are not immediate consequences of the corresponding theorem of the preceding section. In fact, the statement on the factor groups follows from the fact that they are homomorphic images of G and that Z_α is complete. The statement on the completeness of $Z_{\alpha+1}/Z_\alpha$ is then obtained by reference to the completeness of the center.

Let G be an arbitrary (not necessarily complete) locally nilpotent torsion-free group. If it is contained in some complete locally nilpotent torsion-free group $\overline{G}$, then the isolator of G in $\overline{G}$ is the minimal complete subgroup of $\overline{G}$ containing G.

A *completion* of G shall be defined to be an arbitrary minimal complete locally nilpotent torsion-free group G^* containing G. By the first theorem of the present section, *a complete locally nilpotent torsion-free group G^* is a completion of its subgroup G if and only if some positive power of every element of G^* lies in G.*

The following theorem of Mal'cev is fundamental for the whole theory of nilpotent torsion-free groups.

THEOREM. *Every locally nilpotent torsion-free group G can be embedded in a complete locally nilpotent torsion-free group and therefore possesses completions. If G_1^* and G_2^* are two completions of G, then there exists an isomorphism between them that extends the identity automorphism of G, and this isomorphism is unique.*

Mal'cev [6] has proved this theorem by an apparatus from the theory of groups and of Lie algebras. A direct proof has not yet been published, and so we are compelled to quote the theorem without proof.

Independently of Mal'cev's Theorem we can prove some theorems on completions of locally nilpotent torsion-free groups, substantially following Mal'cev [6].

If a complete locally nilpotent torsion-free group G^* is a completion of two of its subgroups G_1 and G_2, then it is also a completion of their intersection $G_1 \cap G_2$.

For if $x \in G^*$, then there exist two natural numbers k_1 and k_2 such that

$$x^{k_1} \in G_1, \qquad x^{k_2} \in G_2,$$

and therefore

$$x^{k_1 k_2} \in (G_1 \cap G_2).$$

If G^* is a completion of G and H^* a complete subgroup of G^*, then H^* is a completion of the intersection $H^* \cap G$, and this intersection is isolated in G. In this way a one-to-one correspondence is established between all the isolated subgroups of G and all the complete subgroups of G^*.

For, some positive power of every element of H^* lies in G, that is, in in $H^* \cap G$; and therefore H^* is a completion of this intersection. Further, if some positive power of an element g of G lies in $H^* \cap G$, then this element g is contained in the complete subgroup H^*, that is, in $H^* \cap G$, and therefore $H^* \cap G$ is isolated in G. Finally, if H is an isolated subgroup of G and H^* is its completion in G^*, then some positive power of every element of $H^* \cap G$ lies in H, and since H is isolated in G,

$$H^* \cap G = H.$$

This proves the theorem completely.

Finally, we prove a theorem that has been communicated to the author by Yu. G. Federov. *If G^* is a completion of a locally nilpotent torsion-free group G, if*

$$E \subseteq Z_1 \subseteq Z_2 \subseteq \ldots \subseteq Z_\alpha \subseteq \ldots$$

is the upper central chain of G, and if Z_α^* is the completion of Z_α in G^*, then

$$E \subseteq Z_1^* \subseteq Z_2^* \subseteq \ldots \subseteq Z_\alpha^* \subseteq \ldots$$

is the upper central chain of G^*.

For some power of an element z_1^* of Z_1^* lies in Z_1; some power of an element g^* of G^* lies in G. These powers are permutable; but as we have proved in the preceding section, this implies that z_1^* and g^* are themselves permutable, and therefore Z_1^* is contained in the center of G^*. On the other hand, if x is an arbitrary element of the center of G^*, then some power of x lies in G, and therefore in Z_1, and then x is contained in Z_1^*. This proves that Z_1^* is the center of G^*.

Suppose we have already proved for all α less than β that Z_α^* is the α-th term of the upper central chain of G^*. Suppose that $\beta - 1$ exists. Since $Z_{\beta-1}$ is isolated in G, we have

$$Z_{\beta-1}^* \cap G = Z_{\beta-1}. \tag{23}$$

as a consequence of the one-to-one correspondence, established above, between the isolated subgroups of G and the complete subgroups of G^*.

The factor group $G^*/Z^*_{\beta-1}$ is the completion of its subgroup $GZ^*_{\beta-1}/Z^*_{\beta-1}$, and $Z^*_\beta/Z^*_{\beta-1}$ is the completion of $Z_\beta Z^*_{\beta-1}/Z^*_{\beta-1}$. For if

$$(g^* Z^*_{\beta-1})^k = z_\beta Z^*_{\beta-1}, \quad g^* \in G^*, \quad z_\beta \in Z_\beta,$$

then

$$g^{*k} \in z_\beta Z^*_{\beta-1} \subset Z^*_\beta,$$

and since Z^*_β is complete, g^* is also contained in Z^*_β. Moreover, $Z_\beta Z^*_{\beta-1}/Z^*_{\beta-1}$ is the center of $GZ^*_{\beta-1}/Z^*_{\beta-1}$: if an element g_0 of G is such that for an arbitrary element of G

$$[g_0 Z^*_{\beta-1}, \quad g Z^*_{\beta-1}] = Z^*_{\beta-1},$$

then by (23),

$$[g_0, g] \in (Z^*_{\beta-1} \cap G) = Z_{\beta-1},$$

and therefore g_0 is contained in Z_β. We now find ourselves in exactly the situation in which the beginning of the proof of the theorem was conducted; we can therefore assume as proved that $Z^*_\beta/Z^*_{\beta-1}$ is the center of $G^*/Z^*_{\beta-1}$. It follows that Z^*_β is the β-th term of the upper central chain of G^*.

If β is a limit number, then Z_β is the union of all Z_α, $\alpha < \beta$. Some power of every element x of Z^*_β lies in Z_β and therefore in some Z_α, $\alpha < \beta$; but then x itself lies in Z^*_α. Thus Z^*_β is the union of the subgroups Z^*_α, $\alpha < \beta$, and is therefore the β-th term of the upper central chain of G^*.

This theorem implies that *the completion of a torsion-free ZA-group is a ZA-group, and the completion of a nilpotent torsion-free group of class k is a nilpotent group of the same class.*

In conclusion, we mention a theorem proved by Gluškov [4] which generalizes the well-known property of complete subgroups of an abelian group: *In a locally nilpotent torsion-free group the product of an arbitrary set of complete subgroups is a complete subgroup.*

APPENDIXES

APPENDIXES

Appendix A (*page* 11)

In the definition of a free product $G = \prod_{\alpha}^{*} G_\alpha$ it is sometimes postulated (for example, in the Russian text) that no factor G_α shall be the trivial subgroup E. If this definition is adopted, then a number of theorems require careful wording. To give but one example: Kuroš's Subgroup Theorem (p. 17) states that every subgroup H of G can be expressed as a free product of a free group F and of groups conjugate to subgroups of the factors G_α

$$H = F * \prod_{\alpha}^{*} g_\alpha^{-1} H_\alpha g_\alpha, \quad \text{with } H_\alpha \subseteq G_\alpha.$$

Now several of these free factors may be trivial groups and would have to be suppressed. The above statement of the theorem would then not be strictly correct and is not easily put into a correct form, because F or some or all of the factors $g_\alpha^{-1} H_\alpha g_\alpha$ may be trivial; or only a single factor (which is then not a free product) may remain. The circumlocution here and in similar situations is avoided by the wider definition given in the text. On the other hand, the term "indecomposable" group is, of course, to be understood as "only trivially decomposable," that is, if $G = H * K$, then H or K is the trivial subgroup E.

Appendix B (*page* 17)

The free product of two cyclic groups of order 2

$$G = \{b\} * \{c\}, \quad b^2 = c^2 = 1$$

is also known as the *infinite dihedral group*. If we put $bc = a$, then we have $c = ba$ and $G = D_\infty = \{a, b\}$ with the defining relations $b^2 = 1$, $bab = a^{-1}$. The name is chosen by analogy with the finite dihedral group $D_n = \{a, b\}$ with the same defining relations as above and in addition $a^n = 1$. The latter group is of order $2n$ and is the group of space symmetries of a plane regular polygon of n sides.

It is mentioned in the text that the modular group of linear substitutions

$$w: \quad \frac{a z + b}{c z + d}$$

with integer coefficients a, b, c, d and with $ad - bc = 1$ is the free product of a cyclic group of order 2 and a cyclic group of order 3. A geometric proof can be found in Klein-Fricke, *Theorie der elliptischen Modulfunktionen*, vol. 1 (1890), pp. 218-219, 452-455.

Here is a short algebraic proof. The composition of linear substitutions is easily seen to follow the law of matrix multiplication. We have, therefore, a homomorphism of the group of unimodular matrices

$$m = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

with integer coefficients and determinant $ad - bc = 1$ onto the group of linear substitutions. The kernel of this homomorphism is the center of the group, consisting of the two matrices

$$\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

(because a change of sign in the coefficients does not change the linear substitution). We take the factor group of this kernel, in other words, we agree to identify two matrices that differ only in the sign of their four coefficients. We have then an isomorphism between this factor group M and the group of substitutions above.

Now let

$$s = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

then

$$s^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$$

for any integer k, and s is an element of infinite order. Let

$$t = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

then

$$t^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

We show first of all that s and t generate the group, $M = \{s, t\}$. If $c = 0$, then $ad = 1$ gives $a = d = \pm 1$, and we can assume that the upper sign holds. The matrix is now

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = s^b.$$

If $c \neq 0$, then

$$tm = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix} \text{ and } s^k m = \begin{pmatrix} a + kc & b + kd \\ c & d \end{pmatrix}.$$

We can assume that

(i) $c > 0$, changing signs if necessary, and

(ii) $c \leqq |a|$.

If this condition is not satisfied in m, we go over to tm, where (ii) is satisfied. Now we divide a by c, $a = qc + a'$, $0 \leqq a' < c$, and obtain

$$s^{-q} m = \begin{pmatrix} a - qc & b - qd \\ c & d \end{pmatrix} = \begin{pmatrix} a' & b' \\ c & d \end{pmatrix}.$$

We again multiply on the left by t and continue the division process. Since $|a| \geqq c > a' > \ldots$, after a finite number of steps we reach a matrix m' with 0 in the upper left corner, so that tm' is a power of s. Hence we see that $m = t^{\alpha} s^{q} t s^{q'} \ldots t s^{q^{(r)}}$, with $\alpha = 0$ or 1. We put

$$u = ts = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix};$$

then

$$u^3 = 1, \; tu = s, \text{ and } tu^{-1} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = s'.$$

When we replace all the powers of s occurring in the above representation by tu, we arrive at

$$m = t^{\alpha} u^{\pm 1} t u^{\pm 1} \ldots t u^{\pm 1} t^{\beta}, \tag{1}$$

with α and $\beta = 0$ or 1. This shows that the group M can be generated by an element of order 2 and one of order 3, $M = \{t, u\}$.

We now have to show the uniqueness of the representation (1). If there were a matrix with two distinct representations, we would obtain a relation of the form $t^{\gamma}u^{\pm 1}tu^{\pm 1} \ldots tu^{\pm 1}t^{\delta} = 1$. We can, in fact, assume that $\gamma = 1$, $\delta = 0$. For if $\gamma = 0$, $\delta = +1$, then transformation by t leads to the required form. But if γ and δ are both 1 or both 0, then a sequence of transformations by t, $u^{\pm 1}$, etc. will lead to a shorter relation of the same form. We now group together the adjacent terms tu and tu^{-1} with equal exponents and use $tu = s$, $tu^{-1} = s'$. We obtain a relation $s^k s'^{k'} s^l s'^{l'} \ldots s^r s'^{r'} = 1$, where all the exponents are non-negative. But

$$s^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}, \quad s'^{k'} = \begin{pmatrix} 1 & 0 \\ k' & 1 \end{pmatrix}, \quad s^k s'^{k'} = \begin{pmatrix} 1 + kk' & k \\ k' & 1 \end{pmatrix}$$

and it is obvious that a product of such matrices can never yield the unit matrix unless $k = k' = l = l' = \ldots = r = r' = 0$. This completes the proof.

Appendix C (*page* 17)

Six proofs of Kuroš's Subgroup Theorem are now available. The proof by Baer and Levi [2] is of a topological nature. The text of the book reproduces the author's original proof [3]. The rather complicated double transfinite induction was simplified in the more recent proofs by Takahasi [1] and M. Hall [5]. Takahasi also obtains an explicit formula

$$r = j(n - 1) + 1 - \sum_{a} d_a$$

for the rank r of the free factor F in terms of the index j of H under G, the number n of factors G_a and the number d_a of double cosets of G modulo (H, G_a); in the case of a free group this formula turns into Schreier's result (see p. 36) on the rank of a subgroup of finite index in a free group of finite rank. M. Hall [5], following the proof of the Nielsen-Schreier Theorem by Levi [2], replaces the transfinite induction by a well-ordering argument based on an alphabetical ordering of the group elements. His proof is very short, but does not yield quite as much. A common feature of these proofs is the use of cancellation arguments, which are necessary to show that certain subgroups, or products, or generators are free. A new method was intro-

duced in the paper by Kuhn [1] where the structure of the subgroup H of G is obtained from its presentation by generators and relations. The most recent paper by Weir [1] contains very lucid proofs, without any cancellation arguments, of the whole group of theorems (the Kuroš Subgroup Theorem, the Nielsen-Schreier Theorem, the Reidemeister-Schreier method of obtaining generators and relations for a subgroup of a free group, and the Schreier formula for the rank of a subgroup of finite index in a free group of finite rank). See also the paper by Fox [4].

Appendix D (*page* 37)

Takahasi [6] has proved that if G is a free group and

$$H_1 \supseteq H_2 \supseteq \ldots$$

is an arbitrary descending sequence of subgroups whose intersection H is not the trivial group, then H has a non-trivial subgroup K which is a common free factor of all but a finite number of the groups H_i. This theorem allows us to strengthen Theorem III by replacing the reference to length 3 in it by *length* 2. It also yields a simple proof of Magnus' Theorem (p. 38). See also Iwasawa [2].

Appendix E (*page* 38)

Note that if R has a unit element 1, then $1-(a \circ b)=(1-a)(1-b)$. The radical elements are then precisely the elements of R of the form $1-a$, where a is a unit in R. The composition $a \circ b$ was introduced by S. Perlis (Bull. Amer. Math. Soc., vol. 48 (1942), pp. 128-132) in an investigation of the radical of an associative algebra.

Appendix F (*page* 50)

To complete the argument of the text it is necessary to show that the set of all countable groups has the cardinal number of the continuum. All countable groups are factor groups of the free group of countable rank and the cardinal number of the set of factor groups of this group clearly does not exceed that of the continuum. On the other hand, the survey of the subgroups of the additive group of rational numbers (see vol. I, § 30, pp. 207-210) shows that these groups alone form a set with the cardinal number of the continuum.

Appendix G (*page* 56)

The example of Higman [3] arises from the group $G = \{a, b, c, d\}$ with the defining relations

$$b^{-1}ab = a^2,$$
$$c^{-1}bc = b^2,$$
$$d^{-1}cd = c^2,$$
$$a^{-1}da = d^2.$$

It is easily seen to be infinite. Now G is either simple or it has normal subgroups. In the latter case let N be a maximal normal subgroup. (Finitely generated groups always have maximal normal subgroups — see B. H. Neumann [5].) The factor group G/N is then simple, but cannot be finite, because the above relations are not compatible with finite orders for $a, b, c,$ and d. Hence G/N is an infinite simple group.

In contrast to Higman's existence proof, Ruth Camm [1] has actually constructed an uncountable number of non-isomorphic infinite simple groups with two generators. Her examples are all free products of two free groups with an amalgamated subgroup.

Other examples of infinite simple groups, apart from the alternating groups on an arbitrary set of symbols, are the locally infinite groups in which all the elements other than the unit element form a single conjugacy class. The existence of such groups was demonstrated by Higman, B. H. Neumann and H. Neumann [1] (see p. 157).

Further examples of infinite simple groups are contained in papers by Chehata [1], Clowes and Hirsch [1], Higman [7].

Appendix H (*page* 56)

The Burnside Problem for the exponent 5 has recently been solved affirmatively by Kostrikin [1] for the case of two generators, and independently by G. Higman [10] for the general case of a finite number of generators. Kostrikin also shows that the order of the group $B_{2,5}$ is 5^{33} or 5^{34} and that its class of nilpotency (see p. 214) is 11 or 12.

Some other recent papers dealing with the Burnside Problem are Green [1], Hall and Higman [1], Lyndon [6, 7], Magnus [13], Meier-Wunderli [1], Sanov [3-6].

Appendix I (*page* 76)

The insolvability of the word problem for groups was first announced, without proofs, in the brief note by Novikov [1]. The full proofs of the theorems announced in [1] are contained in the paper by Novikov [3] which fills 144 pages and has only recently become available for scrutiny. The insolvability of the word problem implies that of the conjugacy problem. For if the conjugacy problem could be solved, then it could be decided algorithmically whether a given word w in a group G is conjugate to 1, that is, is equal to 1. But this would solve the word problem in G. The paper by Novikov [2] contains an independent simplified proof of the insolvability of the conjugacy problem.

For other work on the negative side of the word problem see the papers by Turing [2] and Boone [1-3].

Appendix J (*page* 76)

The "sieve" method of Tartakovskiĭ [1-6] solves the word problem for finitely presented groups in which there is, roughly speaking, very little interdependence and superposition between the defining relations. A detailed account of his work is contained in the review by K. A. Hirsch, Mathematical Reviews, vol. 11 (1950), pp. 493-495. Tartakovskiĭ's results have been extended by Stender [1] to groups with a countable number of generators and defining relations, provided each generator occurs in only a finite number of relations and the lengths of the relations are uniformly bounded.

An independent general approach to the word problem in groups is contained in the thesis by Britton [1]. The range of applicability of his results overlaps those of Tartakovskiĭ and Stender to a large extent, but goes much further in some directions, particularly in groups with an infinite number of generators and defining relations.

For other work on the positive side of the word problem see Haken [1], Peiffer [1].

Appendix K (*page* 89)

A more detailed study of groups with isomorphic subgroup lattices can be found in § 52 of the First (Russian) Edition of this book. See also Birkhoff [5], Chapter VI, 9/10, where further references are listed.

Appendix L

(*page* 93)

The structure of finite and infinite groups with a modular subgroup lattice has been completely determined by Iwasawa [1, 3]. They are direct products of hamiltonian groups (see vol. I, p. 67) and of two special types of finite solvable groups. Further references on the problem of groups with a modular (or some generalization of a modular) subgroup lattice are M. Hall [Birkhoff [5], p. 97, footnote 20], Zacher [3-5], Itô [6].

Appendix M

(*page* 120)

Important contributions to the theory of direct decompositions of a group are contained in a paper by Kulikov [3] (which is also available in an English translation, Amer. Math. Soc. Transl. Project, vol. 2, 1955). Although some elementary topological concepts and methods are used which are not elsewhere dealt with in this book, we shall briefly describe his main results.

Let

$$(D) \qquad G = \sum_{\alpha} D_\alpha, \ \alpha \in A$$

be a direct decomposition of a group not necessarily abelian. Let Ω be a fixed set of endomorphisms of G. The decomposition (D) is made into a topological space as follows. The points of the space are the direct summands D_α; if B is a subset of the index set A, then the subset of points D_β, $\beta \in B$, is called *closed* if the subgroup H generated by it, $H = \sum_{\beta} D_\beta$, $\beta \in B$, is Ω-admissible, that is, if $H\Omega \subseteq H$.

It can happen that the space (D) with this topology satisfies the separation axiom T_0 (Kolmogorov's Axiom): Distinct points have distinct closures. When this occurs, then (D) can be made in a natural way into a partially ordered set $L(D, \Omega)$ by defining that D_α *precedes* D_β if D_α is contained in the closure of D_β.

An endomorphism ω of a group G is called *idempotent* if $\omega^2 = \omega$. An endomorphism ω of a group G is called *normal* if it is permutable with all the inner automorphisms. (An automorphism ω is normal if and only if $g^{-1}g$ is an element of the center of G for all $g \in G$, that is, if the automorphism is *central*.) When Ω is the set of all normal endomorphisms, then the T_0-condition is equivalent to the following: Of two arbitrary summands of (D) neither admits a non-trivial homomorphism into the center of the other.

We can now formulate Kulikov's principal theorem.

Let the direct decomposition of a group G

$$(D) \qquad G = \sum_{a} D_a, \quad a \in A$$

be partially ordered with respect to the set Ω of all normal idempotent endomorphisms of G.

In order that any two direct decompositions of G have centrally isomorphic refinements it is necessary that for every index $a \in A$ any two direct decompositions of D_a have centrally isomorphic refinements. If, in addition, G satisfies at least one of the following two conditions:

(i) G is countable;

(ii) the descending chain condition holds in the partially ordered set

$$L(D, \Omega),$$

then the above condition is also sufficient for the existence of centrally isomorphic refinements of any two direct decompositions of G.

The far-reaching applications of Kulikov's method to the decomposition of abelian groups have been mentioned before (vol. I, p. 216).

Appendix N (*page* 154)

Groups in which all the classes of conjugate elements are finite—or briefly, *FC*-groups—have received much attention in recent years. The relevant papers are Baer [40], B. H. Neumann [11, 15, 19], Haimo [3, 6], Erdös [1].

Appendix O (*page* 157)

Further cases where the minimal or maximal condition for normal subgroups implies the same condition for all subgroups are investigated in papers by P. Hall [12], Čarin [4], McLain [2].

Appendix P (*page* 162)

Consider the free product of two cyclic groups of order 2 or the infinite dihedral group with the defining relations (see Appendix B)

$$D_\infty = \{a, b\}, b^2 = 1, bab = a^{-1}.$$

All the elements of order 2 in D_∞ are of the form $a^\alpha b$. Since $aba^{-1} = a^2 b$, etc., these are easily seen to fall into two conjugate sets: those with even α and those with odd α. The subgroup $H = \{a^2, b\}$ is of index 2 and hence is normal in D_∞. But its intersection with the Sylow 2-subgroup $\{ab\}$ of D_∞ is trivial and is not a Sylow 2-subgroup of H. This shows that the first theorem does not hold. Next, $\{b\}$ is a Sylow 2-subgroup of D_∞ and is its own normalizer in D_∞. Yet the subgroup H above, which contains $\{b\}$ is not its own normalizer but is normal in D_∞. This shows that the second theorem does not hold.

As Kuroš [9] has proved (see p. 164), for arbitrary p-groups P_1 and P_2 the free product $P_1 * P_2$ is a group for which P_1 and P_2 are Sylow p-subgroups. This shows that Sylow p-subgroups of infinite groups, so far from being conjugate, need not even be isomorphic nor of equal order. Another simple example is the following.

Let $G = \{a, b, c, d\}$ with the defining relations $b^2 = 1$, $bab = a^{-1}$, $ac = ca$, $ad = da$, $b^{-1}c^{-1}bc = a$, $bd = db$, $d^2 = 1$, $cdcd = a$. (G is an extension of the infinite dihedral group $\{a, b\}$ by another infinite dihedral group.) A principal series of G is

$$G \supset \{a, b, c\} \supset \{a, b\} \supset \{a\} \supset 1.$$

The four factor groups are cyclic: the first and third of order 2, the second and fourth of infinite order. It follows easily that the order of a Sylow 2-subgroup cannot exceed 4. All the elements of order 2 in G are of the following forms: $a^\alpha b$, $a^\alpha c^{-2\alpha} d$, $a^\alpha b c^\gamma d$. G has no elements of order 4. A simple calculation shows that the elements of the form $a^\alpha c^{-2\alpha} d$ are permutable with every element of the form $a^{\alpha'} b$, and that the element $a^\alpha b c^{2\gamma} d$ is permutable with $a^{\alpha - \gamma} b$ but with no other elements of order 2. Finally, the elements of the form $a^\alpha b c^\gamma d$ with odd γ are not permutable with any other element of order 2. Hence G has Sylow 2-subgroups both of order 2 and of order 4. (See also Zappa [2].)

Appendix Q (*page* 165)

The example of Schmidt [6] of an infinite p-group without center is reproduced in § 30 of the First (Russian) Edition of this book. Infinite p-groups can also coincide with their derived group. This again is in contrast to the case of finite p-groups, which are nilpotent (see p. 216). Such examples have been constructed by Ado [1] and Schmidt [7]. Following Ado's idea, McLain [1] has even given an example of a p-group G that has both center

E and derived group G. In fact, G has no characteristic subgroups except E and G.

Let $R = \{\alpha, \beta, \gamma, \ldots\}$ be the set of all rational numbers, and K a division ring. We form the vector space V over K with the basis elements $e_{\alpha\beta}$, $\alpha < \beta$, and define a multiplication by the rule

$$e_{\alpha\beta}e_{\gamma\delta} = e_{\alpha\delta} \text{ when } \beta = \gamma, \text{ and}$$
$$= 0 \text{ otherwise.}$$

The set of elements $G = \{1 + v\}$ with $v \in V$ then forms a group. If the characteristic of K is a prime number p, then G is a locally finite p-group; if the characteristic of K is 0, then G is locally infinite. (If K is countable, then G is countable.)

Every element $g \in G$ has a unique representation of the form

$$g = 1 + \Sigma a_{\alpha\beta}e_{\alpha\beta},\ a_{\alpha\beta} \in K,$$

where all but a finite number of the coefficients $a_{\alpha\beta}$ are 0. G can be generated by the elements $1 + ae_{\alpha\beta}$, $a \in K$. If N is a proper normal subgroup $\neq E$ of G, then there exist two rational numbers α, β such that for all ξ, η satisfying the condition $\xi < \alpha < \beta < \eta$, N contains the elements $1 + ae_{\xi\eta}$. Every order-preserving mapping of the rationals onto themselves induces an automorphism θ of G as follows: If in the mapping $\alpha \to \alpha'$, $\beta \to \beta'$, then

$$(1 + \Sigma a_{\alpha\beta}e_{\alpha\beta})\theta = 1 + \Sigma a_{\alpha\beta}e_{\alpha'\beta'}.$$

It follows readily that if N is a characteristic subgroup of G and $N \neq E$, then $N = G$.

Appendix R (*page* 166)

Recent results on locally free groups and related topics are contained in the papers by G. Higman [4-6], Specker [1], and Takahasi [3].

Appendix S (*page* 168)

The author's proof is rather condensed and requires, strictly speaking, one further transfinite induction or application of Zorn's Lemma. His argument shows that if the projection set P is not complete, then it is properly contained in another projection set—but the latter need not be complete. When the projection sets containing P are partially ordered by inclusion, then one proves easily that the union of a transfinite ascending chain of such sets is

itself a projection set containing P. Hence, by Zorn's Lemma, there exists at least one maximal projection set containing P, and by what the author has shown, every such maximal projection set is complete.

The theorem is a special case of a theorem by Steenrod (*Universal homology groups,* Amer. J. Math., vol. 58 (1936), pp. 661-701; Theorem 2. 1. See also Lefschetz, *Algebraic Topology,* New York 1942, p. 42). This states that the inverse (or "projective") limit of a system of non-empty compact sets is non-empty. If the topology is taken as discrete, then "compact" is the same as "finite," the projections are obviously continuous, and we obtain the author's theorem. A careful analysis of a similar embedding situation is contained in a paper by B. H. Neumann [16]; see also Robinson [1].

Appendix T (*page* 194)

Important new results on solvable groups subject to various finiteness conditions are contained in the paper by P. Hall [12]. He shows by examples that finitely generated solvable groups need not even satisfy the maximal condition for normal subgroups (whereas a finitely generated nilpotent group satisfies the maximal condition for subgroups; see p. 232). He also proves that the set of non-isomorphic finitely generated groups satisfying the condition $G'' = E$ ("metabelian" groups) is countable. In contrast to this stands his main result: that the set of non-isomorphic finitely generated groups satisfying the condition $[G'', G] = E$ is not countable. In fact, the condition $[G'', G] = E$ is equivalent to the conditions that the second derived group G'' is contained in the center Z of G and that the factor group G/Z of the center is metabelian. Hall shows that the center Z can be chosen arbitrarily as a non-trivial countable abelian group, and for every such choice of Z the set of non-isomorphic two generator groups G satisfying the above condition is not countable.

Two main results of the paper by Mal'cev [10] (which is also available in English translation: Amer. Math. Soc. Transl. Project, vol. 2 (1955)) are that in a solvable group the maximal condition for subgroups is a consequence of the maximal condition for abelian subgroups, and that every solvable group of unimodular matrices with integer coefficients satisfies the maximal condition for subgroups. Extending the latter result Smirnov [3] has shown that every solvable group of automorphisms of a solvable group with maximal condition for subgroups also satisfies the maximal condition for subgroups. Alternative proofs of the theorems of Mal'cev and Smirnov are contained in the paper by Baer [62]; see also the much earlier paper by Zassenhaus [3].

Appendix U (*page* 201)

An important supplement to § 60 of this book is the long paper by P. Hall [13]. It gives a systematic account of all the known results and many new results on the Π-structure (existence, conjugacy, containedness) of finite groups subject to varying restrictions, where Π is a set of prime numbers. See also Wielandt [5], Zappa [13].

Appendix V (*page* 210)

After a long period of stagnation, the theory of finite simple groups is beginning to receive attention again. Until recently the only known finite groups were

(i) the alternating groups A_n, $n \geqq 5$, and five "exceptional" multiply transitive permutation groups discovered by Mathieu;

(ii) the "classical" simple groups (special projective, unitary, symplectic, orthogonal) associated with a finite field $GF(p^a)$.

P. Hall has proved the following result (unpublished). Let l be any prime number dividing the order of G, a simple group of the above list; $v_l(G)$ the order of a Sylow l-subgroup of G, and $w_l(G)$ the number of elements of G whose order is a power of l. Then for all the groups of type (i) above and, except for a few that are isomorphic to groups of type (ii), provided l is not the characteristic of the field, for those of type (ii),

$$w_l(G) > [v_l(G)]^2.$$

But for $l = p$ and the groups of type (ii),

$$w_p(G) = [v_p(G)]^2.$$

This result suggests the conjecture that for simple groups of finite composite order $w_l(G) \geqq [v_l(G)]^2$. It would include as a special case Burnside's Theorem (see p. 194) on the solvability of groups of order $p^a q^\beta$.

New simple groups have been discovered by Chevalley [1]. His paper gives a uniform procedure of associating with every simple complex Lie group a finite simple group. He determines the orders of these finite analogues to the "exceptional" Lie groups of types G_2, F_4, E_6, E_7, E_8 (the first-named had previously been treated by Dickson: Math. Ann., vol. 60 (1905), pp. 137-150) and investigates the structure of their Sylow subgroups.

Appendix W (*page* 215)

In the First (Russian) Edition of this book Kuroš raised the problem whether there exist algebraic operations in the set of all groups, similar to the formation of the direct product and the free product (§ 17 and § 33), with the following properties:

(i) The operation assigns to an arbitrary collection of groups A_α a group G which contains isomorphic images G_α of the groups A_α and is generated by them, $G = \{G_\alpha\}$;

(ii) if $H_\alpha = \{G_\beta\}$, $\beta \neq \alpha$, and $\overline{H}_\alpha$ the least normal subgroup of G containing H_α, then the intersection $G_\alpha \cap \overline{H}_\alpha = E$ for all α;

(iii) the operation satisfies the most general associative and commutative laws as they are expressed in properties I and II of § 17 and § 33.

Golovin [2-5] has constructed a countable sequence of operations satisfying these requirements. (The papers [3-5] are also available in English translation: Amer. Math. Soc. Trans. Project, vol. 2 (1955).) These are the k-th nilpotent products mentioned in the text. Further examples were found by Miss R. R. Struik [1]. All these are special cases of a very general construction: the formation of the *verbal product* of a given set of groups, which is described and studied in a paper by Moran [1].

Let x_α, x_α^{-1} be the letters of an alphabet and

$$w = x_{\alpha_1}^{\varepsilon_1} x_{\alpha_2}^{\varepsilon_2} \dots x_{\alpha_n}^{\varepsilon_n} \quad (\varepsilon_i = \pm 1, \quad i = 1, 2, \dots, n)$$

be a word in this alphabet. When arbitrary elements of a group G are substituted for the letters $x_{\alpha_1}^{\varepsilon_1}$ (the same group element when the indices represent the same letter), then we obtain a *value* of the word w in G. The group generated by all possible values of w in G is called the *verbal subgroup* $V(G)$ *associated with the word* w (see B. H. Neumann [4]). $V(G)$ is a fully invariant subgroup of G, and if G is a free group, the converse holds (Levi [3]). However, in the general case, a group may have fully invariant subgroups that are not verbal: for example, the group generated by all the elements of finite order in a group G is fully invariant but need not be verbal. Familiar examples of verbal subgroups of a group G are the terms of the derived chain and of the lower central chain (§ 14), the group generated by the k-th powers of all the elements of G, and so on.

Now let G_α be a given set of groups; $F = \prod_\alpha {}^* G_\alpha$, their free product; $C(F) = [G_\alpha]_F$, the least normal subgroup of F generated by all the commutators of the form $[g_\alpha, g_\beta]$, $\alpha \neq \beta$, $g_\alpha \in G_\alpha$, $g_\beta \in G_\beta$; $V(F)$, an arbitrary verbal

subgroup of F. Then Moran proves that the *verbal product*

$$\prod_a^v G_a = F/(V(F) \cap C(F))$$

satisfies all the requirements (i)—(iii) above.

The examples of Golovin and Miss Struik arise from special choices of the verbal subgroups $V(F)$.

It is known (S. Moran, unpublished) that there exist operations which satisfy the requirements (i)—(iii) but are not verbal products.

Appendix X (*page* 218)

The Φ-subgroup both of finite and infinite groups has received much attention in recent years. Some of the relevant papers are Baer [52, 55], Gaschütz [2], D. G. Higman [3], G. Higman and B. H. Neumann [1], Hirsch [9], Huppert [3], Itô [7], Zacher [1].

Appendix Y (*page* 226)

Another class of generalized nilpotent groups is formed by the groups G in which for any two elements g, h a commutator identity

$$[g, h, h, \ldots, h] = 1$$

holds, where the number of repetitions of h may depend on g and h. They have been studied, under the name of *Engel groups,* by Gruenberg [2] and, under the name of *nilgroups,* by Plotkin [5]. See also the papers by Baer [60], Hirsch [10], Plotkin [7, 8], and Schenkman [1].

BIBLIOGRAPHY

BIBLIOGRAPHY

This Bibliography lists the group-theoretical papers of recent years that have a bearing on the material covered by the text of both volumes; together with those entries in the Bibliography of Vol. I that are marked by a dagger (†), it constitutes a supplement to the Bibliography of the second Russian edition. The numbering of the entries is consecutive with that of Vol. I.

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.

ASANO, K.

[1] *Bemerkungen über die Erweiterungstheorie von Gruppen,* J. Inst. Polytech. Osaka City Univ. Ser. A., vol. 5 (1954), pp. 75—80.

AYOUB, C. W.

[1] *A theory of normal chains,* Canadian J. Math., vol. 4 (1952), pp. 62—188.

[2] *On the primary subgroups of a group,* Trans. Amer. Math. Soc., vol. 72 (1952), pp. 450—466.

AZUMAYA, G.

[1] *On generalized semi-primary rings and Krull-Remak-Schmidt's theorem,* Japan. J. Math., vol. 19 (1948), pp. 525—547.

BAER, R.

[46] *Klassifikation der Gruppenerweiterungen,* J. reine angew. Math., vol. 187 (1949), pp. 75—94.

[47] *Free mobility and orthogonality,* Trans. Amer. Math. Soc., vol. 68 (1950), pp. 439—460.

[48] *Ein Einbettungssatz für Gruppenerweiterungen,* Arch. Math., vol. 2 (1950), pp. 178—185.

[49] *Endlichkeitskriterien für Kommutatorgruppen,* Math. Ann., vol. 124 (1952), pp. 161—177.

[50] *Factorization of n-soluble and n-nilpotent groups,* Proc. Amer. Math. Soc., vol. 4 (1953), pp. 15—26.

[51] *Group elements of prime power index,* Trans. Amer. Math. Soc., vol. 75 (1953), pp. 20—47.

[52] *Nilpotent characteristic subgroups of finite groups,* Amer. J. Math., vol. 75 (1953), pp. 633—644.

[53] *The hypercenter of a group,* Acta Math., vol. 89 (1953), pp. 165—208.

[54] *Das Hyperzentrum einer Gruppe. II,* Arch. Math., vol. 4 (1953), pp. 86—96.

[55] *Das Hyperzentrum einer Gruppe. III,* Math. Zeit., vol. 59 (1953), pp. 299—338.

[56] *Das Hyperzentrum einer Gruppe. IV,* Arch. Math., vol. 5 (1954), pp. 56—59.

[57] *Direkte Faktoren endlicher Gruppen,* J. reine angew. Math., vol. 192 (1953), pp. 167—179.

[58] *Supersoluble groups,* Proc. Amer. Math. Soc., vol. 6 (1955), pp. 16—32.

[59] *Finite extensions of abelian groups with minimum condition,* Trans. Amer. Math. Soc., vol. 79 (1955), pp. 521—540.

[60] *Über Nil-Gruppen,* Math. Zeit., vol. 62 (1955), pp. 402—437.

[61] *Burnsidesche Eigenschaften,* Arch. d. Math., vol. 6 (1955), pp. 165—169.

[62] *Auflösbare Gruppen mit Maximalbedingung,* Math. Ann., vol. 129 (1955), pp. 139—173.

BAEVA, N. V.

*[1] *Completely factorizable groups,* Doklady Akad. Nauk SSSR (N.S.), vol. 92 (1953), pp. 877—880.

BEAUMONT, R. A. and ZUCKERMANN, H. S.

[1] *A characterization of the subgroups of the additive rationals,* Pacific J. Math., vol. 1 (1951), pp. 169—177.

BEST, E. and TAUSSKY, O.

[1] *A class of groups,* Proc. Roy. Irish Acad. A, vol. 47 (1942), pp. 55—62.

BOONE, W. W.

[1] *Certain simple unsolvable problems of group theory. I,* Nederl. Akad. Wetensch. Indag. Math., vol. 6 (1954), pp. 231—237.

[2] *Certain simple unsolvable problems of group theory. II,* Nederl. Akad. Wetensch. Indag. Math., vol. 16 (1954), pp. 492—497.

[3] *Certain simple unsolvable problems of group theory. III,* Nederl. Akad. Wetensch. Indag. Math., vol. 17 (1955), pp. 252—256.

BOREVIČ, Z. I.

*[1] *On homology groups connected with a free group,* Izvestiya Akad. Nauk SSSR. Ser. Math., vol. 16 (1952), pp. 365—384.

*[2] *On an Abelian group with operators,* Doklady Akad. Nauk SSSR (N.S.), vol. 91 (1953), pp. 193—195.

BRITTON, J. L.

[1] *Solution of the word problem for certain types of groups,* Thesis, University of Manchester, 1953; to appear in Proc. Glasgow Math. Assoc., vol. 3 (1956).

CAMM, R.

[1] *Simple free products,* J. London Math. Soc., vol. 28 (1953), pp. 66—76.

ČARIN, V. S.

*[4] *On the minimal condition for normal subgroups of locally solvable groups,* Mat. Sbornik N.S., vol. 33 (1953), pp. 27—36.

*[5] *On groups of automorphisms of certain classes of solvable groups,* Ukrain. Mat. Ž., vol. 5 (1953), pp. 363—369.

*[6] *On the groups of automorphisms of nilpotent groups,* Ukrain. Mat. Ž., vol. 6 (1954), pp. 295—304.

CASADIO, G.

[1] *Costruzione di gruppi come prodotto di sottogruppi permutabili,* Rend. Mat. sue Appl. Univ. Roma Ist. Naz. Alta Mat. (5), vol. 2 (1941), pp. 348—360.

ČERNIKOV, S. N.

*[22] *Groups with systems of complemented subgroups,* Doklady Akad. Nauk SSSR (N.S.), vol. 92 (1953), pp. 891—894.

*[23] *Groups with systems of complemented subgroups,* Mat. Sbornik N.S., vol. 35 (1954), pp. 93—128.

*[24] *On the complementation of the Sylow Π-subgroups in some classes of infinite groups,* Doklady Akad. Nauk SSSR (N.S.), vol. 102 (1955), pp. 457—459.

CHARLES, B.

[1] *Le centre de l'anneau des endomorphisms d'un groupe abelien primaire,* C.R. Acad. Sci. Paris, vol. 236 (1953), pp. 1122—1123.

CHEHATA, C. G.

[1] *An algebraically simple ordered group,* Proc. London Math. Soc. (3), vol. 2 (1952), pp. 183—197.

[2] *Commutative extension of partial automorphisms of groups,* Proc. Glasgow Math. Assoc., vol. 1 (1953), pp. 170—181.

[3] *Simultaneous extension of partial endomorphisms of groups,* Proc. Glasgow Math. Assoc., vol. 2 (1954), pp. 37—46.

CHEN, K. T.

[1] *Integration in free groups,* Ann. Math. (2), vol. 54 (1951), pp. 147—162.

[2] *Commutator calculus and link invariants,* Proc. Amer. Math. Soc., vol. 3 (1952), pp. 44—55.

[3] *A group ring method for finitely generated groups,* Trans. Amer. Math. Soc., vol. 76 (1954), pp. 275—287.

CHEVALLEY, C.

[1] *On some simple groups,* Tohoku Math. J. (2), vol. 1 (1955).

CLOWES, J. S.

[1] *On groups of odd order,* J. London Math. Soc., vol. 27 (1952), pp. 507—510.

CLOWES, J. S. and HIRSCH, K. A.

[1] *Simple groups of infinite matrices,* Math. Zeit., vol. 58 (1953), pp. 1—3.

COHN, P. M.

[1] *Generalization of a theorem of Magnus,* Proc. London Math. Soc. (3), vol. 2 (1952), pp. 297—310.

[2] *A countably generated group which cannot be covered by finite permutable subsets,* J. London Math. Soc., vol. 29 (1954), pp. 248—249.

ČUNIHIN, S. A.

*[11] *On weakening the conditions in theorems of Sylow's type,* Doklady Akad. Nauk SSSR (N.S.), vol. 83 (1952), pp. 663—665.

*[12] *On subgroups of a finite group,* Doklady Akad. Nauk SSSR (N.S.), vol. 86 (1952), pp. 27—30.

*[13] *On the embedding and number of subgroups of* Π*-separable groups,* Doklady Akad. Nauk SSSR (N.S.), vol. 91 (1953), pp. 461—462.

*[14] *On existence and conjugacy of subgroups of a finite group,* Mat. Sbornik N.S., vol. 33 (1953), pp. 111—132.

*[15] *On the decomposition of* Π*-separable groups into a product of subgroups,* Doklady Akad. Nauk SSSR (N.S.), vol. 95 (1954), pp. 725—727.

*[16] *On factorization of finite groups,* Doklady Akad. Nauk SSSR (N.S.), vol. 97 (1954), pp. 977—980.

DIETZMANN, A. P.

*[8] *On criteria for non-simplicity of groups,* Doklady Akad. Nauk SSSR (N.S.), vol. 44 (1944), pp. 89—91.

DOUGLAS, J.

[1] *On finite groups with two independent generators,* Proc. Nat. Acad. Sci. U.S.A., vol. 37 (1951), pp. 604—610, 677—691, 749—760, 808—813.

DYUBYUK, P. E.

*[2] *On the automorphisms of p-groups,* Mat. Sbornik N.S., vol. 18 (1946), pp. 281—298.

*[3] *On the number of subgroups of an abelian p-group,* Isv. Akad. Nauk SSSR. Ser. Mat., vol. 12 (1948), pp. 351—378.

*[4] *On the number of subgroups of given index of a finite p-group,* Mat. Sbornik N.S., vol. 27 (1950), pp. 129—138.

*[5] *On the number of subgroups of certain categories of finite p-groups,* Mat. Sbornik N.S., vol. 30 (1952), pp. 575—580.

EASTERFIELD, T. E.

[1] *The orders of products and commutators in prime-power groups,* Proc. Cambridge Philos. Soc., vol. 36 (1940), pp. 14—26.

ECKMANN, B.

[2] *Cohomology of groups and transfer,* Ann. of Math. (2), vol. 58 (1953), pp. 481—493.

EDEL'MAN, S. L.

*[1] *On the p-normal series of a group,* Doklady Akad. Nauk SSSR. (N.S.), vol. 79 (1951), pp. 209—212.

EILENBERG, S.

[1] *Topological methods in abstract algebra. Cohomology theory of groups,* Bull. Amer. Math. Soc., vol. 55 (1949), 3—37.

ERDÖS, J.

[1] *The theory of groups with finite classes of conjugate elements,* Acta Math. Acad. Sci. Hungar., vol. 5 (1954), pp. 45—58.

[2] *On direct decompositions of torsion-free abelian groups,* Publ. Math. Debrecen, vol. 3 (1954), pp. 281—288.

FADDEEV, D. K.

*[3] *On a theorem in the theory of homology groups,* Doklady Akad. Nauk SSSR (N.S.), vol. 92 (1953), pp. 703—705.

FOX, R. H.

[1] *On Fenchel's conjecture about F-groups,* Mat. Tidskr. B (1952), pp. 61—65.

[2] *Free differential calculus: I. Derivation in the free group ring,* Ann. of Math. (2), vol. 57 (1953), pp. 547—560.

[3] *Free differential calculus: II. The isomorphism problem of groups,* Ann. of Math. (2), vol. 59 (1954), pp. 196—210.

[4] *Free differential calculus: III.* Ann. of Math. (2),

FUCHS, L.

[1] *The direct sum of cyclic groups,* Acta Math. Acad. Sci. Hungar., vol. 3 (1952), pp. 177—195.

[2] *Über die Zerlegung einer Gruppe nach zwei Untergruppen,* Monatsh. Math., vol. 57 (1953), pp. 109—112.

[3] *On abelian groups in which the classes of isomorphic proper subgroups contain the same number of subgroups,* Čehoslovack. Mat. Ž. (2), vol. 77 (1953), pp. 387—390.

[4] *On the structure of abelian p-groups,* Acta Math. Acad. Sci. Hungar., vol. 4 (1953), pp. 267—288.

[5] *On a special kind of duality in group theory. II,* Acta Math. Acad. Sci. Hungar., vol. 4 (1953), pp. 299—314.

[6] *On a property of basic subgroups,* Acta Math. Acad. Sci. Hungar., vol. 5 (1954), pp. 143—144.

FUCHS, L., KERTÉSZ, A. and SZELE, T.

[1] *On a special kind of duality in group theory. I,* Acta Math. Acad. Sci. Hungar., vol. 4 (1953), pp. 169—178.

[2] *Abelian groups in which every serving subgroup is a direct summand,* Publ. Math. Debrecen, vol. 3 (1949), pp. 95—105.

GACSÁLYI, S.

[1] *On algebraically closed abelian groups,* Publ. Math. Debrecen, vol. 2 (1952), pp. 292—296.

[2] *On pure subgroups and direct summands of abelian groups,* Publ. Math. Debrecen, vol. 4 (1955), pp. 89—92.

GASCHÜTZ, W.

[1] *Zur Erweiterungstheorie der endlichen Gruppen,* J. reine angew. Math., vol. 190 (1952), pp. 93—107.

[2] *Über die Φ-Untergruppen endlicher Gruppen,* Math. Zeit., vol. 58 (1953), pp. 160—170.

[3] *Gruppen deren sämtliche Untergruppen Zentralisatoren sind,* Arch. Math., vol. 6 (1954), pp. 5—8.

GLUŠKOV, V. M.

*[5] *On the central series of infinite groups,* Mat. Sbornik N.S., vol. 31 (1952), pp. 491—496.

GOL'BERG, P. A.

*[4] *Sylow bases of infinite groups,* Mat. Sbornik N.S , vol. 32 (1953), pp. 465—476.

*[5] *On a condition for conjugacy of Sylow Π-bases of an arbitrary group,* Mat. Sbornik N.S., vol. 36 (1955), pp. 335—340.

GONCALVES, J. V.

[1] *On groups having a set of p-Sylow subgroups,* Univ. Lisboa. Revista Fac. Ci. A. Ci. Mat. (2), vol. 2 (1952), pp. 161—168.

GORČINSKIĬ, YU. N.

*[1] *Groups with a finite number of classes of conjugate elements,* Mat. Sbornik N.S., vol. 31 (1952), pp. 167—182.

*[2] *Periodic groups with a finite number of classes of conjugate elements,* Mat. Sbornik N.S., vol. 31 (1952), pp. 209—216.

GREEN, J. A.

[1] *On groups with odd prime-power exponent,* J. London Math. Soc., vol. 27 (1952), pp. 467—485.

GRIFFITHS, H. B.

[1] *A note on commutators in free products,* Proc. Cambridge Phil. Soc., vol. 50 (1954), pp. 178—188.

[2] *A note on commutators in free products II,* Proc. Cambridge Phil. Soc., vol. 51 (1955), pp. 245—251.

GRÜN, OTTO

[7] *Über eine gewisse Klasse von endlichen Gruppen,* Mat. Nachr., vol. 8 (1952), pp. 167—169.

[8] *Beiträge zur Gruppentheorie. V,* Osaka Math. J., vol. 5 (1953), pp. 117—146.

[9] *Über das direkte Produkt regulärer p-Gruppen,* Arch. Math., vol. 5 (1954), pp. 241—243.

GRUENBERG, K. W.

[1] *A note on a theorem of Burnside,* Proc. Cambridge Phil. Soc., vol. 48 (1952), p. 202.

[2] *Two theorems on Engel groups,* Proc. Cambridge Phil. Soc., vol. 49 (1953), pp. 377—380.

[3] *Residual properties of groups,* Proc. London Math. Soc. (3), vol. 6 (1956).

HAEFELI-HUBER, V. E.

[1] *Ein Dualismus als Klassifikationsprinzip in der abstrakten Gruppentheorie,* Thesis, University of Zürich (1948).

HAIMO, F.

[2] *A class of inverse limit groups,* Amer. J. Math., vol. 71 (1949), pp. 171—177.

[3] *Groups with a certain condition on conjugates,* Canadian J. Math., vol. 4 (1952), pp. 369—372.

[4] *Some non-abelian extensions of completely divisible groups,* Proc. Amer. Math. Soc., vol. 5 (1954), pp. 256—258.

[5] *Automorphisms generated by a class of subnormal subgroups,* Duke Math. J., vol. 21 (1954), pp. 349—353.

[6] *The FC-chain of a group,* Canadian J. Math., vol. 5 (1953), pp. 498—511.

[7] *Power-type endomorphisms of some class 2 groups,* Pacific J. Math., vol. 5 (1955), pp. 201—213.

[8] *Normal automorphisms and their fixed points,* Trans. Amer. Math. Soc., vol. 78 (1955), pp. 150—167.

HAJÓS, G.

[1] *Sur la factorisation des groupes abéliens,* Časopis Pest. Mat. Fys., vol. 74 (1949), pp. 157—162.

[2] *Sur le probleme de factorisation des groupes cycliques,* Acta Math. Acad. Sci. Hungar., vol. 1 (1950), pp. 189—194.

HAKEN, H.

[1] *Zum Identitätsproblem bei Gruppen,* Math. Zeit., vol. 56 (1952), pp. 335—362.

HALL, M., JR.

[5] *Subgroups of free products,* Pacific J. Math., vol. 3 (1953), pp. 115—120.

[6] *On a theorem of Jordan,* Pacific J. Math., vol. 4 (1954), pp. 219—226.

HALL, P.

[11] *The splitting properties of relatively free groups,* Proc. London Math. Soc. (3), vol. 4 (1954), pp. 343—356.

[12] *Finiteness conditions for soluble groups,* Proc. London Math. Soc. (3), vol. 4 (1954), pp. 419—436.

[13] *Theorems like Sylow's,* Proc. London Math. Soc. (3), vol. 6 (1956).

HALL, P. and HIGMAN, G.

[1] *The p-length of a p-soluble group, and reduction theorems for Burnside's problem,* Proc. London Math. Soc. (3), vol. 6 (1956), pp. 1—42.

HANNINK, G.

[1] *Verlagerung und Nichteinfachheit von Gruppen,* Monatsh. Math. Phys., vol. 50 (1942), pp. 207—233.

HIGMAN, D. G.

[1] *Lattice homomorphisms induced by group homomorphisms,* Proc. Amer. Math. Soc., vol. 2 (1951), pp. 467—478.

[2] *Focal series in finite groups,* Canadian J. Math., vol. 5 (1953), pp. 477—497.

[3] *Remarks on splitting extensions,* Pacific J. Math., vol. 4 (1954), pp. 545—555.

HIGMAN, G.

[5] *Almost free groups,* Proc. London Math. Soc. (3). vol. 1 (1951), pp. 284—290.

[6] *On a problem of Takahasi,* J. London Math. Soc., vol. 28 (1953), pp. 250—252.

[7] *On infinite simple permutation groups,* Publ. Math. Debrecen, vol. 3 (1954), pp. 221—226.

[8] *A remark on finitely generated nilpotent groups,* Proc. Amer. Math. Soc., vol. 6 (1955), pp. 284—285.

[9] *Finite groups having isomorphic images in every finite group of which they are homomorphic images,* Quart. J. of Math. (Oxford Series), (1956).

[10] *On finite groups of exponent five,* Proc. Cambridge Phil. Soc., vol. 52 (1956).

HIGMAN, G. and NEUMANN, B. H.

[1] *On two questions of Itô,* J. London Math. Soc., vol. 29 (1954), pp. 84—88.

HIRSCH, K. A.

[6] *On a theorem of Burnside,* Quart. J. Math. Oxford Ser. (2), vol. 1 (1950), pp. 97—99.

[7] *Sur les groupes résolubles à condition maximale,* Colloques Internat. du CNRS., vol. 24 (1950), pp. 209—210.

[8] *On infinite soluble groups. IV,* J. London Math. Soc., vol. 27 (1952), pp. 81—85.

[9] *On infinite soluble groups. V,* J. London Math. Soc., vol. 29 (1954), pp. 250—254.

[10] *Über lokal-nilpotente Gruppen,* Math. Zeit., vol. 63 (1955), pp. 290—294.

HOCHSCHILD, G. and SERRE, J.-P.

[1] *Cohomology of group extensions,* Trans. Amer. Math. Soc., vol. 74 (1953), pp. 110—143.

HONDA, K.

[1] *On primary groups,* Comment. Math. Univ. St. Paul, vol. 2 (1954), pp. 71—83.

HÖNIG, C. S.

[1] *Classification of the additive groups of rational numbers,* Bol. Soc. Mat. São Paulo, vol. 3, no. 1—2 (1948), 37—47 (1951). [In Portuguese.]

HOWSON, A. G.

[1] *On the intersection of finitely generated free groups,* J. London Math. Soc., vol. 29 (1954), pp. 428—434.

HUGHES, N. J. S.

[1] *The use of bilinear mappings in the classification of groups of class* 2, Proc. Amer. Math. Soc., vol. 2 (1951), pp. 742—747.

[2] *The unique decomposition of regular* ω*-linear mappings as direct products,* Proc. Amer. Math. Soc., vol. 3 (1952), pp. 359—362.

HUPPERT, B.

[1] *Über das Produkt von paarweise vertauschbaren zyklischen Gruppen,* Math. Zeit., vol. 58 (1953), pp. 243—264.

[2] *Über die Auflösbarkeit faktorisierbarer Gruppen,* Math. Zeit., vol. 59 (1953), pp. 1—7.

[3] *Normalteiler und maximale Untergruppen endlicher Gruppen,* Math. Zeit., vol. 60 (1954), pp. 409—434.

HUPPERT, B. and ITÔ, N.

[1] *Über die Auflösbarkeit faktorisierbarer Gruppen. II,* Math. Zeit., vol. 61 (1954), pp. 94—99.

ITÔ, N.

[1] *Note on p-groups,* Nagoya Math. J., vol. 1 (1950), pp. 113—116.

[2] *Note on (LM)-groups of finite orders,* Kodai Math. Sem. Rep., (1951), pp. 1—6.

[3] *A theorem on the alternating group* $A_n (n \geqq 5)$, Math. Japonicae, vol. 2 (1951), pp. 59—60.

[4] *Remarks on factorizable groups,* Ann. Sci. Math. Szeged, vol. 14 (1951), pp. 83—84.

[5] *On a theorem of L. Rédei and J. Szép concerning p-groups,* Ann. Sci. Math. Szeged, vol. 14 (1952), pp. 186—187.

[6] *Note on A-groups,* Nagoya Math. J., vol. 4 (1952), pp. 79—81.

[7] *Note on S-groups,* Proc. Japan Acad., vol. 29 (1953), pp. 149—150.

[8] *Remarks on O. Grün's paper "Beiträge zur Gruppentheorie III,"* Math. Nachr., vol. 6 (1952), pp. 319—325.

[9] *On* Π*-structures of finite groups,* Tôhoku Math. J. (2), vol. 4 (1952), pp. 172—177.

[10] *On the factorization of the linear fractional group* $LF(2, p^n)$, Acta Sci. Math. Szeged, vol. 15 (1953), pp. 79—84.

[11] *Über das Produkt von zwei abelsche Gruppen,* Math. Zeit., vol. 62 (1955), pp. 400—401.

[12] *Über das Produkt von zwei zyklischen* 2*-Gruppen,* Nagoya Math. J., (1956).

ITÔ, N. and NAGATA, M.

[1] *Note on groups of automorphisms,* Kodai Math. Sem. Rep., No. 3 (1949), pp. 37—93.

IWASAWA, K.

[4] *On linearly ordered groups,* J. Math. Soc. Japan, vol. 1 (1948), pp. 1—9.

JENNINGS, S. A.

[2] *The group ring of a class of infinite nilpotent groups,* Canadian J. Math., vol. 7 (1955), pp. 169—187.

KALOUJNINE, L.

*[13] *Über eine Verallgemeinerung der p-Sylowgruppen symmetrischer Gruppen,* Acta Math. Acad. Sci. Hungar., vol. 2 (1951), pp. 197—221.

[14] *Über gewisse Beziehungen zwischen einer Gruppe und ihren Automorphismen,* Bericht Math. Tagung Berlin, January 1953, pp. 164—172.

KAPLANSKY, I.

[4] *Some result on abelian groups,* Proc. Nat. Acad. Sci. U.S.A., vol. 38 (1952), pp. 538—540.

KEMHADZE, Š. S.

*[3] *On the determination of regular p-groups,* Uspehi Matem. Nauk (N.S.), vol. 7 (1952), No. 6 (52), 193—196.

KERTÉSZ, A.

[1] *On groups every subgroup of which is a direct summand,* Publ. Math. Debrecen, vol. 2 (1951), pp. 74—75.

[2] *On the decomposability of abelian p-groups into the direct sum of cyclic groups,* Acta Math. Acad. Sci. Hungar., vol. 3 (1952), pp. 121—126.

[3] *On fully decomposable abelian torsion groups,* Acta Math. Acad. Sci. Hungar., vol. 3 (1952), pp. 225—232.

[4] *On a theorem of Kulikov and Dieudonné,* Acta Sci. Math. Szeged, vol. 15 (1953), pp. 61—69.

[5] *On subgroups and homomorphic images,* Publ. Math. Debrecen, vol. 3 (1954), pp. 174—179.

KERTÉSZ, A. and SZELE, T.

[1] *On abelian groups every multiple of which is a direct summand,* Acta Sci. Math. Szeged, vol. 14 (1952), pp. 157—166.

[2] *Abelian groups every finitely generated subgroup of which is an endomorphic image,* Acta Sci. Math. Szeged, vol. 15 (1953), pp. 70—76.

KINOSITA, Y.

[1] *On an enumeration of certain subgroups of a p-group,* J. Osaka Inst. Sci. Tech., Part I, vol. 1 (1949), pp. 13—20.

KNOCHE, H. G.

[1] *Über den Frobenius'schen Klassenbegriff in nilpotenten Gruppen,* Math. Zeit., vol. 55 (1951), pp. 71—83.

[2] *Über den Frobenius'schen Klassenbegriff in nipotenten Grupen. II,* Math. Zeit., vol. 59 (1953), pp. 8—16.

KOCHENDÖRFFER, R.

[1] *Zur Theorie des Rédeischen schiefen Produktes,* J. reine angew. Math., vol. 192 (1953), pp. 96—101.

KOSTRIKIN, A. I.

*[1] *Solution of the restricted Burnside problem for the exponent* 5, Izvestiya Akad. Nauk SSSR. Ser. Mat., vol. 19 (1955), pp. 233—244.

KUHN, H. W.

[1] *Subgroup theorems for groups presented by generators and relations,* Ann. of Math. (2), vol. 56 (1952), pp. 22—46.

KULIKOV, L. YA.

*[4] *Generalized primary groups. I,* Trudy Moskov. Mat. Obšč., vol. 1 (1952), pp. 247—326.

*[5] *Generalized primary groups. II,* Trudy Moskov. Mat. Obšč., vol. 2 (1953), pp. 85—167.

LAZARD, M.

[1] *Sur certaines suites d'éléments dans les groupes libres et leurs extensions,* C. R. Acad. Sci. Paris, vol. 236 (1953), pp. 36—38.

[2] *Problèmes d'extensions concernant les N-groupes; inversion de la formule de Hausdorff,* C. R. Acad. Sci. Paris, vol. 237 (1953), pp. 1377—1379.

LEDERMANN, W. and NEUMANN, B. H.

[1] *On the order of the automorphism group of a finite group. I,* Proc. Roy. Soc. A, (1956).

LYNDON, R. C.

[4] *Two notes on nilpotent groups,* Proc. Amer. Math. Soc., vol. 3 (1952), pp. 579—583.

[5] *On the Fuchs-Rabinovič series for free groups,* Portugal. Math., vol. 12 (1953), pp. 115—118.

[6] *On Burnside's problem,* Trans. Amer. Math. Soc., vol. 77 (1954), pp. 202—215.

[7] *On Burnside's problem. II,* Trans. Amer. Math. Soc., vol. 78 (1955), pp. 329—332.

MCLAIN, D. H.

[1] *A characteristically-simple group,* Proc. Cambridge Phil. Soc., vol. 50 (1954), pp. 641—642.

[2] *A class of locally nilpotent groups,* Thesis, Cambridge, 1956.

MACLANE, S.

[3] *Cohomology theory of abelian groups,* Proc. Int. Congr. Math. Cambri Mass. 1950, vol. 2, pp. 8—14.

MAL'CEV, A. I.

*[11] *On ordered groups,* Izvestiya Akad. Nauk SSSR. Ser. Mat., vol. 13 (19 pp. 473—482.

*[12] *On the completion of group order,* Trudy Mat. Inst. Steklov, vol. 38 (195 pp. 173—175.

MATSUSHITA, S. I.

[1] *Sur la puissance des ordres dans un groupe libre,* Nederl. Akad. Wetens Indag. Math., vol. 15 (1953), pp. 15—16.

MEIER-WUNDERLI, H.

[2] *Metabelsche Gruppen,* Comment. Math. Helv., vol. 25 (1951), pp. 1—10.

[3] *Note on a basis of P. Hall for the higher commutators in free groups,* Commer Math. Helv., vol. 26 (1952), pp. 1—5.

MILLER, C.

[1] *The second homology group of a group; relations among commutators,* Pro Amer. Math. Soc., vol. 3 (1952), pp. 588—595.

MIŠINA, A. P.

*[3] *On the isomorphism of complete direct sums of abelian groups of rank without torsion,* Mat. Sbornik N.S., vol. 31 (1952), pp. 118—127.

MORAN, S.

[1] *Associative operations on groups. I,* Proc. London Math. Soc. (3), vol. (1956).

NAGAO, H.

[2] *A note on extensions of groups,* Proc. Japan Acad., vol. 25 (1949), No. 10 pp. 11—14.

NEUMANN, B. H.

[11] *Groups with finite classes of conjugate elements,* Proc. London Math. Soc (3), vol. 1 (1951), pp. 241—256.

[12] *A note on algebraically closed groups,* J. London Math. Soc., vol. 27 (1952) pp. 247—249.

[13] *On a problem of Hopf,* J. London Math. Soc., vol. 28 (1953), pp. 351—353.

[14] *A note on means in groups,* J. London Math. Soc., vol. 28 (1953), pp. 472—476.

[15] *Groups covered by permutable subsets,* J. London Math. Soc., vol. 29 (1954), pp. 236—248.

[16] *An embedding theorem for algebraic systems,* Proc. London Math. Soc. (3), vol. 4 (1954), pp. 138—153.

[17] *An essay on free products of groups with amalgamations,* Philos. Trans. Roy. Soc. A, vol. 246 (1954), pp. 503—554.

[18] *Groups covered by finitely many cosets,* Publ. Math. Debrecen, vol. 3 (1955), pp. 227—242.

[19] *Groups with finite classes of conjugate subgroups,* Math. Zeit., vol. 63 (1955), pp. 76—96.

[20] *Ascending derived series,* Compositio Math., vol. 30 (1956).

[21] *Groups with automorphisms that leave only the neutral element fixed,* Arch. Math, vol. (1956).

[22] *On a question of Gaschütz,* Arch. Math, vol. 7 (1956).

NEUMANN, B. H. and NEUMANN, H.

[3] *Extending partial endomorphisms of groups,* Proc. London Math. Soc. (3), vol. 2 (1952), pp. 337—348.

[4] *On a class of abelian groups,* Arch. Math., vol. 4 (1953), pp. 79—85.

[5] *A contribution to the embedding theory of group amalgams,* Proc. London Math. Soc. (3), vol. 3 (1953), pp. 243—256.

[6] *Partial endomorphisms of finite groups,* J. London Math. Soc., vol. 29 (1954), pp. 434—440.

NEUMANN, H.

[4] *On the intersection of finitely generated groups,* Publ. Math. Debrecen, vol. 5 (1956).

NIELSEN, J.

[5] *The commutator group of the free product of cyclic groups,* Mat. Tidsskr. B. (1948), pp. 49—56. [In Danish.]

[6] *A study concerning the congruence subgroups of the modular group,* Danske Vid. Selsk. Mat.-Fys. Medd., vol. 25, No. 18 (1950), 32 pp.

[7] *A basis for subgroups of free groups,* Math. Scand., vol. 3 (1955), pp. 31—43.

NOVIKOV, P. S.

*[2] *Unsolvability of the conjugacy problem in the theory of groups,* Izv. Akad. Nauk SSSR. Ser. Mat., vol. 18 (1954), pp. 485—525.

*[3] *Algorithmic unsolvability of the identity problem,* Trudy Mat. Inst. Steklov, vol. 44 (1955).

OṄO, K. and TSUBOI, T.

[1] *Remarks on groups,* Sci. Rep. Yokohama Nat. Univ., Sect. I, vol. 2 (1953), pp. 13—15.

PETRESCO, J.

[1] *Sur les commutateurs,* Math. Zeit., vol. 61 (1954), pp. 348—356.

PIC, GH.

[1] *Sur le quasi-centre d'un groupe,* Acad. Repub. Pop. Romîne. Stud. Cerc. Mat., vol. 4 (1953), pp. 7—21. [In Romanian.]

ʏ, B. I.

] *On the theory of solvable torsion-free groups,* Doklady Akad. Nauk SSSR. (N.S.), vol. 84 (1952), pp. 665—668.

] *On nil groups,* Doklady Akad. Nauk SSSR. (N.S.), vol. 94 (1954), pp. 999—1001.

] *Lattice isomorphisms of solvable R-groups,* Doklady Akad. Nauk SSSR. (N.S.), vol. 95 (1954), pp. 1141—1144.

'] *On some criteria of locally nilpotent groups,* Uspehi Mat. Nauk (N.S.), vol. 9 (1954), No. 3 (61), pp. 181—186.

;] *On the nil-radical of a group,* Doklady Akad. Nauk SSSR. (N.S.), vol. 98 (1954), pp. 341—343.

)] *On the theory of solvable, torsion-free groups,* Mat. Sbornik (N.S.), vol. 36 (1955), pp. 31—38.

)] *On the theory of solvable groups with finiteness conditions,* Doklady Akad. Nauk SSSR. (N.S.), vol. 100 (1955), pp. 417—420.

ʁ.

l] *A theorem on abelian groups,* J. London Math. Soc., vol. 22 (1947), pp. 219—226.

2] *A proof of the basis theorem for finitely generated abelian groups,* J. London Math. Soc., vol. 26 (1951), pp. 74—75, 160.

L.

l] *Das "schiefe Produkt" in der Gruppentheorie mit Anwendung auf die endlichen nicht kommutativen Gruppen mit lauter kommutativen echten Untergruppen und die Ordnungszahlen, zu denen nur kommutative Gruppen gehören,* Comment. Math. Helv., vol. 20 (1947), pp. 225—262.

2] *Vereinfachter Beweis des Satzes von Minkowski-Hajós,* Acta Sci. Math. Szeged, vol. 13 (1949), pp. 21—35.

3] *Die Reduktion des gruppentheoretischen Satzes von Hajós auf den Fall von p-Gruppen,* Monatsh. Math. Phys., vol. 53 (1949), pp. 221—226.

4] *Kurzer Beweis des gruppentheoretischen Satzes von Hajós,* Comment. Math. Helv., vol. 23 (1949), pp. 272—282.

5] *Die Anwendung des schiefen Produktes in der Gruppentheorie,* J. reine angew. Math., vol. 188 (1950), pp. 201—227.

6] *Ein Satz über die endlichen einfachen Gruppen,* Acta Math. Copenhagen, vol. 84 (1950), pp. 129—153.

7] *Zur Theorie der faktorisierbaren Gruppen. I,* Acta Math. Acad. Sci. Hungar., vol. 1 (1950), pp. 74—98.

8] *Die endlichen Gruppen ohne direkt unzerlegbare Untergruppen,* Math. Ann., vol. 122 (1950), pp. 127—130.

9] *Endlich-projektivgeometrisches Analogon des Minkowskischen Fundamentalsatzes,* Acta Math. Copenhagen, vol. 84 (1950), pp. 155—158.

0] *Über die Basen endlicher Gruppen,* Math. Zeit., vol. 53 (1951), pp. 454—455.

[11] *Ein Beitrag zum Problem der Faktorisation von endlichen abelschen Gruppen,* Acta Math. Acad. Sci. Hungar., vol. 1 (1950), pp. 197—207.

[12] *Die Einfachheit der alternierenden Gruppe,* Monatsh. Math. Phys., vol. 55 (1951), pp. 328—329.

[13] *Die Holomorphentheorie für Gruppen und Ringe,* Acta Math. Acad. Sci. Hungar., vol. 5 (1954), pp. 169—194.

RÉDEI, L. and STEINFELD, O.

[1] *Gegenseitige Schreiersche Gruppenerweiterungen,* Acta Sci. Math. Szeged, vol. 15 (1954), pp. 243—250.

RÉDEI, L. and STÖHR, A.

[1] *Über ein spezielles schiefes Produkt in der Gruppentheorie,* Acta Sci. Math. Szeged, vol. 15 (1953), pp. 7—11.

RÉDEI, L. and SZÉP, J.

[1] *Über die endlichen nilpotenten Gruppen,* Monatsh. Math. Phys., vol. 55 (1951), pp. 200—205.

REE, R.

[1] *On ordered, finitely generated, solvable groups,* Trans. Royal Soc. Canada Sec. III, vol. 48 (1954), pp. 39—42.

REED, I. S.

[1] *A general isomorphism theorem for factor groups,* Math. Mag., vol. 24 (1951). pp. 191—194.

ROBINSON, A.

[1] *Note on an embedding theorem for algebraic systems,* J. London Math. Soc., vol. 30 (1955), pp. 249—252.

SASIADA, E.

[1] *On abelian groups every countable subgroup of which is an endomorphic image,* Bull. Acad. Polon. Sci. Cl. III, vol. 2 (1954), pp. 359—362.

SATO, S.

[2] *Note on lattice isomorphisms between abelian groups and non-abelian groups,* Osaka Math. J., vol. 3 (1951), pp. 215—220.

[3] *On the lattice homomorphisms of infinite groups. I,* Osaka Math. J., vol. 4 (1952), pp. 229—234.

SCHENKMAN, E.

[1] *A generalization of the central elements of a group,* Pacific J. Math., vol. 3 (1953), pp. 501—504.

[2] *Two theorems on finitely generated groups,* Proc. Amer. Math. Soc., vol. 5 (1954), pp. 497—498.

[3] *The existence of outer automorphisms of some nilpotent groups of class 2,* Proc. Amer. Math. Soc., vol. 6 (1955), pp. 6—11.

[4] *The splitting of certain solvable groups,* Proc. Amer. Math. Soc., vol. 6 (1955), pp. 286—290.

SCHIEK, H.

[1] *Bemerkung über eine Relation in freien Gruppen,* Math. Ann., vol. 126 (1953), pp. 375—376.

SCOTT, W. R.

[3] *Means in groups,* Amer. J. Math., vol. 74 (1952), pp. 667—675.

[4] *The number of subgroups of given index in nondenumerable abelian groups,* Proc. Amer. Math. Soc., vol. 5 (1954), pp. 19—22.

[5] *On the order of the automorphism group of a finite group,* Proc. Amer. Math. Soc., vol. 5 (1954), pp. 23—24.

SEGAL, I. E.

[1] *The non-existence of a relation which is valid for all finite groups,* Bol. Soc. Mat. São Paulo, vol. 2, No. 2 (1947), pp. 3—5 (1949).

SESEKIN, N. F.

*[2] *On the theory of locally nilpotent torsion-free groups,* Doklady Akad. Nauk SSSR. (N.S.), vol. 84 (1952), pp. 225—228.

*[3] *On locally nilpotent torsion-free groups,* Mat. Sbornik N.S., vol. 32 (1953), pp. 407—442.

SESEKIN, N. F. and STAROSTIN, A. I.

*[1] *On a class of periodic groups,* Uspehi Mat. Nauk (N.S.), vol. 9 (1954), No. 4 (62), pp. 225—228.

SHENITZER, A.

[1] *Decomposition of a group with a single defining relation into a free product,* Proc. Amer. Math. Soc., vol. 6 (1955), pp. 273—279.

SMIRNOV, D. M.

*[2] *On automorphisms of solvable groups,* Doklady Akad. Nauk SSSR. (N.S.), vol. 84 (1952), pp. 891—894.

*[3] *On groups of automorphisms of solvable groups,* Mat. Sbornik N.S., vol. 32 (1953), pp. 365—384.

*[4] *On groups with upper central series,* Mat. Sbornik N.S., vol. 33 (1953), pp. 471—484.

*[5] *Infrainvariant subgroups,* Uč. Zap. Ivanovsk Ped. Inst., vol. 4 (1953), pp. 92—96.

SPECKER, E.

[1] *Additive Gruppen von Folgen ganzer Zahlen,* Portugal, Math., vol. 9 (1950), pp. 131—140.

STENDER, P. V.

*[1] *On the application of the sieve method to the solution of the word problem for certain groups with a denumerable set of generating elements and a denumerable set of defining relations,* Mat. Sbornik N.S., vol. 32 (1953), pp. 97—108.

STRUIK, R. R.

[1] *On associative products of groups,* Bull. Amer. Math. Soc., vol. 61 (1955), pp. 219—220; to appear in Trans. Amer. Math. Soc.

SUZUKI, M.

[3] *On the finite groups with a complete partition,* J. Math. Soc. Japan, vol. 2 (1950), pp. 165—185.

[4] *A characterization of the simple groups LF* (2, p), J. Fac. Sci. Univ. Tokyo, Sect. I., vol. 6 (1951), pp. 259—293.

SZEKERES, G.

[2] *On a certain class of metabelian groups,* Ann. Math. Princeton (2), vol. 49 (1948), pp. 43—52.

[3] *Determination of a certain family of finite metabelian groups,* Trans. Amer. Math. Soc., vol. 66 (1949), pp. 1—43.

SZELE, T.

[5] *Neuer vereinfachter Beweis des gruppentheoretischen Satzes von Hajós,* Publ. Math. Debrecen, vol. 1 (1949), pp. 56—62.

[6] *Über die direkten Teiler der endlichen abelschen Gruppen,* Comment. Math. Helv., vol. 22 (1949), pp. 117—124.

[7] *Sur la decomposition directs des groupes abeliens,* C. R. Acad. Sci. Paris, vol. 229 (1949), pp. 1052—1053.

[8] *Ein Analogen der Körpertheorie für abelsche Gruppen,* J. reine angew. Math., vol. 188 (1950), pp. 167—192.

[9] *Die unendliche Quaternionengruppe,* Acad. Repub. Pop. Române. Bul. Sti. A., vol. 1 (1949), pp. 799—802.

[10] *On direct sums of cyclic groups,* Publ. Math. Debrecen, vol. 2 (1951), pp. 76—78.

[11] *Sur les groupes ayant un sous-groupe parfait,* Bull. Sci. Math. (2), vol. 74 (1950), pp. 207—209.

[12] *Gruppentheoretische Beziehungen bei gewissen Ringkonstruktionen,* Math. Zeit., vol. 54 (1951), pp. 168—180.

[13] *On a theorem of Pontrjagin,* Acta Math. Acad. Sci. Hungar., vol. 2 (1951), pp. 121—129.

[14] *On groups with atomic layers,* Acta Math. Acad. Sci. Hungar., vol. 3 (1952), pp. 127—129.

[15] *On direct decompositions of abelian groups,* J. London Math. Soc., vol. 28 (1953), pp. 247—250.

[16] *On non-countable abelian p-groups,* Publ. Math. Debrecen, vol. 2 (1952), pp. 300—301.

[17] *On direct sums of cyclic groups with one amalgamated subgroup,* Publ. Math. Debrecen, vol. 2 (1952), pp. 302—307.

[18] *The multiplicative group of the roots of unity,* Magyar Tud. Akad. Mat. Fiz. Oszt. Közl., vol. 3 (1953), pp. 55—58.

[19] *On arbitrary systems of linear equations,* Publ. Math. Debrecen, vol. 2 (1952), pp. 297—299.

[20] *On the basic subgroups of abelian p-groups,* Acta Math. Acad. Sci. Hungar., vol. 5 (1954), pp. 129—141.

SZELE, T. and SZENDREI, J.

[1] *On abelian groups with commutative endomorphism ring,* Acta Math. Acad. Sci. Hungar., vol. 2 (1951), pp. 309—324.

SZÉLPÁL, I.

[1] *Die abelschen Gruppen ohne eigentliche Homomorphismen,* Acta Univ. Szeged. Sect. Sci. Math., vol. 13 (1949), pp. 51—53.

[2] *Die unendlichen abelschen Gruppen mit lauter endlichen echten Untergruppen,* Publ. Math. Debrecen, vol. 1 (1949), pp. 63—64.

[3] *The abelian groups with torsion-free endomorphism ring,* Publ. Math. Debrecen, vol. 3 (1954), pp. 106—108.

[4] *Über die untere Grenze der Ordnung n-stufig nicht-kommutativen Gruppen,* Comm. Math. Helv. vol. 27 (1953), pp. 73—74.

SZENDREI, J.

[1] *Eine neue Definition des Holomorphes der Gruppe und der Holomorphe des Ringes,* Acta Math. Acad. Sci. Hungar., vol. 5 (1954), pp. 197—201.

SZÉP, J.

[1] *On simple groups,* Publ. Math. Debrecen, vol. 1 (1949), p. 98.

[2] *On the structure of groups which can be represented as the product of two subgroups,* Acta Sci. Math. Szeged, vol. 12 (1950), pp. 57—61.

[3] *On factorisable simple groups,* Acta Sci. Math. Szeged, vol. 14 (1951), p. 22.

[4] *Zur Theorie der faktorisierbaren Gruppen,* Publ. Math. Debrecen, vol. 2 (1951), pp. 43—45.

[5] *Zur Theorie der endlichen einfachen Gruppen,* Acta Sci. Math. Szeged, vol. 14 (1951), pp. 111—112.

[6] *Zur Theorie der einfachen Gruppen,* Acta Sci. Math. Szeged, vol. 14 (1952), p. 246.

[7] *Über endliche einfache Gruppen,* C. R. de Premier Congres des Math. Hongrois 1950, (1952), pp. 451—453. [In Hungarian.]

[8] *Bemerkung zu einem Satz von O. Ore.,* Publ. Math. Debrecen, vol. 3 (1954), pp. 81—82.

SZÉP, J. and RÉDEI, L.

[1] *On factorisable groups,* Acta Sci. Math. Szeged, vol. 13 (1950), pp. 235—238.

[2] *Eine Verallgemeinerung der Remakschen Zerlegung,* Acta Sci. Math. Szeged, vol. 15 (1953), pp. 85—86.

[3] *Zur Theorie der faktorisierbaren Gruppen,* Acta Sci. Math. Szeged, vol. 16 (1955), pp. 54—57.

TAKAHASI, M.

[4] *Note on word subgroups in free products of groups,* J. Inst. Polytech. Osaka City Univ. Ser. A. Math., vol. 2 (1951), pp. 13—18.

[5] *Primitive locally free groups,* J. Inst. Polytech. Osaka City Univ. Ser. A. Math., vol. 2 (1951), pp. 1—11.

[6] *Note on chain conditions in free groups,* Osaka Math. J., vol. 3 (1951), pp. 221—225.

[7] *Group extensions and their splitting groups,* J. Inst. Polytech. Osaka City Univ. Ser. A. Math., vol. 5 (1954), pp. 81—85.

TAUNT, D. R.

[1] *On A-groups,* Proc. Cambridge Phil. Soc., vol. 45 (1949), pp. 24—42.

[2] *Remarks on the isomorphism problem in theories of construction of finite groups,* Proc. Cambridge Phil. Soc., vol. 51 (1955), pp. 16—24.

[3] *Finite groups having unique proper characteristic subgroups. I,* Proc. Cam bridge Phil. Soc., vol. 51 (1955), pp. 25—36.

TAYLOR, R. L.

[1] *Compound group extensions. I,* Trans. Amer. Math. Soc., vol. 75 (1953), pp. 106—135.

[2] *Compound group extensions. II,* Trans. Amer. Math. Soc., vol. 75 (1953), pp. 304—310.

[3] *Compound group extensions III,* Trans. Amer. Math. Soc., vol. 79 (1955), pp. 490—520.

TSUBOI, T.

[1] *On finite simple groups,* Sci. Rep. Saitama Univ. Ser. A., vol. 1 (1953), pp. 55—57.

[2] *On abelian normal subgroups,* Sci. Rep. Saitama Univ. Ser. A., vol. 1 (1954), pp. 101—104.

[3] *Note on metabelian groups,* Sci. Rep. Saitama Univ. Ser. A., vol. 1 (1953), pp. 59—62.

TUAN, H. F.

[1] *An Anzahl theorem of Kulakov's type for p-groups,* Sci. Rep. Nat. Tsing Hua Univ. Ser. A., vol .5 (1948), pp. 182—189.

[2] *A theorem about p-groups with abelian subgroups of index p,* Acad. Sinica Science Record, vol. 3 (1950), pp. 17—23.

TURING, A. M.

[2] *The word problem in semi-groups with cancellation,* Ann. of Math. (2), vol. 52 (1950), pp. 491—505.

VINOGRADOV, A. A.

*[1] *On the free product of ordered groups,* Mat. Sbornik N.S., vol. 25 (1949), pp. 163—168.

WEDDERBURN, J. H. M.

[1] *On the direct product in the theory of finite groups,* Ann. of Math., vol. 10.

WEIR, A. J.

[1] *The Reidemeister-Schreier and Kuroš subgroup theorems,* Matematika, vol. 3 (1956).

WEVER, F.

[2] *Über die Kennzeichnung von Relationen endlicher Gruppen,* Arch. Math. vol. 5 (1954), pp. 326—331.

WIELANDT, H.

[4] *Über das Produkt paarweise vertauschbarer nilpotenter Gruppen,* Math. Zeit., vol. 55 (1951), pp. 1—7.

[5] *Zum Satz von Sylow,* Math. Zeit., vol. 60 (1954), pp. 407—408.

YAMABE, H.

[1] *A condition for an abelian group to be a free abelian group with a finite basis,* Proc. Japan Acad., vol. 27 (1951), pp. 205—207.

YEH, Y.

[1] *On prime power abelian groups,* Bull. Amer. Math. Soc., vol. 54 (1948), pp. 323—327.

ZACHER, G.

[1] *Costruzione dei gruppi finiti a sottogruppo di Frattini identico,* Rend. Sem. Mat. Univ., Padova, vol. 21 (1952), pp. 383—394.

[2] *Caratterizzazione dei t-gruppi finiti risolubili,* Ricerche di Mat., vol. 1 (1952), pp. 287—294.

[3] *Caratterizzazione dei gruppi risolubili d'ordine finito complementati,* Rend. Sem. Mat. Univ. Padova, vol. 22 (1953), pp. 113—122.

[4] *Determinazione dei gruppi d'ordine finite relativamente complementati,* Rend. Acad. Sci. Fis. Mat. Napoli (4), vol. 19 (1953), pp. 200—206.

[5] *Sugli elementi modulari in un p-gruppo,* Rend. Sem. Mat. Univ. Padova, vol. 24 (1955), pp. 165—182.

ZAPPA, G.

[6] *Sulla costruzione dei gruppi prodotto di due dati sottogruppi permutabili tra loro,* Atti Secondo Congresso Un. Mat. Ital. Bologna (1942), pp. 119—125.

[7] *Determinazione dei gruppi finiti in omomorfismo strutturale con un gruppo ciclico,* Rend. Sem. Mat. Univ. Padova, vol. 18 (1949), pp. 140—162.

[8] *Sulla condizione perche un omomorfismo ordinario sia anche un omomorfismo strutturale,* Giorn. Mat. Battaglini (4), vol. 2 (78) (1949), pp. 182—192.

[9] *Sulla condizione perche un emitropismo inferiore tipico tra due gruppi sia un omotropismo,* Gion. Mat. Battaglini (4), vol. 4 (80) (1951), pp. 80—101.

[10] *Sulla risolubilitá dei gruppi finiti in isomorfismo reticolare con un gruppo resolubile,* Giorn. Mat. Battaglini (4), vol. 4 (80) (1951), pp. 213—225.

[11] *Sulle p-catene dei gruppi p-risolubili,* Giorn. Mat. Battaglini (4), vol. 3 (79) (1950), pp. 121—126.

[12] *Sugli omomorfismi del reticolo dei sottogruppi di un gruppo finito,* Ricerche Mat., vol. 1 (1952), pp. 78—106.

[13] *Sui gruppi p-supersolubili,* Rend. Accad. Sci. Fis. Mat. Napoli, (4), vol. 17 (1951), pp. 328—339.

[14] *Sopra un extenzione di Wielandt del teorema di Sylow.* Boll. Un. Mat. Ital. (3), vol. 9 (1954), pp. 349—353.

ZEEMAN, E. C.

[1] *On direct sums of free cycles,* J. London Math. Soc., vol. 30 (1955), pp. 195—212.

INDEX

AUTHOR INDEX

INDEX

CHELSEA
SCIENTIFIC
BOOKS

THEORY OF FUNCTIONS

By C. CARATHEODORY

Translated by F. STEINHARDT. The recent, and already famous textbook, *Funktionentheorie.*

Partial Contents: **Part One.** Chap. I. Algebra of Complex Numbers. II. Geometry of Complex Numbers. III. Euclidean, Spherical, and Non-Euclidean Geometry. **Part Two.** Theorems from Point Set Theory and Topology. Chap. I. Sequences and Continuous Complex Functions. II. Curves and Regions. III. Line Integrals. **Part Three.** Analytic Functions. Chap. I. Foundations. II. The Maximum-modulus principle. III. Poisson Integral and Harmonic Functions. IV. Meromorphic Functions. **Part Four.** Generation of Analytic Functions by Limiting Processes. Chap. I. Uniform Convergence. II. Normal Families of Meromorphic Functions. III. Power Series. IV. Partial Fraction Decomposition and the Calculus of Residues. **Part Five.** Special Functions. Chap. I. The Exponential Function and the Trigonometric Functions. II. Logarithmic Function. III. Bernoulli Numbers and the Gamma Function.

Vol. II.: **Part Six.** Foundations of Geometric Function Theory. Chap. I. Bounded Functions. II. Conformal Mapping. III. The Mapping of the Boundary. **Part Seven.** The Triangle Function and Picard's Theorem. Chap. I. Functions of Several Complex Variables. II. Conformal Mapping of Circular-Arc Triangles. III. The Schwarz Triangle Functions and the Modular Function. IV. Essential Singularities and Picard's Theorems.

"A book by a master . . . Carathéodory himself regarded [it] as his finest achievement . . . written from a catholic point of view."—*Bulletin of A.M.S.*

—Vol. I. Second edition. 1958. 310 pp. 6x9. [97] **$4.95**
—Vol. II. Second edition. 1960. 220 pp. 6x9. [106] **$4.95**

ALGEBRAIC THEORY OF MEASURE AND INTEGRATION

By C. CARATHÉODORY

Translated from the German by FRED E. J. LINTON. By generalizing the concept of point function to that of a function over a Boolean ring ("soma" function), Prof. Carathéodory gives an algebraic treatment of measure and integration.

CONTENTS: CHAP. I. Somas (Axiomatic method, somas as elements of a Boolean ring, . . .). II. Set of Somas. III. Place Functions (Functionoids). IV. Computation with Place Functions. V. Measure Functions. VI. The Integral. VII. Application of Integration to Limit Processes. VIII. Computation of Measure Functions. IX. Regular Measure Functions. X. Isotypic Regular Measure Functions. XI. Content Functions. APPENDIX: Somas as Elements of Partially Ordered Sets.

—1963. 378 pp. 6x9. [161] **$7.50**

ASYMPTOTIC SERIES

By W. B. FORD

TWO VOLUMES IN ONE: *Studies on Divergent Series and Summability* and *The Asymptotic Developments of Functions Defined by MacLaurin Series.*

PARTIAL CONTENTS: I. MacLaurin Sum-Formula; Introduction to Study of Asymptotic Series. II. Determination of Asymptotic Development of a Given Function. III. Asymptotic Solutions of Linear Differential Equations. . . . V. Summability, etc. *I.* First General Theorem. . . . *III.* MacLaurin Series whose General Coefficient is Algebraic. . . . *VII.* Functions of Bessel Type. *VIII.* Asymptotic Behavior of Solution of Differential Equations of Fuchsian Type. Bibliography.

—1916; 1936-60. x + 341 pp. 6x9. [143] Two vols. in one. **$6.00**

THE CALCULUS OF EXTENSION

By H. G. FORDER

—1941-60. xvi + 490 pp. 5⅜x8. [135] **$4.95**

RUSSIAN MATHEMATICAL BIBLIOGRAPHY

By G. E. FORSYTHE

A bibliography of Russian Mathematics Books for the quarter century 1920-55. Added subject index.

—1956. 106 pp. 5x8. [111] **$3.95**

CURVE TRACING

By P. FROST

This much-quoted and charming treatise gives a very readable treatment of a topic that can only be touched upon briefly in courses on Analytic Geometry. Teachers will find it invaluable as supplementary reading for their more interested students and for reference. The Calculus is not used.

Seventeen plates, containing over 200 figures, illustrate the discussion in the text.

—5th (unaltered) ed. 1960. 210 pp. + 17 fold-out plates. 5⅜x8. [140] **$3.95**

THE THEORY OF MATRICES

By F. R. GANTMACHER

This treatise, by one of Russia's leading mathematicians gives, in easily accessible form, a coherent account of matrix theory with a view to applications in mathematics, theoretical physics, statistics, electrical engineering, etc. The individual chapters have been kept as far as possible independent of each other, so that the reader acquainted with the contents of Chapter I can proceed immediately to the chapters that especially interest him. Much of the material has been available until now only in the periodical literature.

Partial Contents. VOL. ONE. I. Matrices and Matrix Operations. II. The Algorithm of Gauss and Applications. III. Linear Operators in an n-Dimensional Vector Space. IV. Characteristic Polynomial and Minimal Polynomial of a Matrix (Generalized Bézout Theorem, Method of Faddeev for Simultaneous Computation of Coefficients of Characteristic Polynomial and Adjoint Matrix, . . .). V. Functions of Matrices (Various Forms of the Definition, Components, Application to Integration of System of Linear Differential Eqns, Stability of Motion, . . .). VI. Equivalent Transformations of Polynomial Matrices; Analytic Theory of Elementary Divisors. VII. The Structure of a Linear Operator in an n-Dimensional Space (Minimal Polynomial, Congruence, Factor Space, Jordan Form, Krylov's Method of Transforming Secular Eqn, . . .). VIII. Matrix Equations (Matrix Polynomial Eqns, Roots and Logarithm of Matrices, . . .). IX. Linear Operators in a Unitary Space. X. Quadratic and Hermitian Forms.

VOL. TWO. XI. Complex Symmetric, Skew-symmetric, and Orthogonal Matrices. XII. Singular Pencils of Matrices. XIII. Matrices with Non-Negative Elements (Gen'l and Spectral Properties, Reducible M's, Primitive and Imprimitive M's, Stochastic M's, Totally Non-Negative M's, . . .). XIV. Applications of the Theory of Matrices to the Investigation of Systems of Linear Differential Equations. XV. The Problem of Routh-Hurwitz and Related Questions (Routh's Algorithm, Lyapunov's Theorem, Infinite Hankel M's, Supplements to Routh-Hurwitz Theorem, Stability Criterion of Liénard and Chipart, Hurwitz Polynomials, Stieltjes' Theorem, Domain of Stability, Markov Parameters, Problem of Moments, Markov and Chebyshev Theorems, Generalized Routh-Hurwitz Problem, . . .). BIBLIOGRAPHY.

—Vol. I. 1960. x + 374 pp. 6x9. [131] **$6.00**
—Vol. II. 1960. x + 277 pp. 6x9. [133] **$6.00**

LECTURES ON ANALYTICAL MECHANICS

By F. R. GANTMACHER

Translated from the Russian by PROF. B. D. SECKLER, with additions and revisions by Prof. Gantmacher.

Partial Contents: CHAP. I. Differential Equations of Motion of a System of Particles. II. Equations of Motion in a Potential Field. III. Variational Principles and Integral-Invariants. IV. Canonical Transformations and the Hamilton-Jacobi Equation. V. Stable Equilibrium and Stability of Motion of a System (Lagrange's Theorem on stable equilibrium, Tests for unstable E., Theorems of Lyapunov and Chetayev, Asymptotically stable E., Stability of linear systems, Stability on basis of linear approximation, . . .). VI. Small Oscillations. VII. Systems with Cyclic Coordinates. BIBLIOGRAPHY.

—Approx. 300 pp. 6x9. [175] **In prep.**

LECTURES ON ERGODIC THEORY

By P. R. HALMOS

CONTENTS: Introduction. Recurrence. Mean Convergence. Pointwise Convergence. Ergodicity. Mixing. Measure Algebras. Discrete Spectrum. Automorphisms of Compact Groups. Generalized Proper Values. Weak Topology. Weak Approximation. Uniform Topology. Uniform Approximation. Category. Invariant Measures. Generalized Ergodic Theorems. Unsolved Problems.

"Written in the pleasant, relaxed, and clear style usually associated with the author. The material is organized very well and painlessly presented. A usually associated with the author."

—1960. (Repr. of 1956 ed.) viii + 101 pp. 5¼x8. [142] **$2.95**

ALGEBRAIC LOGIC

By P. R. HALMOS

"Algebraic Logic is a modern approach to some of the problems of mathematical logic, and the theory of polyadic Boolean algebras, with which this volume is mostly concerned, is intended to be an efficient way of treating algebraic logic in a unified manner.

"[The material] is accessible to a general mathematical audience; no vast knowledge of algebra or logic is required . . . Except for a slight Boolean foundation, the volume is essentially self-contained."—*From the Preface.*

—1962 271 pp. 6x9 [154] **$3.95**

RAMANUJAN:
Twelve Lectures on His Life and Works

By G. H. HARDY

The book is somewhat more than an account of the mathematical work and personality of Ramanujan; it is one of the very few full-length books of "shop talk" by an important mathematician.

—viii + 236 pp. 6x9. [136] **$3.95**

GRUNDZÜGE DER MENGENLEHRE

By F. HAUSDORFF

Some of the topics in the Grundzüge omitted from later editions:

Symmetric Sets—Principle of Duality—most of the "Algebra" of Sets—most of the "Ordered Sets"—Partially Ordered Sets—Arbitrary Sets of Complexes—Normal Types—Initial and Final Ordering—Complexes of Real Numbers—General Topological Spaces—Euclidean Spaces—the Special Methods Applicable in the Euclidean plane—Jordan's separation Theorem—The Theory of Content and Measure—The Theory of the Lebesgue Integral.

—First edition. viii+476 pp. [61] **$6.00**

SET THEORY

By F. HAUSDORFF

Now for the first time available in English, Hausdorff's classic text-book has been an inspiration and a delight to those who have read it in the original German. The translation is from the Third (latest) German edition.

"We wish to state without qualification that this is an indispensable book for all those interested in the theory of sets and the allied branches of real variable theory."—*Bulletin of A. M. S.*

—2nd ed. 1962. 352 pp. 6x9. [119] **$6.50**

VORLESUNGEN ÜBER DIE THEORIE DER ALGEBRAISCHEN ZAHLEN

By E. HECKE

"An elegant and comprehensive account of the modern theory of algebraic numbers."

—*Bulletin of the A. M. S.*

—1923. 264 pp. 5½x8½. [46] **$3.95**

INTEGRALGLEICHUNGEN UND GLEICHUNGEN MIT UNENDLICHVIELEN UNBEKANNTEN

By E. HELLINGER and O. TOEPLITZ

"Indispensable to anybody who desires to penetrate deeply into this subject."—*Bulletin of A.M.S.*

—With a preface by E. Hilb. 1928. 286 pp. 5¼x8. [89] **$4.50**

Grundzüge Einer Allgemeinen Theorie der LINEAREN INTEGRALGLEICHUNGEN

By D. HILBERT

—306 pp. 5½x8¼. [91] **$4.50**

PRINCIPLES OF MATHEMATICAL LOGIC

By D. HILBERT and W. ACKERMANN

The famous *Grundüge der Theoretischen Logik* translated into English, with added notes and revisions by PROF. R. E. LUCE.

"The best textbook in a Western European language for a student wishing a fairly thorough treatment."—*Bulletin of the A. M. S.*

—1950-59. xii + 172 pp. 6x9. [69] **$3.95**

DETERMINANTENTHEORIE EINSCHLIESSLICH DER FREDHOLMSCHEN DETERMINANTEN

By G. KOWALEWSKI

"A classic in its field."—*Bulletin of the A. M. S.*

—Third edition. 1942. 328 pp. 5½x8. [39] **$4.95**

GROUP THEORY

By A. KUROSH

Translated from the second Russian edition and with added notes by PROFESSOR K. A. HIRSCH.

Partial Contents: PART ONE: The Elements of Group Theory. Chap. I. Definition. II. Subgroups (Systems, Cyclic Groups, Ascending Sequences of Groups). III. Normal Subgroups. IV. Endomorphisms and Automorphisms. Groups with Operators. V. Series of Subgroups. Direct Products. Defining Relations, etc. PART TWO: Abelian Groups. VI. Foundations of the Theory of Abelian Groups (Finite Abelian Groups, Rings of Endomorphisms, Abelian Groups with Operators). VII. Primary and Mixed Abelian Groups. VIII. Torsion-Free Abelian Groups. Editor's Notes. Bibliography.

Vol. II. PART THREE: Group-Theoretical Constructions. IX. Free Products and Free Groups (Free Products with Amalgamated Subgroup, Fully Invariant Subgroups). X. Finitely Generated Groups. XI. Direct Products. Lattices (Modular, Complete Modular, etc.). XII. Extensions of Groups (of Abelian Groups, of Non-commutative Groups, Cohomology Groups). PART FOUR: Solvable and Nilpotent Groups. XIII. Finiteness Conditions, Sylow Subgroups, etc. XIV. Solvable Groups (Solvable and Generalized Solvable Groups, Local Theorems). XV. Nilpotent Groups (Generalized, Complete, Locally Nilpotent Torsion-Free, etc.). Editor's Notes. Bibliography.

—Vol. I. 2nd ed. 1959. 271 pp. 6x9. [107] **$5.50**
—Vol. II. 2nd ed. 1960. 308 pp. 6x9. [109] **$5.50**

LECTURES ON GENERAL ALGEBRA

By A. G. KUROSH

Translated from the Russian by PROFESSOR K. A. HIRSCH, with a special preface for this edition by PROFESSOR KUROSH.

Partial Contents: CHAP. I. Relations. II. Groups and Rings (Groupoids, Semigroups, Groups, Rings, Fields, . . . , Gaussian rings, Dedekind rings). III. Universal Algebras. Groups with Multioperators (. . . Free universal algebras, Free products of groups). IV. Lattices (Complete lattices, Modular lattice, Schmidt-Ore Theorem, . . . , Distributive lattices). V. Operator Groups and Rings. Modules. Linear Algebras (. . . Free modules, Vector spaces over fields, Rings of linear transformations, . . . , Derivations, Differential rings). VI. Ordered and Topological Groups and Rings. Rings with a Valuation. BIBLIOGRAPHY.

—1963. 335 pp. [168] **$6.95**

DIFFERENTIAL AND INTEGRAL CALCULUS

By E. LANDAU

A masterpiece of rigor and clarity.

—2nd ed. 1960. 372 pp. 6x9. [78] **$6.00**

ELEMENTARE ZAHLENTHEORIE

By E. LANDAU

"Interest is enlisted at once and sustained by the accuracy, skill, and enthusiasm with which Landau marshals . . . facts and simplifies . . . details."

—G. D. Birkhoff, Bulletin of the A. M. S.

—1927. vii + 180 + iv pp. 5½x8¼. [26] **$3.50**

VORLESUNGEN ÜBER ZAHLENTHEORIE

By E. LANDAU

The various sections of this important work (Additive, Analytic, Geometric, and Algebraic Number Theory) can be read independently of one another.

—Vol. I, Pt. 2. * (Additive Number Theory) xii + 180 pp. Vol. II. (Analytical Number Theory and Geometrical Number Theory) viii + 308 pp. Vol. III. (Algebraic Number Theory and Fermat's Last Theorem) viii + 341 pp. 5¼x8¼. * (Vol. I, Pt. 1 is issued as **Elementare Zahlentheorie** (in German) or as **Elementary Number Theory** (in English). Orig. publ. at $26.40. [32] Three Vols. in one. **$14.00**

ELEMENTARY NUMBER THEORY

By E. LANDAU

The present work is a translation of Prof. Landau's famous *Elementare Zahlentheorie*, with added exercises by Prof. Paul T. Bateman.

—1958. 256 pp. 6x9. [125] **$4.95**

GRUNDLAGEN DER ANALYSIS

By E. LANDAU

The student who wishes to study mathematical German will find Landau's famous *Grundlagen der Analysis* ideally suited to his needs.

Only a few score of German words will enable him to read the entire book with only an occasional glance at the Vocabulary! [A COMPLETE German-English vocabulary, prepared with the novice especially in mind, has been appended to the book.]

—3rd ed. 1960. 173 pp. 5⅜x8. [24] Cloth **$3.50**
[141] Paper **$1.95**

FOUNDATIONS OF ANALYSIS

By E. LANDAU

"Certainly no clearer treatment of the foundations of the number system can be offered. . . . One can only be thankful to the author for this fundamental piece of exposition, which is alive with his vitality and genius."*—J. F. Ritt, Amer. Math. Monthly.*

—2nd ed. 1960. 6x9. [79] **$3.95**

ELEMENTS OF ALGEBRA

By HOWARD LEVI

"This book is addressed to beginning students of mathematics.... The level of the book, however, is so unusually high, mathematically as well as pedagogically, that it merits the attention of professional mathematicians (as well as of professional pedagogues) interested in the wider dissemination of their subject among cultured people . . . a closer approximation to the right way to teach mathematics to beginners than anything else now in existence."—*Bulletin of the A. M. S.*

—4th ed. 1962. 189 pp. 5⅜x8. [103] **$3.50**

THE THEORY OF MATRICES

By C. C. MacDUFFEE

"No mathematical library can afford to be without this book."—*Bulletin of the A. M. S.*

—(Ergeb. der Math.) 2nd edition. 116 pp. 6x9. Orig. publ. at $5.20. [28] **$2.95**

COMBINATORY ANALYSIS, Vols. I and II

By P. A. MACMAHON

TWO VOLUMES IN ONE.

A broad and extensive treatise on an important branch of mathematics.

—xx + 300 + xx + 340 pp. 5⅜x8. [137] Two vols. in one. **$7.50**

MACMAHON, "Introduction . . . ," see Klein

FORMULAS AND THEOREMS FOR THE FUNCTIONS OF MATHEMATICAL PHYSICS

By W. MAGNUS and F. OBERHETTINGER

Gathered into a compact, handy and well-arranged reference work are thousands of results on the many important functions needed by the physicist, engineer and applied mathematician.

Translated by J. WERMER.

—1954. 182 pp. 6x9. [51] **$3.90**

THEORY OF NUMBERS

By G. B. MATHEWS

CHAPTER HEADINGS: I. Elementary Theory of Congruences. II. Quadratic Congruences. III. Binary Quadratic Forms; Analytical Theory. IV. Binary Quadratic Forms; Geometrical Theory. V. Generic Characters of Binary Quadratics. VI. Composition of Forms. VII. Cyclotomy. VIII. Determination of Number of Improperly Primitive Classes for a Given Determinant. IX. Applications of the Theory of Quadratic Forms. X. The Distribution of Primes.

A reprint of the first edition, with correction of errata and some improvements of notation.

—2nd ed. 1892-1962. xii+323 pp. 5⅜x8. [156] **$3.95**

THE DEVELOPMENT OF MATHEMATICS IN CHINA AND JAPAN

By Y. MIKAMI

"Filled with valuable information. Mikami's [account of the mathematicians he knew personally] is an attractive features."
—*Scientific American.*

—1913-62. x + 347 pp. 5⅜x8. [149] **$4.95**

KURVENTHEORIE

By K. MENGER

—1932-63. vi+376 pp. 5⅜x8¼. [172] **In prep.**

GEOMETRIE DER ZAHLEN

By H. MINKOWSKI

—viii + 256 pp. 5½x8¼. [93] **$4.50**

DIOPHANTISCHE APPROXIMATIONEN

By H. MINKOWSKI

—viii + 235 pp. 5¼x8¼. [118] **$4.50**

MORDELL, "Fermat's Last Theorem," see *Klein*

INVERSIVE GEOMETRY

By F. MORLEY and F. V. MORLEY

—xi + 273 pp. 5¼x8¼. [101] **$3.95**

INTRODUCTION TO NUMBER THEORY

By T. NAGELL

A special feature of Nagell's well-known text is the rather extensive treatment of Diophantine equations of second and higher degree. A large number of non-routine problems are given.

—1951-64. Corr. repr. of 1st ed. 309 pp. 5⅜x8. [163] Prob. **$4.95**

THE THEORY OF SUBSTITUTIONS

By E. NETTO

Partial Contents: CHAP. I. Symmetric and Alternating Functions. II. Multiple- valued Functions and Groups of Substitutions. III. The Different Values of a Multiple-valued Function and their Algebraic Relation to One Another. IV. Transitivity and Primitivity; Simple and Compound Groups; Isomorphism. V. Algebraic Relations between Functions Belonging to the Same Group . . . VII. Certain Special Classes of Groups. VIII. Analytical Representation of Substitutions. The Linear Group. IX. Equations of Second, Third, Fourth Degrees. Groups of an Equation. X. Cyclotomic Equations. XI. Abelian Equations . . . XIII. Algebraic Solution of Equations. XIV. Group of an Algebraic Equation. XV. Algebraically Solvable Equations.

—In prep. Corr. repr. of 1st ed. 310 pp. 5⅜x8. Prob. **$3.95**