THE THEORY OF GROUPS

BY
HANS ZASSENHAUS

TRANSLATED FROM THE GERMAN
BY
SAUL KRAVETZ

CHELSEA PUBLISHING COMPANY
231 WEST 29th STREET, NEW YORK 1, N. Y.
1949

PRINTED IN THE UNITED STATES OF AMERICA

EDITOR'S PREFACE

Zassenhaus' *Lehrbuch der Gruppentheorie*, with its "van der Waerden approach," has been the modern classic of discrete group theory ever since its first appearance twelve years ago. With this book now in English, it will be possible for the beginning student of groups to view them against the background of modern algebra, and to see how its spirit of generality applies, without stepping outside of his own language or rummaging through the journals to do so.

The first chapter is somewhat condensed and seems to be intended as much for establishing the author's point of view by a review of fundamentals as for serving as a starting point for those unacquainted with modern algebra. An elegant treatment of finite rotation groups and a way of reading off the associative law from the group table are highlights of the chapter.

In Chapter II the treatment of linear associative algebras (Hypercomplex systems), rings, the application of "rings" without commutative addition to permutation groups, and structure theorems of Ore firmly establish the connection between groups and modern algebra.

The theorems of Fitting and Schmidt-Remak on decompositions, and elementary divisor theory applied to abelian groups, further establish this connection in Chapter III, where group extensions and the rôle of retracts in that theory are also treated.

In the chapter on p-groups (Chapter IV) work of P. Hall, Wieland, Reidemeister and others is included, and results on some infinite groups are obtained.

In Chapter V the representation of groups by monomial matrices with coset entries leads to representations by their determinants and hence to the important notion of *transfer* (Verlagerung). This concept and others of recent origin lead to simplified statements and proofs of some of the more difficult classical theorems of Burnside. A principal ideal theorem for group theory forms a fitting close to the book.

The bibliography at the end has been supplemented in order to help the reader acquaint himself with *some* of the more recent investigations of the topics introduced in the book.

In some spots the text has been altered slightly for clarity, but these are few,and the translator has preserved as much as possible the succinct style and flavor of the original German.

The editor wishes to thank Mr. A. Fass and Mr. F. Steinhardt for their very valuable help.

Alfred W. Jones

PREFACE

Investigations published within the last fifteen years have greatly deepened our knowledge of groups and have given wide scope to group-theoretic methods. As a result, what were isolated and separate insights before, now begin to fit into a unified, if not yet final, pattern. I have set myself the task of making this pattern apparent to the reader, and of showing him, as well, in the group-theoretic methods, a useful tool for the solution of mathematical and physical problems.

It was a course by E. Artin, given in Hamburg during the Winter Semester of 1933 and the Spring Semester of 1934, which started me on an intensive study of group theory. In this course, the problems of the theory of finite groups were transformed into problems of general mathematical interest. While any question concerning a single object [e.g., finite group] may be answered in a finite number of steps, it is the goal of research to divide the infinity of objects under investigation into classes of types with similar structure.

The idea of O. Hölder for solving this problem was later made a general principle of investigation in algebra by E. Nöther. We are referring to the consistent application of the concept of homomorphic mapping. With such mappings one views the objects, so to speak, through the wrong end of a telescope. These mappings, applied to finite groups, give rise to the concepts of normal subgroup and of factor group. Repeated application of the process of diminution yields the composition series, whose factor groups are the finite simple groups. These are, accordingly, the bricks of which every finite group is built. How to build is indicated—in principle at least—by Schreier's extension theory. The Jordan-Hölder-Schreier theorem tells us that the type and the number of bricks is independent of the diminution process. The determination of all finite simple groups is still the main unsolved problem.

After an exposition of the fundamental concepts of group theory in Chapter I, the program calls for a detailed investigation of the concept of homomorphic mapping, which is carried out in Chapter II. Next, Chapter III takes up the question of how groups are put together from their simple components. According to a conjecture of Artin, insight into the nature of simple groups must depend on further research on p-groups. The elements of the theory of p-groups are expounded in

Chapter IV. Finally, Chapter V describes a method by which solvable factor groups may be split off from a finite group.

For the concepts and methods presented in Chapter II, particularly those in § 7, one may also consult v. d. Waerden, *Moderne Algebra* I (Berlin 1937). [English translation: *Modern Algebra*, New York, 1949]. The first part of Chapter III follows a paper by Fitting, while the proof of the basis theorem for abelian groups, and Schreier's extension theory, are developed on the basis of a course by Artin. The presentation of the theory of p-groups makes use of a paper by P. Hall. The section on monomial representations and transfers into a subgroup has also been worked out on the basis of a course by Artin. In addition one should consult the bibliography at the end of the book.

Many of the proofs in the text are shorter and—I hope—more transparent than the usual, older, ones. The proof of the Jordan-Hölder-Schreier theorem, as well as the proofs in Chapter IV, §§ 1 and 6, owe their final form to suggestions of E. Witt.

I am grateful to Messrs. Brandt, Fitting, Koethe, Magnus, Speiser, Threlfall and v. d. Waerden for their valuable suggestions in reading the manuscript. I also wish to thank Messrs. Hannink and Koluschnin for their help.

The group-theoretic concepts taken up in this book are developed from the beginning. The knowledge required for the examples and applications corresponds to the contents, say, of the book by Schreier and Sperner, *Analytische Geometrie und Algebra*, Part I (Leipzig, 1935) [English translation: *Analytic Geometry and Algebra*, Chelsea Publishing Company, New York, *in prep.*]. A historic introduction to group theory may be found in the book by Speiser: *Theorie der Gruppen von endlicher Ordnung* (Berlin, 1937) [also New York, 1944].

I would suggest to the beginner that he familiarize himself first with Chapters I and II, Chapter III, §§ 1, 3, 4, 6, and 7, and Chapter IV, §§ 1 and 3, and also with the corresponding exercises. Then the program outlined in this preface will become clear to him.

Hamburg, October 1937 ***HANS ZASSENHAUS***

TABLE OF CONTENTS

IV. Sylow p-groups and p-groups

V. Transfers into a subgroup

I. ELEMENTS OF GROUP THEORY

§ 1. The Axioms of Group Theory

DEFINITION: A *group* is a set in which an operation called multiplication is defined under which there corresponds to each ordered pair x, y of elements of the set a unique third element z of the set. z is called the *product* of the factors x and y, written $z = xy$. For this multiplication we have

I. *The associative law:* $a(bc) = (ab)c$.

II. *The existence of a left identity* e *with the property* $ea = a$ *for all elements* a *of the group.*

III. *The solvability of the equation* $xa = e$ *for all elements* a *of the group.*

The associative law states that a product of three factors is determined solely by the order of its factors, its value being independent of the insertion of parentheses.

We assert: A product of arbitrarily many factors is determined solely by the order of its factors.

In order to prove this, let n be a number greater than three and assume the statement true for products of fewer than n factors. We write, for every $m < n$, a product of m factors $a_1, a_2, \ldots, a_m$ —in that order—as $P = a_1 \cdot a_2 \cdot \ldots \cdot a_m$ and have thus designated, unambiguously, an element of the group.

Now let P be a product of the n factors $a_1, a_2, \ldots, a_n$. After all of the parentheses have been removed except the last two pairs, P can be decomposed into two factors

$$P_1 = a_1 \cdot a_2 \cdot \ldots \cdot a_m$$

and

$$P_2 = a_{m+1} \cdot \ldots \cdot a_n,$$

with $0 < m < n$. We shall show that P is equal to the particular product $a_1 \cdot (a_2 \cdot \ldots \cdot a_n)$ and so we may assume $m > 1$. Then

$$\begin{aligned} P = P_1 P_2 &= (a_1 \cdot \ldots \cdot a_m)(a_{m+1} \cdot \ldots \cdot a_n) \\ &= (a_1 (a_2 \cdot \ldots \cdot a_m))(a_{m+1} \cdot \ldots \cdot a_n) \\ &= a_1 ((a_2 \cdot \ldots \cdot a_m)(a_{m+1} \cdot \ldots \cdot a_n)) \\ &= a_1 (a_2 \cdot \ldots \cdot a_n) \ . \end{aligned}$$

A non-empty system of elements in which multiplication is defined and is associative is called a *semi-group*.

For example the natural numbers form a semi-group under ordinary multiplication or addition as the operation.

The rational integers (positive, negative, and zero) form an additive group and a multiplicative semi-group. The rational numbers different from zero form a multiplicative group. All rational numbers form an additive group.

We assert that in a group every left unit e is also a right unit, (i.e., $ae=a$ holds for all group elements a.) In order to prove this, we solve $xa=e$ and $yx=e$. Then

$$(yx)a = ea = a$$
$$= y(xa) = ye = y(ee) = (ye)e = ae.$$

Similarly, $ye=y$, hence $y=a$, $ax=xa=e$.

We call one of the solutions of the equation $xa=e$ the *inverse element* of a and denote it by a^{-1}. Thus

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

If $xa=b$, then on right multiplication by a^{-1}, it follows that

$$ba^{-1}=(xa)a^{-1}=x(aa^{-1})=xe=x.$$

Conversely $ba^{-1}\cdot a=b\cdot a^{-1}a=be=b$. Thus the equation $xa=b$ has one and only one solution, $x=ba^{-1}$. Similarly it follows that the equation $ay=b$ has one and only one solution, $y=a^{-1}b$.

Multiplication in a group has a unique inverse.

The element e is called the identity or unit element of the group. It is uniquely determined as the solution of either of the equations $ax=a$ or $ya=a$. Similarly the inverse a^{-1} of the element a is uniquely determined as the solution of the equation $xa=e$ or $ay=e$.

The product of n equal factors a is denoted by a^n. Furthermore, if we set $a^0=e$, $a^1=a$ and $a^{-n}=(a^{-1})^n$ then the two power rules

$$a^n\cdot a^m=a^{n+m},$$
$$(a^n)^m=a^{nm},$$

are valid for arbitrary integral exponents n, m, as can be shown by induction.

Axioms II. and III. are not symmetric; they can be replaced by the two symmetric axioms:

II. a. *A group is non-empty.*

III. a. *Multiplication has an inverse, i.e., the equations*

$$xa = b$$

and

$$ay = b$$

are solvable for all pairs of elements a, b *of the group.*

Obviously II. a. is an immediate consequence of II., and III. a. follows from I.-III. If, conversely, I., II. a., III. a. are assumed, then we can find an element a in the given set and solve the equations $ea = a$, $ay = b$. From this it follows that

$$eb = e(ay) = (ea)y = ay = b$$

for all elements b.

Thus II. is valid. III. is a consequence of III. a.

A group which consists of a finite number of elements is called a *finite group*. The number of its elements is called its *order*. The order of an infinite group is defined to be zero.

In every group the *cancellation laws* hold:

III. b. $ax = ay$ *implies* $x = y$.

III. c. $xa = ya$ *implies* $x = y$.

THEOREM 1: *A finite semi-group in which the cancellation laws hold is a group.*

In order to prove this, let $a_1, a_2, \ldots, a_n$ be the finite number of elements and let a be a particular element. From III. b. it follows that the n elements $aa_1, aa_2, \ldots, aa_n$ are all distinct and so $ay = b$ is solvable for every pair a, b in the semi-group. The solvability of $xa = b$ follows similarly from the other cancellation law.

An abstract group is completely known if each of its elements is represented by a symbol and the product of any two symbols in any given order is exhibited.

The multiplication rule is given conveniently by a square table, in which the products in a row have the same left factor and the products in a column have the same right factor.

The multiplication tables of groups having at most three elements are the following:

Z_1

	e
e	e

Z_2

	e	a
e	e	a
a	a	e

Z_3

	e	a	b
e	e	a	b
a	a	b	e

The different multiplication tables of a group can be transformed into one another by row interchanges and column interchanges.

The existence of unique inverses is equivalent to the fact that each group element occurs exactly once in every row and column.

In order to exhibit[1] the associative law we agree to put the unit element of the group in the upper left corner of the square table. If we call the row starting with a, the a-row, and the column headed by b the b-column, then we find the product of a by b at the intersection of the a-row and b-column. The initial elements of each row and column may thus be omitted.

A table, constructed as above, is called *normal*, if in addition every element of the main diagonal is the identity element of the group. For example, the normal multiplication tables for groups of four and five elements are as follows:

Z_4

e	a	b	c
c	e	a	b
b	c	e	a
a	b	c	e

$\mathfrak{V}_4$

e	a	b	c
a	e	c	b
b	c	e	a
c	b	a	e

Z_5

e	a	b	c	d
d	e	a	b	c
c	d	e	a	b
b	c	d	e	a
a	b	c	d	e

The element a_{ik} at the intersection of i-th row and the k-th column is $a_{i1}a_{k1}^{-1}$, so that the rectangle rule

$$a_{ik}a_{kl} = a_{il}$$

holds. This may be seen from the following section of the table:

$$\begin{array}{ccc} a & \cdots\cdots & e \\ \vdots & & \vdots \\ ab & \cdots\cdots & b \end{array}$$

The rectangle rule is equivalent to the associative law.

The problem of abstract group theory is to examine all multiplication tables in which Axioms I.-III. are satisfied.

§ 2. Permutation Groups

For finite groups, the problem stated at the close of the last section can be solved by trial. For example, it can easily be established that the

[1] Brandt, Über eine Verallgemeinerung des Gruppenbegriffs, *Math. Ann.* 96 (1927) p. 365.

only multiplication tables for groups whose order is at most five are those which we have given previously. We can see, however, even from these first examples, that the direct verification of the associative law is time-consuming.

We must look about for more serviceable realizations of abstract groups. Naturally we require that the multiplication table be determined easily from the realization. An example of a domain in which arbitrary abstract groups can be realized is the group of permutations of a set of objects.

We denote single-valued mappings of a given set $\mathfrak{M}$ onto itself by lower case Greek letters, and elements of the set itself by lower case Roman letters. Let πx be the image of x under the mapping π. Any two single-valued mappings π, ϱ can be combined into a third single-valued mapping $\pi\varrho$ according to the rule $(\pi\varrho)x = \pi(\varrho x)$. The associative law is valid for this relation, since

$$(\pi(\varrho\sigma))x = \pi((\varrho\sigma)x) = \pi(\varrho(\sigma x)) = (\pi\varrho)(\sigma x) = ((\pi\varrho)\sigma)x.$$

The identity mapping $\underline{1}$, defined by $\underline{1}\, x = x$, is the unit element of this multiplicative set of mappings.

The single-valued mappings of a set onto itself form a semi-group with unit element.

A one-to-one mapping of a given set onto itself is called a permutation.

A permutation is a single-valued mapping π, for which $\pi x = a$ is solvable for every a and for which $\pi x = \pi y$ implies $x = y$. Therefore $\pi x = a$ is uniquely solvable for every a, and the solution is designated by $\pi^{-1}a$. $\pi(\pi^{-1}a) = a$, for every a. Therefore $\pi\pi^{-1} = \underline{1}$. Similarly $\pi^{-1}(\pi a) = a$, and therefore $\pi^{-1}\pi = \underline{1}$. Conversely, if the single-valued mapping π has an inverse mapping π^{-1}, defined by $\pi\pi^{-1} = \pi^{-1}\pi = \underline{1}$, then π is a permutation, since the equation $\pi x = a$ has the solution $\pi^{-1}a$ and $\pi x = \pi y$ implies $\pi^{-1}\pi x = \pi^{-1}\pi y$ and therefore $x = y$.

The inverse of the permutation π is the permutation π^{-1}; and if π, ϱ are two permutations, then the two-sided (i.e., right and left) inverse of $\pi\varrho$ is $\varrho^{-1}\pi^{-1}$. We conclude that the totality of permutations of the objects of a set form a group.

In order to see at a glance the effect of a single-valued mapping π we write it

$$\begin{pmatrix} x, & y, & \dots \\ \pi x, & \pi y, & \dots \end{pmatrix} \qquad (\textit{functional notation}).$$

Here $x, y, \ldots$ run through the elements of the given set in any order. Under every element is placed its image element. A shorter functional notation for π is $\begin{pmatrix} x \\ \pi x \end{pmatrix}$. Multiplication is indicated by

$$\begin{pmatrix} x \\ \varrho x \end{pmatrix}\begin{pmatrix} x \\ \pi x \end{pmatrix} = \begin{pmatrix} x \\ \varrho(\pi x) \end{pmatrix}. \quad *$$

π is a permutation, then, if and only if every element of $\mathfrak{M}$ occurs exactly once in the lower row of the parenthesis symbol indicated above.

$\pi = \begin{pmatrix} x\,y, & \cdots \\ \pi x, \pi y, & \ldots \end{pmatrix} = \begin{pmatrix} x \\ \pi x \end{pmatrix}$, which indicates the mapping $x \to \pi(x)$.

Then $\pi^{-1} = \begin{pmatrix} \pi x, & \pi y, & \ldots \\ x, & y, & \ldots \end{pmatrix} = \begin{pmatrix} \pi x \\ x \end{pmatrix}$.

Groups whose elements are permutations of a given set and are also multiplied like the permutations, are called permutation groups.

THEOREM 2: *Every group can be represented as a permutation group* (Cayley).

Proof: We take the permuted objects to be the elements of the group. The mapping $\pi_a = \begin{pmatrix} x \\ ax \end{pmatrix}$ is a permutation since $ax = b$ has a unique solution x . From the associative law it follows that the corresponding permutations multiply like the group elements. Since $\pi_a e = a$, the correspondence $\pi_a \longleftrightarrow a$ is one-to-one. The parenthesis notation for π_a is derived from the multiplication table of the group by writing the a-row under the e-row. This permutation group is called the (left) regular permutation group of the given abstract group.

The group of all permutations of a finite set of n things is denoted by $\mathfrak{S}_n$ and is called the symmetrical group on n objects. The permuted objects may be numbered from 1 to n , and we may think not of the permuted objects themselves but merely of their numbers. The latter are permuted just as the objects to which they correspond. Every permutation may be written uniquely as $\begin{pmatrix} 1, & 2, & \ldots, & n \\ i_1, & i_2, & \ldots, & i_n \end{pmatrix}$, where $i_1, i_2, \ldots, i_n$ run through the n integers $1, 2, \ldots, n$ in a definite order. We shall refer to these n consecutive integers hereafter as the *ciphers* of the permutation. Since there are $n!$ permutations of n elements, $\mathfrak{S}_n$ has the order $n!$.

* *Editor's note:* Since these permutations are mappings applied as operators from the *left* it follows that in the product $\varrho\pi$ the permutation π is followed by the permutation ϱ. This is contrary to the order used by such authors as Burnside, Speiser, and Dubreil.

The permutations of n ciphers can be written still more simply in cycle notation.

A permutation π is called d-cycle if π permutes cyclically a certain set of d ciphers $i_1, i_2, \ldots, i_d$:

$$\pi i_m = i_{m+1}, \quad \pi i_d = i_1 \ (m = 1, 2, \ldots, d-1)$$

and if π leaves every other cipher fixed. For example

$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$ is a 2-cycle (transposition) and

$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$ is a 3-cycle .

We may then denote the d-cycle by $(i_1, i_2, \ldots, i_d)$.However the same d-cycle has d different cycle notations, one for each different initial symbol.

Every permutation of n ciphers can be written as the product of disjoint cycles (i.e., cycles having no cipher in common).

For example $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 2 & 1 \end{pmatrix} = (15)(234)$. This decomposition is naturally unique up to the order of factors, as regards the set of elements in any cycle.

In order to prove the above, let π be a permutation of n ciphers $1, 2, \ldots, n$. Among the $n+1$. ciphers $1, \pi 1, \ldots, \pi^n 1$ certainly two are equal. Let $\pi^i 1 = \pi^k 1$ with $i > k \geqq 0$ be the first equation of this sort. If $k > 0$, then we could conclude that $\pi^{i-1} 1 = \pi^{k-1} 1$. Therefore $k = 0$ and $z_1 = (1, \pi 1, \ldots, \pi^{i-1} 1)$ is an i-cycle. Now we construct a cycle z_2 containing a cipher not occuring in z_1 . Continue this process. z_2 must be disjoint from z_1 and since finally all the ciphers are used, π is a product of disjoint cycles.

(1) represents uniquely the identical permutation $\underline{1}$. If the 1-cycles are deleted from the set of other permutations in $\mathfrak{S}_n$, then the cycle notation remains unambiguous, e.g.,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 3 & 5 \end{pmatrix} = (12)(34)(5) = (12)(34).$$

Multiplication of permutations in cycle notation can easily be carried out. E.g., to calculate(123) (45) (234), proceed as follows: The cycle farthest to the right containing 1 indicates $1 \to 2$. The cycle farthest to the right containing 2 indicates $2 \to 3$. The one farthest to right containing 3, but to the left of the one just used, gives $3 \to 1$. Hence (12) is one cycle of the product. Continuing to work from right

to left,* $3 \to 4 \to 5$, $5 \to 4$, $4 \to 2 \to 3$, giving **(354)**. Hence

(123) (45) (234) = (12) (354).

The simplest non-identical permutations are the transpositions.

Every permutation of n ciphers is a product, the factors being among the n-1 transpositions $(1, 2), (2, 3), \ldots, (n\text{-}1, n)$,

i.e. *every interchange of n ciphers can be arrived at by interchange of neighboring ciphers.*

This follows from

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

and

(2) $$(i_1, i_2, \ldots, i_m) = (i_1, i_2)(i_2, i_3), \ldots, (i_{m-1}, i_m).$$

DEFINITION: *A permutation of $n > 1$ ciphers is called even or odd according to whether the number*

$$\varepsilon_\pi = \prod_{i<k} \frac{\pi k - \pi i}{k - i} \qquad \text{(here } \prod \text{ indicates ordinary product)}$$

is equal to $+1$ *or* -1.

If π and ϱ are two permutations in $\mathfrak{S}_n$, then

$$\varepsilon_{\varrho\pi} = \prod_{i<k} \frac{\varrho\pi k - \varrho\pi i}{k - i} = \prod_{i<k} \frac{\varrho\pi k - \varrho\pi i}{\pi k - \pi i} \cdot \prod_{i<k} \frac{\pi k - \pi i}{k - i} = \varepsilon_\varrho \cdot \varepsilon_\pi.$$

Thus all the even permutations form a group. It is called the alternating permutation group of n ciphers and is denoted by $\mathfrak{A}_n$. The transposition $(j, j+1)$ is an odd permutation as can immediately be seen. A permutation is even or odd according to whether it is the product of an even or odd number of transpositions.

From (1) and (2) it follows that an m-cycle is even or odd according to whether m is odd or even. An arbitrary permutation is even or odd according to whether the number of cycles with an even number of members in its decomposition is even or odd.

To every even permutation π there corresponds an odd permutation $(12)\pi$, and this correspondence is one-to-one, i.e., there are as many even as odd permutations.

The alternating permutation group on n ciphers thus has order $\frac{1}{2}n!$.

* *Editor's Note:* In Burnside, Speiser, et al., the procedure would be to start from the left and work to the right.

§ 3. Investigation of Axioms

If the e-row is made equal to the e-column by means of appropriate row and column interchanges in the multiplication tables of § 1, then for these special cases the tables are symmetric about the main diagonal. In a group whose order is less than 6 the equation $ab = ba$ is valid.

We call a group *abelian* (or *commutative*) if the commutative law

IV. $ab = ba$ holds.

In an abelian group a product of n factors is uniquely determined by its factors, irrespective of order and insertion of parentheses.

We must show that $a_1 \cdot a_2 \cdot \ldots \cdot a_n = a_{i_1} \cdot a_{i_2} \cdot \ldots \cdot a_{i_n}$, where $\begin{pmatrix} 1, & 2, & \ldots, & n \\ i_1, & i_2, & \ldots, & i_n \end{pmatrix}$ is a permutation. Since every interchange of n factors can be effected by the interchange of neighboring factors, we merely have to prove that

$$a_1 \cdot a_2 \cdot \ldots \cdot a_i \cdot a_{i+1} \cdot \ldots \cdot a_n = a_1 \cdot a_2 \cdot \ldots \cdot a_{i+1} \cdot a_i \cdot \ldots \cdot a_n$$

This follows from the associative and commutative laws.

In general, groups are non-commutative, e.g., $\mathfrak{S}_3$ has a multiplication table which is not symmetric:

	e	a	b	c	d	f
e	e	a	b	c	d	f
(123) $= a$	a	b	e	d	f	c
(132) $= b$	b	e	a	f	c	d
(12) $= c$	c	f	d	e	b	a
(13) $= d$	d	c	f	a	e	b
(23) $= f$	f	d	c	b	a	e

The independence of axiom IV. from the group axioms I.-III. is shown by the above example. Similarly we show that the axioms I.-III. are independent of one another.

1. III. does not follow from I., II. and the solvability of $ax = e$, e.g.,

	e	e'
e	e	e'
e'	e	e'

2. There are multiplicative domains in which II., III.a., IV. are valid but I. is not, e.g.,

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	c	d	f	e
b	b	c	e	f	a	d
c	c	d	f	e	b	a
d	d	f	a	b	e	c
f	f	e	d	a	c	b

we have

$(ab)b = f$

$a(bb) = a.$

§ 4. Subgroups

DEFINITION: A subset $\mathfrak{U}$ of a given group $\mathfrak{G}$ is called a *subgroup* if the elements of $\mathfrak{U}$ form a group with the multiplication defined for $\mathfrak{G}$.

$\mathfrak{G}$ and e are trivial subgroups of $\mathfrak{G}$. A subgroup different from $\mathfrak{G}$ is called a *proper subgroup*. A subgroup different from $\mathfrak{G}$ and e is called a *non-trivial subgroup*. A proper subgroup $\mathfrak{U}$ is called a *largest* (*maximal*) *subgroup* if there is no subgroup of $\mathfrak{G}$ containing $\mathfrak{U}$ and different from $\mathfrak{U}$ and $\mathfrak{G}$. The subgroup $\mathfrak{U}$ is called a *smallest* (*minimal*) *subgroup* if e is the largest proper subgroup of $\mathfrak{U}$.

DEFINITION: *Two elements a and b are called right congruent under $\mathfrak{U}$, if $a = bU$ where $U \in \mathfrak{U}$.*[1]) *Thus two elements are called right congruent if they differ by a factor on the right which is in $\mathfrak{U}$.* We denote the right congruence of a to b by $a \equiv b(\mathfrak{U}r)$. This symbol, $\equiv$, has the following three properties:

1. $a \equiv a$ (since $a = ae$, $e \in \mathfrak{U}$);
2. $a \equiv b$ implies $b \equiv a$ ($a = bU$ implies $b = aU^{-1}$);
3. $a \equiv b$, $b \equiv c$ implies $a \equiv c$ ($a = bU_1$, $b = cU_2$ implies $a = cU_2U_1$ where $U_2U_1 \in \mathfrak{U}$).

A right congruence may be multiplied on the right by a factor from $\mathfrak{U}$ and by any factor on the left. Thus from $a \equiv b(\mathfrak{U}r)$ it follows that $xa \equiv xb(\mathfrak{U}r)$ and conversely. Also either side of a right congruence may be multiplied on the right by an element of $\mathfrak{U}$.

All the elements congruent to an element a form the left coset* belonging to a. Every element of the group belongs to one and only one left coset. Since the mapping $U \to aU$ is one-one, there are as many elements in each left coset as there are in $\mathfrak{U}$. The number of different left cosets is called the *index* of $\mathfrak{U}$ in $\mathfrak{G}$, and is denoted by $\mathfrak{G}.\mathfrak{U}$.

[1] $U \in \mathfrak{U}$ is read: The element U belongs to the set $\mathfrak{U}$.

* The terms *residue class*, *coset* and *remainder class* are synonymous. (*Ed.*)

DEFINITION: *A system of elements which contains exactly one element from each left coset is called a system of right representatives.*

To each representative system of the cosets of $\mathfrak{G}$ there corresponds a mapping $G \to \bar{G}$, which maps each element G of $\mathfrak{G}$ onto its representative $\bar{G}$. A representative function of the left cosets of $\mathfrak{G}$ is characterized as a single-valued function $G \to \bar{G}$ defined on $\mathfrak{G}$ with the three properties

1. $\bar{\bar{G}} = \bar{G}$
2. $\bar{G}^{-1}G \in \mathfrak{U}$
3. $\overline{GU} = \bar{G}$ for all U belonging to $\mathfrak{U}$.

Furthermore the rule $\overline{HG} = \overline{H\bar{G}}$ is valid. Such a mapping will be called a *right representative function* of $\mathfrak{G}$ with respect to $\mathfrak{U}$, written $\mathfrak{G}(\mathfrak{U}r)$.

Let $\{a_i\}$ be a system of right representatives of $\mathfrak{G}$ with respect to $\mathfrak{U}$ and $\{b_k\}$ a system of right representatives of $\mathfrak{U}$ with respect to the subgroup $\mathfrak{U}$ of $\mathfrak{V}$. We will show that $\{a_i b_k\}$ is then a system of right representatives of $\mathfrak{G}$ with respect to $\mathfrak{V}$:

From $$a_i b_k \equiv a_l b_m (\mathfrak{V}r)$$
it follows that $$a_i b_k \equiv a_l b_m (\mathfrak{U}r),$$
whence $a_i \equiv a_l(\mathfrak{U}r)$. Hence $i = l$.
Therefore $a_i b_k \equiv a_i b_m(\mathfrak{V}r)$,
whence $b_k \equiv b_m(\mathfrak{V}r)$. Hence $k = m$.

If a belongs to $\mathfrak{G}$, then $a = a_i U$ has a solution $U \in \mathfrak{U}$, and $U = b_k \cdot V$ has a solution $V \in \mathfrak{V}$. Hence $a \equiv a_i b_k(\mathfrak{V}r)$, Q.E.D. We therefore have:

If $G \to \bar{G}$ is a representative function $\mathfrak{G}(\mathfrak{U}r)$ and $U \to \underline{U}$ a representative function $\mathfrak{U}(\mathfrak{V}r)$, then $G \to \overline{G} = \bar{G}\,\underline{\bar{G}^{-1}G}$ is a representative function

$$\mathfrak{G}(\mathfrak{V}r).$$

We see, then, that the formula $\mathfrak{G} : \mathfrak{V} = (\mathfrak{G} : \mathfrak{U})(\mathfrak{U} : \mathfrak{V})$ holds for indices. If $\mathfrak{G}$ is finite, then $\mathfrak{G} : e = \mathfrak{G} : 1$ is the order of $\mathfrak{G}$, and so the following relation holds:

$$\mathfrak{G} : 1 = (\mathfrak{G} : \mathfrak{U})(\mathfrak{U} : 1).$$

We state this relation in the form—

$$\textit{Number of cosets } \mathfrak{G}(\mathfrak{U}r) = \frac{\textit{Number of elements in group}}{\textit{Number of elements in subgroup}}$$

Thus the order of any subgroup divides the order of the group.

We call two elements a and b *left congruent* with respect to $\mathfrak{U}$ if $a = Ub$ with $U \in \mathfrak{U}$, and we write $a \equiv b(\mathfrak{U}l)$. The three rules mentioned above are also valid for the left congruence. Cancellation and multiplication on the right of a left congruence preserves the congruence. Either side of a left congruence may be altered on the left only by an element in $\mathfrak{U}$. The definitions of right coset and system of left representatives are analagous to those of left coset and system of right representatives.

A left residue (representative) function is characterized by the three properties:

1. $\bar{\bar{G}} = \bar{G}$
2. $G\bar{G}^{-1} \in \mathfrak{U}$
3. $\overline{UG} = G$

for all $U \in \mathfrak{U}$.

From the right congruence $a \equiv b(\mathfrak{U}r)$ follows the left congruence $a^{-1} \equiv b^{-1}(\mathfrak{U}l)$ and conversely. Therefore if $\{a_i\}$ is a system of left representatives, then $\{a_i^{-1}\}$ is a system of right representatives.

A group has just as many right residue classes as left residue classes with respect to a subgroup. Moreover,

THEOREM 3: *If the index of a group with respect to a subgroup is finite, then the right and left cosets have a common system of representatives.*

If $\mathfrak{U}$ is finite, then r right residue classes contain at most r left residue classes. The same is true if only $(\mathfrak{G} : \mathfrak{U}$ is finite, as follows from a remark on p. 37.

We shall prove the more general theorem:

THEOREM 4:[1] *If a set $\mathfrak{M}$ is subdivided into n disjoint classes in two ways and if any r classes of the first subdivision contain at most r classes of the second subdivision, then the two subdivisions have a common system of representatives.*

This is clear if $n = 1$. We shall employ induction on n, assuming $n \geqq 2$.

Let $\mathfrak{M} = \sum \mathfrak{A}_i = \sum \mathfrak{B}_i$ be the two subdivisions of $\mathfrak{M}$. A sum of r $\mathfrak{A}$-classes which contains r $\mathfrak{B}$-classes is called a fundamental set. $\mathfrak{M}$ is itself a fundamental set. We show next that the sum and the intersection

[1] I owe the simple proof of this theorem to a communication from Herr Willi Maak.

of two fundamental sets are also fundamental sets. Let $\mathfrak{N}_1$ and $\mathfrak{N}_2$ be fundamental sets containing r and s $\mathfrak{A}$-classes respectively. The intersection $\mathfrak{D}$ of $\mathfrak{N}_1$ and $\mathfrak{N}_2$ consists of d $\mathfrak{A}$-classes. Consequently the sum $\mathfrak{S}$ of $\mathfrak{N}_1$ and $\mathfrak{N}_2$ consists of $r+s-d$ $\mathfrak{A}$-classes. The number d' of $\mathfrak{B}$-classes lying in $\mathfrak{D}$ is by hypothesis at most d. Since r and s $\mathfrak{B}$-classes lie in $\mathfrak{N}_1$ and $\mathfrak{N}_2$ respectively, $\mathfrak{S}$ contains at least $r+s-d'$ $\mathfrak{B}$-classes. It follows from our hypothesis that $r+s-d' \leqq r+s-d$ and $d' \leqq d$. Therefore $d'=d$. Thus the intersection and the sum of two fundamental sets are also fundamental sets.

There is a smallest non-empty fundamental set $\mathfrak{N}$. There are an $\mathfrak{A}$-class, call it $\mathfrak{A}_1$, and a $\mathfrak{B}$-class, call it $\mathfrak{B}_1$, lying in $\mathfrak{N}$ and having an element a_1 in common. Let $\mathfrak{M}$ be formed by deleting $\mathfrak{A}_1$ and $\mathfrak{B}_1$ from $\mathfrak{M}$; let $\mathfrak{A}_i'$ be obtained from $\mathfrak{A}_i$ by deleting the intersection of $\mathfrak{A}_i$ with $\mathfrak{B}_1$ and let $\mathfrak{B}_i$ be obtained from $\mathfrak{B}_i$ by deleting the intersection of $\mathfrak{A}_1$ and $\mathfrak{B}_i$. $\mathfrak{M}'=\sum\mathfrak{A}_i'=\sum\mathfrak{B}_i'$ are two subdivisions of $\mathfrak{M}$ into $n-1$ disjoint classes where n is the number of $\mathfrak{A}$-classes in $\mathfrak{M}$.

If r $\mathfrak{A}'$ classes contain more than r $\mathfrak{B}'$-classes, then

$$\mathfrak{A}_2'+\mathfrak{A}_3'+\cdots+\mathfrak{A}_{r+1}' \geqq \mathfrak{B}_2'+\mathfrak{B}_3'+\cdots+\mathfrak{B}_{r+2}',$$

After adding $\mathfrak{A}_1$, it follows that

$$\mathfrak{A}_1+\mathfrak{A}_2+\cdots+\mathfrak{A}_{r+1} \geqq \mathfrak{B}_2+\mathfrak{B}_3+\cdots+\mathfrak{B}_{r+2}.$$

$\mathfrak{A}_1+\mathfrak{A}_2+\cdots+\mathfrak{A}_{r+1}$ is a fundamental set which contains $\mathfrak{A}_1'$. Since its intersection with the smallest fundamental set $\mathfrak{N}$ is non-empty, it contains $\mathfrak{N}$ and therefore also contains $\mathfrak{B}_1$. But then $\mathfrak{A}_1+\mathfrak{A}_2+\cdots+\mathfrak{A}_{r+1}$ would contain $r+2$ $\mathfrak{B}$-sets which is contrary to assumption. We can therefore apply the induction assumption to both subdivisions of $\mathfrak{M}'$; after appropriate numbering of the $\mathfrak{B}_i'$ we obtain a representative system $a_2, a_3, \ldots, a_n$ where $a_i \in \mathfrak{A}_i', \mathfrak{B}_i'$ for $i>1$. Finally $a_1, a_2, \ldots, a_n$ is the common representative system which was sought.

A Remark on Congruence Relations

A *congruence relation* is defined in a set if for two elements a, b of the set, one and only one of the following two relations holds:

a is congruent to b: $a \equiv b$

a is non-congruent to b: $a \not\equiv b$

A *normal congruence* satisfies the following three requirements:

1. (Reflexitivity) Every element is congruent to itself.
2. (Symmetry) The sides of a congruence may be interchanged: $a \equiv b$ implies $b \equiv a$.

3. (Transitivity) $a \equiv b$, $b \equiv c$ implies $a \equiv c$.

For example, the ordinary equality relation in the set is a normal congruence relation.

Exercise: To a normal congruence relation corresponds a decomposition of the given set into disjoint classes in accordance with the rule:

Exactly those elements of the set which are congruent to a are put into the class $\mathfrak{R}_a$. Two classes are regarded as equal if they are the same subset of the given set. Two classes having any element in common are equal.

Exercise: If the set $\mathfrak{M}$ has a decomposition $\mathfrak{M} = \sum_{i=1}^{\omega} \mathfrak{R}_i$ into disjoint non-empty subsets $\mathfrak{R}_i$, then this decomposition is the class decomposition which corresponds to the following normal congruence relation:

a is congruent to b if a and b lie in the same subset of the decomposition.

a is not congruent to b if a and b do not lie in same subset of the decomposition.

A subset $\mathfrak{S}$ of a given set $\mathfrak{M}$ is called a *residue system* relative to a normal congruence relation, if $\mathfrak{S}$ contains exactly one element from each class, this element being called the *representative* of the class.

We obtain the residue system by choosing an element from each class and forming the subset $\mathfrak{S}$ of $\mathfrak{M}$ consisting of precisely these chosen elements. Then there corresponds to every residue system $\mathfrak{S}$ a *representative function* which associates an $\bar{a}$ of $\mathfrak{S}$ to every element a in according to the rule: $\bar{a}$ is the element of $\mathfrak{S}$ congruent to a.

Exercise: A single valued function on a given set $\mathfrak{M}$, which maps a on $\bar{a}$, is a representative function if and only if $\bar{\bar{a}} = \bar{a}$.

Here, given the representative function, the congruence relation is defined by the rule:

a is congruent to b, if $\bar{a} = \bar{b}$;
a is non-congruent to b, if $\bar{a} \neq \bar{b}$.

Exercise: If the left cancellation rule: $ab \equiv ac$ implies $b \equiv c$, holds for a normal congruence relation in a group $\mathfrak{G}$, then the relation is a right congruence with respect to the subgroup $\mathfrak{U}$ which consists of all elements congruent to e.

If the right cancellation rule: $ba \equiv ca$ implies $b \equiv c$, holds, then the normal congruence is a left congruence with respect to the subgroup $\mathfrak{U}$ which consists of all the elements congruent to e.

§ 5. Cyclic Groups

A group is called *cyclic* if it can be generated by one of its elements through multiplication and the taking of inverses (i.e., the group consists precisely of the set of all powers of the element a, positive, negative and zero).

The group $\mathfrak{G}$ generated by a is denoted by (a). Every element of $\mathfrak{G}$ is a power of a.

We wish to determine the subgroups $\mathfrak{U}$ of a cyclic group $\mathfrak{G}$. If $\mathfrak{U}$ is different from (e), then $\mathfrak{U}$ contains a power of a with an exponent different from zero. Since, if a^m lies in $\mathfrak{U}$, a^{-m} does also, we can assume that for some $m > 0$, a^m lies in $\mathfrak{U}$. Let d be the smallest of these natural numbers m. Then $e, a, a^2, \ldots, a^{d-1}$ must be mutually non-congruent with respect to $\mathfrak{U}$; therefore $\mathfrak{G} : \mathfrak{U} \geqq d$. Every rational interger m can be put in the form $m = qd + r$ where the quotient q is a rational integer and the remainder r is a non-negative integer less than d. The element a^m in $\mathfrak{G}$ has the form $a^r \cdot (a^d)^q$, therefore $a^m \equiv a^r$ and $\mathfrak{G} : \mathfrak{U} \leqq d$. From the two inequalities it follows that $\mathfrak{G} : \mathfrak{U} = d$ and that $e, a, a^2, \ldots, a^{d-1}$ is a system of representatives of $\mathfrak{G}$ with respect to $\mathfrak{U}$. $\mathfrak{U}$ consists of all powers of a^d.

Every subgroup of a cyclic group is cyclic. The index of a subgroup different from e is finite, and for every divisor $d > 0$ of $\mathfrak{G} : 1$, there is only the one subgroup (a^d) of index d.

We shall see later that this last property characterizes the cyclic groups.

If $\mathfrak{G}$ has an order n different from zero, then two of the powers $a^0 = e, a, \ldots, a^n$ are equal. From $a^r = a^s$ it follows that $a^{r-s} = e$; thus a power of a with positive exponent lies in the subgroup e. Since $\mathfrak{G} : e = n$, we have $(a^n) = e$ and $\mathfrak{G}$ consists of the n elements $e, a, a^2, \ldots, a^{n-1}$.

n is the smallest positive number for which $a^n = e$. If $a^x = e$ then x is divisible by n.

DEFINITION: In an arbitrary group, the order of the cyclic subgroup generated by the element a is called the *order of the element* a. The order of an element is therefore either zero or the smallest positive number for which $a^n = e$.

The order of a group element is a divisor of the order of the group.

For a finite group of order N we have as a consequence the analog of the Fermat theorem, for groups:

$$a^N = e.$$

How can the order of a permutation in $\mathfrak{S}_n$ be read off from its decomposition into cycles?

If $\pi = (i_1, i_2, \ldots, i_d)$ is a d-cycle, then $\pi^d = \underline{1}$. If $0 < y < d$, then $\pi^y i_1 = i_{1+y} \neq i_1$, therefore $\pi^y \neq \underline{1}$. The order of a d-cycle is d. Now let $\pi = z_1 \cdot z_2 \cdot \ldots \cdot z_k$ be the cycle representation of π, where z_i is a d_i-cycle. If $\pi^d = \underline{1}$ then $z_i{}^d = \underline{1}$; thus d_i is a divisor of d. The least common multiple d' of all the d_i is a divisor of d. Since conversely $z_i{}^{d'} = \underline{1}$ and therefore $\pi^{d'} = \underline{1}$, we have:

The order of a permutation of n ciphers is equal to the least common multiple of the orders of cycles in its cycle representation.

§ 6. Finite Rotation Groups

As an example of the meaning of the previous concepts, let us examine the finite rotation groups.

The rotations of cartesian three-dimensional space about the fixed point O have the following properties:

1. Every rotation about O permutes the points of the unit sphere $\mathfrak{K}$ with center O and is uniquely determined by its effect on the points of the surface of the unit sphere.

2. Two rotations carried out consecutively produce a rotation.

If σ and τ are two rotations about O, then $\sigma\tau$ is the rotation which transforms the point P into the point $\sigma(\tau P)$.

3. A rotation either leaves all points on $\mathfrak{K}$ fixed or it leaves exactly two points fixed.

In the latter case, the two fixed points are called the *poles* of the rotation. The rotation which leaves all points fixed, is denoted by $\underline{1}$.

4. A rotation angle φ_σ is associated with every rotation σ; φ_σ is uniquely determined to within addition of an integral multiple of 2π. Two rotations σ, τ with two common fixed points satisfy $\varphi_{\sigma\tau} \equiv \varphi_\sigma + \varphi_\tau (2\pi)$

We wish to know which multiplication tables represent finite multiplicative domains $\mathfrak{G}$ of rotations.

Since $\mathfrak{G}$ consists of a finite number of permutations, $\mathfrak{G}$ is a finite group. The unit element of $\mathfrak{G}$ is $\underline{1}$. Let the number N of rotations in $\mathfrak{G}$ be greater than 1.

We say two points are *conjugate* under $\mathfrak{G}$ if there is a rotation in $\mathfrak{G}$ which sends one of the two points into the other. The finite number of poles of rotations in $\mathfrak{G}$ fall into classes of conjugate poles; let us call them $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_H$.

All the rotations in $\mathfrak{G}$ which have the same pole P, together with $\underline{1}$,

form a subgroup $\mathfrak{g}$. We call $\mathfrak{g}$ the subgroup belonging to P.

The p poles conjugate to P have the form $\sigma_1 P, \sigma_2 P, \ldots, \sigma_p P$ with $\sigma_i \in \mathfrak{G}$. If $\sigma \in \mathfrak{G}$ then $\sigma P = \sigma_i P$ is solvable, i.e.,

$$\sigma_i^{-1}.\ \sigma P = \underline{1} P = P,\ \sigma_i^{-1}\sigma \in \mathfrak{g},\ \sigma \equiv \sigma_i (\mathfrak{g} r).$$

Thus all the rotations in $\mathfrak{G}$ fall into p left cosets with respect to $\mathfrak{g}$ and these are determined by their effect on P. $\mathfrak{g}$ is one of these complexes and contains $n = N/p$ elements. P is called n-tuple pole in $\mathfrak{G}$.

If $\mathfrak{g}$ belongs to P, we determine the group belonging to τP.

If σ_1 is such that $\sigma_1 \tau P = \tau P$, it follows that $\tau^{-1}\sigma_1 \tau P = P$; therefore $\sigma = \tau^{-1}\sigma_1 \tau \in \mathfrak{g}$ and $\sigma_1 = \tau\sigma\tau^{-1}$. If $\sigma P = P$, then $\tau\sigma\tau^{-1}(\tau P) = \tau P$. Therefore the group $\tau\mathfrak{g}\tau^{-1}$ belongs to τP . In that account we also say: $\tau\sigma\tau^{-1}$ is *conjugate* to σ .

We determine the number of poles of rotations in $\mathfrak{G}$. There are exactly $2(N-1)$, since there are precisely $N-1$ non-identity rotations in $\mathfrak{G}$. On the other hand there are exactly $n_i = N/p_i$ rotations in $\mathfrak{G}$ which leave a pole of the i-th class fixed. Hence a totality of $p_i(n_i - 1)$ non-identical rotations leave *some* pole of the i-th class fixed.

Therefore $$2N - 2 = \sum_1^H p_i (n_i - 1),$$

i.e., $$2(1 - 1/N) = \sum_1^H (1 - 1/n_i).$$

From the further conditions $N \geqq n_i \geqq 2$ it follows that $2 \leqq H \leqq 3$. Furthermore

I. if $H = 2,\ n_1 = n_2 = N$ arbitrary > 1.

II. if $H = 3,\ 2 = n_1 \leqq n_2 \leqq n_3,\ n_2 \leqq 3$:

$n_1 = n_2 = 2,\ n_3 = N/2,$

$n_1 = 2,\ n_2 = n_3 = 3,\ N = 12,$

$n_1 = 2,\ n_2 = 3,\ n_3 = 4,\ N = 24,$

$n_1 = 2,\ n_2 = 3,\ n_3 = 5,\ N = 60.$

I. $H=2$: All rotations $\neq \underline{1}$ have the same poles. Let φ_σ be the smallest of all the positive rotation angles corresponding to rotations in $\mathfrak{G}$. If τ is any rotation in $\mathfrak{G}$ there exists a rational integer m such that $m\varphi_\sigma \leqq \varphi_\tau < (m+1)\varphi_\sigma$. Since $\varphi_{\sigma^{-1}} = -\varphi_\sigma,\ \varphi_{\sigma^m} = m\varphi_\sigma$, we have $0 \leqq \varphi_{\sigma - m\tau} < \varphi_\sigma$. Therefore $\varphi_{\sigma - m\tau} = 0$ and $\tau = \sigma^m$ because of property 4 of rotations.

$\mathfrak{G}$ is a cyclic group of order N generated by σ , where $\varphi_\sigma = 2\pi/N$, and is designated by Z_N .

II.a. $H = 3,\ n_1 = n_2 = 2,\ n_3 = N/2.$

$\mathfrak{P}_3$ consists of two poles P, Q, and therefore a rotation in $\mathfrak{G}$ either will leave both poles fixed or will interchange the poles; thus $\mathfrak{g}_P = \mathfrak{g}_Q$. $\mathfrak{G}$ decomposes into $\mathfrak{g}$ and $\tau\mathfrak{g}$; the square of any rotation σ in $\mathfrak{G}$, which does not lie in $\mathfrak{g}$, is $\underline{1}$, since it leaves the fixed points of σ fixed, and also leaves P and Q fixed.

From $\tau^2 = (\tau\sigma)^2 = \underline{1}$ for all σ in $\mathfrak{g}$, it follows that $\tau\sigma = \sigma^{-1}\tau$.

Therefore

$$\tau\sigma_1 \cdot \tau\sigma_2 = \sigma_1^{-1}\tau\tau\sigma_2 = \sigma_1^{-1}\sigma_2.$$

Since $\mathfrak{g}$ is cyclic, by I., the multiplication table of $\mathfrak{G}$ is uniquely determined by its order. The table on page 9 shows $\mathfrak{G}$ for $N=6$. $\mathfrak{G}$ is called a dihedral group and is denoted by D_N .

II.b. $n_1 = 2,\ n_2 = n_3 = 3,\ N = 12.$

The eleven rotations $\neq \underline{1}$ permute the four triple poles of the second (and third) class in 3-cycles and double transpositions. Thus $\mathfrak{G}$ is the alternating permutation group on the four triple poles of one of the latter two classes. $\mathfrak{G}$ is called the tetrahedral group.

II.c. $n_1 = 2,\ n_2 = 3,\ n_3 = 4,\ N = 24.$

The eight triple poles fall into four pairs of poles, such that a rotation in $\mathfrak{G}$ either has both poles of a pair as fixed points or else has neither. A rotation σ which takes each of the four pole pairs into itself has the identity as its square. If $\sigma \neq \underline{1}$, then σ interchanges the two poles in each pair and since, for every τ in $\mathfrak{G}$, $\tau\sigma\tau^{-1}$ has the same property, $\sigma\tau\sigma\tau^{-1} = \underline{1}$. If, however, τ is a rotation of order 3, then $\sigma\tau$ interchanges the poles of τ and consequently $\sigma\tau\sigma\tau = \underline{1}$. But this would give $\tau^{-1} = \tau,\ \tau^2 = 1$, a contradiction, and so σ must be $\underline{1}$ and $\mathfrak{G}$ is the symmetric permutation group of its four pair of triple poles. $\mathfrak{G}$ is called the octahedral group.

II.d. $n_1 = 2,\ n_2 = 3,\ n_3 = 5,\ N = 60.$

The 30 poles fall into 15 pairs of double poles, such that a rotation in $\mathfrak{G}$ leaves neither or both of the poles of each pair fixed. Let (PQ) be one of these pairs and let σ be a rotation $\neq \underline{1}$ in $\mathfrak{G}$ with poles P, Q.

There exists in $\mathfrak{G}$ a rotation τ which maps P onto Q. $\tau\sigma\tau^{-1}$ leaves the point Q fixed; therefore since Q is a double pole,

$$\tau\sigma\tau^{-1} = \sigma,\ \tau\sigma = \sigma\tau,\ Q \neq \tau Q = \tau\sigma Q = \sigma\tau Q.$$

Since τQ is a pole of σ, it follows that $\tau Q = P$. If conversely ϱ is a rotation in $\mathfrak{G}$ which leaves (PQ) fixed, then either ϱ or $\varrho\tau^{-1}$ leaves each of the points P, Q fixed. Of the elements of $\mathfrak{G}$ only $\underline{1}, \sigma, \tau, \sigma\tau$ leave

the pole-pair (PQ) fixed. These four rotations are exactly those rotations in $\mathfrak{G}$ *which commute with* σ. *The* square of a rotation in $\mathfrak{G}$ *which* leaves (PQ) fixed has more than two fixed points and therefore is $\underline{1}$. From this we conclude: If a pole-pair (PQ) remains fixed under a rotation in $\mathfrak{G}$, then the three rotations $\neq \underline{1}$, which leave PQ fixed, leave the pole-pairs of each of them fixed. In this way the 30 double poles fall into five sextuples of poles which are permuted by $\mathfrak{G}$. By their effect upon a sextuple, the 60 rotations of $\mathfrak{G}$ fall into five complexes, each consisting of twelve rotations. All the rotations which leave a sextuple fixed form a subgroup of order 12 which has double and triple poles only; therefore the subgroup is the tetrahedral group. This tetrahedral group is generated by its elements of order 3. If a rotation of order 3 leaves each of the five sextuples of poles fixed, then all the rotations in $\mathfrak{G}$ of order 3 have this property, since they are all conjugate to one another under $\mathfrak{G}$. Then all the rotations in the tetrahedral group which belong to a sextuple leave the whole sextuple fixed. A rotation of order 2 does not have this property. Therefore the 59 rotations $\neq \underline{1}$ in $\mathfrak{G}$ permute the five pole sextuples in either a 3-cycle, a 5-cycle, or a double transposition. $\mathfrak{G}$ is the alternating permutation group on its five sextuples of double poles. $\mathfrak{G}$ is called the icosahedral group.

The names of the last four types are related to the regular polyhedra whose vertices are poles of the third class. Geometrically it can be seen that $\mathfrak{G}$ consists of all the rotations of space which carry the corresponding regular polyhedron into itself. Conversely, from the existence of the regular polyhedra we can deduce the existence of the rotation groups named after them.

In cases b) – d), the poles of the second class are the vertices of the dual regular polyhedra: tetrahedron, hexahedron (cube), dodecahedron. If the poles of third (second) class are at the vertices of the regular polyhedron, then the poles of second (third) class lie on the lines from O to the midpoints of the faces.

The double poles of the first class lie on the lines from O to the midpoints of the edges. The five sextuples of double poles of the icosahedral group are similar to the five vertex sextuples of the five octahedra inscribed in the icosahedron.

§ 7. Calculus of Complexes

In order to know the structure of a given group $\mathfrak{G}$, we must investigate its subsets.

We call any subset of a semi-group $\mathfrak{G}$ a *complex*. Let the empty subset be denoted by 0.

The set-theoretic relations of complexes are expressed by means of the symbols $=, \subseteq, \subset, \cap, \cup, +, -$. The equality of two complexes is expressed by $\mathfrak{R}_1 = \mathfrak{R}_2$ i.e., $\mathfrak{R}_1$ and $\mathfrak{R}_2$ contain the same elements. The three well-known rules are valid for this equality relation.

$\mathfrak{R}_1 \subseteq \mathfrak{R}_2$ means that the complex $\mathfrak{R}_1$ is contained in the complex $\mathfrak{R}_2$, i.e., every element in $\mathfrak{R}_1$, lies in $\mathfrak{R}_2$. Equivalent to this is $\mathfrak{R}_2 \supseteq \mathfrak{R}_1$ i.e., $\mathfrak{R}_2$ contains $\mathfrak{R}_1$. We have the rules:

a) $\mathfrak{R} \subseteq \mathfrak{R}$

b) If $\mathfrak{R}_1 \subseteq \mathfrak{R}_2$ and $\mathfrak{R}_2 \subseteq \mathfrak{R}_3$ then $\mathfrak{R}_1 \subseteq \mathfrak{R}_3$.

The equality of two complexes $\mathfrak{R}_1, \mathfrak{R}_2$ is equivalent to: $\mathfrak{R}_1 \subseteq \mathfrak{R}_2$ and $\mathfrak{R}_2 \subseteq \mathfrak{R}_1$.

If the complex $\mathfrak{R}_1$ is a proper subset of $\mathfrak{R}_2$, we denote this condition by $\mathfrak{R}_1 \subset \mathfrak{R}_2$, i.e., $\mathfrak{R}_1$ lies in $\mathfrak{R}_2$ but there is an element in $\mathfrak{R}_2$ which is not in $\mathfrak{R}_1$. The following two rules are valid:

a) $\mathfrak{R} \not\subset \mathfrak{R}$.

b) $\mathfrak{R}_1 \subset \mathfrak{R}_2$, $\mathfrak{R}_2 \subset \mathfrak{R}_3$ imply $\mathfrak{R}_1 \subset \mathfrak{R}_3$.

The totality of all elements which lie simultaneously in n given complexes $\mathfrak{R}_1, \mathfrak{R}_2, \ldots, \mathfrak{R}_n$ is called the *intersection* of the $\mathfrak{R}_i$. It is denoted by $\mathfrak{R}_1 \cap \mathfrak{R}_2 \cap \mathfrak{R}_3 \cap \ldots \cap \mathfrak{R}_n$.

The following rules are valid for the intersection:

$$\mathfrak{R} \cap \mathfrak{R} = \mathfrak{R},$$

$$\mathfrak{R}_1 \cap \mathfrak{R}_2 = \mathfrak{R}_2 \cap \mathfrak{R}_1 \quad \text{(commutative law)}$$

$$(\mathfrak{R}_1 \cap \mathfrak{R}_2) \cap \mathfrak{R}_3 = \mathfrak{R}_1 \cap (\mathfrak{R}_2 \cap \mathfrak{R}_3) \qquad \text{(associative law)}$$

$$(\mathfrak{R}_1 \cap \mathfrak{R}_2 \cap \ldots \cap \mathfrak{R}_n) \cap (\mathfrak{R}_{n+1} \cap \ldots \cap \mathfrak{R}_{n+m}) = \mathfrak{R}_1 \cap \mathfrak{R}_2 \cap \ldots \cap \mathfrak{R}_{n+m}.$$

The inequality $\mathfrak{R}_1 \subseteq \mathfrak{R}_2$ is equivalent to $\mathfrak{R}_1 \cap \mathfrak{R}_2 = \mathfrak{R}_1$. $\mathfrak{R}_1 \subset \mathfrak{R}_2$ is equivalent to $\mathfrak{R}_1 \cap \mathfrak{R}_2 = \mathfrak{R}_1$ and $\mathfrak{R}_1 \neq \mathfrak{R}_2$.

If $\mathfrak{k}_i \subseteq \mathfrak{R}_i$, then $(\mathfrak{k}_1 \cap \mathfrak{k}_2) \subseteq (\mathfrak{R}_1 \cap \mathfrak{R}_2)$.

The totality of all elements that lie either in $\mathfrak{R}_1$ or in $\mathfrak{R}_2 \ldots$ or in $\mathfrak{R}_n$ is called the *sum* of $\mathfrak{R}_1, \mathfrak{R}_2, \ldots, \mathfrak{R}_n$. It is denoted by $\mathfrak{R}_1 \cup \mathfrak{R}_2 \cup \ldots \cup \mathfrak{R}_n$. The above four rules are valid if $\cap$ is replaced by $\cup$. The relation $\mathfrak{R}_1 \subseteq \mathfrak{R}_2$ is equivalent with $\mathfrak{R}_1 \cup \mathfrak{R}_2 = \mathfrak{R}_2$. $\mathfrak{R}_1 \subset \mathfrak{R}_2$ is equivalent with $\mathfrak{R}_1 \cup \mathfrak{R}_2 = \mathfrak{R}_2$ and $\mathfrak{R}_1 \neq \mathfrak{R}_2$. If $\mathfrak{k}_i \subseteq \mathfrak{R}_i$, then $\mathfrak{k}_1 \cup \mathfrak{k}_2 \subseteq \mathfrak{R}_1 \cup \mathfrak{R}_2$.
The relation between sum and intersection is distributive:

$$\mathfrak{R}_1 \cap (\mathfrak{R}_2 \cup \mathfrak{R}_3) = (\mathfrak{R}_1 \cap \mathfrak{R}_2) \cup (\mathfrak{R}_1 \cap \mathfrak{R}_3),$$

$$\mathfrak{R}_1 \cup (\mathfrak{R}_2 \cap \mathfrak{R}_3) = (\mathfrak{R}_1 \cup \mathfrak{R}_2) \cap (\mathfrak{R}_1 \cup \mathfrak{R}_3).$$

The sum of pairwise disjoint complexes $\mathfrak{R}_1, \mathfrak{R}_2, \ldots, \mathfrak{R}_n$ is denoted by $\mathfrak{R}_1 + \mathfrak{R}_2 + \cdots + \mathfrak{R}_n$.

The rules for the symbol $\cup$ remain valid if $+$ is substituted for $\cup$ everywhere and it is assumed that the sets on the left connected by the plus symbol are disjoint. The second distributive law is an exception.

If $\mathfrak{R}_1$ is contained in $\mathfrak{R}_2$, then the difference set, denoted by $\mathfrak{R}_2 - \mathfrak{R}_1$, consists of those elements of $\mathfrak{R}_2$which are not in $\mathfrak{R}_1$. It follows that: $\mathfrak{R}_2 = \mathfrak{R}_1 + (\mathfrak{R}_2 - \mathfrak{R}_1)$,and $\mathfrak{R}_2 - \mathfrak{R}_1$ is uniquely determined by this equation.

Beside these set-theoretic operations we also introduce the *product* of n complexes $\mathfrak{R}_1, \mathfrak{R}_2, \ldots, \mathfrak{R}_n$: $\mathfrak{R}_1 \cdot \mathfrak{R}_2 \cdot \ldots \cdot \mathfrak{R}_n$ is the set of all products $x_1 \cdot x_2 \cdot \ldots \cdot x_n$, where $x_i \in \mathfrak{R}_i$ and n is a positive integer. We have:

$$\mathfrak{R}_1 (\mathfrak{R}_2 \mathfrak{R}_3) = (\mathfrak{R}_1 \mathfrak{R}_2) \mathfrak{R}_3 = \mathfrak{R}_1 \mathfrak{R}_2 \mathfrak{R}_3 \quad \text{(the associative law)}.$$

The combination of product with sum or intersection satisfies

$$\mathfrak{R}_1 (\mathfrak{R}_2 \cap \mathfrak{R}_3) \subseteq \mathfrak{R}_1 \mathfrak{R}_2 \cap \mathfrak{R}_1 \mathfrak{R}_3,$$
$$\mathfrak{R}_1 (\mathfrak{R}_2 \cup \mathfrak{R}_3) = \mathfrak{R}_1 \mathfrak{R}_2 \cup \mathfrak{R}_1 \mathfrak{R}_3.$$

If $\mathfrak{k}_i \subseteq \mathfrak{R}_i$, then $\mathfrak{k}_1 \mathfrak{k}_2 \subseteq \mathfrak{R}_1 \mathfrak{R}_2$.

In a group $\mathfrak{G}$ we define the *inverse complex* of a non-empty complex as the complex consisting of all the inverses of the elements of $\mathfrak{R}$. It is denoted by $\mathfrak{R}^{-1}$.

$\mathfrak{R}\mathfrak{R}^{-1} \geq e$, but $\mathfrak{R}\mathfrak{R}^{-1} = e$ if and only if $\mathfrak{R}$ consists of exactly one element. Furthermore:

$$(\mathfrak{R}^{-1})^{-1} = \mathfrak{R}$$
$$(\mathfrak{R}_1 \cup \mathfrak{R}_2)^{-1} = \mathfrak{R}_1^{-1} \cup \mathfrak{R}_2^{-1},$$
$$(\mathfrak{R}_1 \cap \mathfrak{R}_2)^{-1} = \mathfrak{R}_1^{-1} \cap \mathfrak{R}_2^{-1},$$
$$(\mathfrak{R}_1 \cdot \mathfrak{R}_2)^{-1} = \mathfrak{R}_2^{-1} \cdot \mathfrak{R}_1^{-1},$$

and if $\mathfrak{k} \subseteq \mathfrak{R}$, then $\mathfrak{k}^{-1} \subseteq \mathfrak{R}^{-1}$.

Necessary and sufficient conditions that a complex $\mathfrak{U}$ be a subgroup, are:

$$\mathfrak{U} \neq 0,$$
$$\mathfrak{U}\mathfrak{U} \subseteq \mathfrak{U},$$
$$\mathfrak{U}^{-1} \subseteq \mathfrak{U}.$$

The latter two conditions can be replaced by

$$\mathfrak{U}\mathfrak{U}^{-1} \subseteq \mathfrak{U},$$

for then $e \subseteq \mathfrak{U}$, and so it follows that $\mathfrak{U}^{-1} \subseteq \mathfrak{U}$. Taking inverses in this inequality, we get $\mathfrak{U} \subseteq \mathfrak{U}^{-1}$; therefore $\mathfrak{U} = \mathfrak{U}^{-1}$, $\mathfrak{U}\mathfrak{U} \subseteq$ [illegible].

The intersection of two subgroups is itself a subgroup. The product of two subgroups is a subgroup when the two factors can be interchanged.

If a non-empty complex $\mathfrak{U}$ contains only a finite number of elements, then the condition $\mathfrak{U}\mathfrak{U} \subseteq \mathfrak{U}$ is necessary and sufficient for $\mathfrak{U}$ to be a subgroup, since the cancellation laws hold in $\mathfrak{U}$.

Let $\mathfrak{R}$ be a non-empty complex. Let $\mathfrak{R}_1 = \mathfrak{R} \cup \mathfrak{R}^{-1}$. Then $\mathfrak{R}_1^{-1} = \mathfrak{R}_1$ and $\mathfrak{R}_1 \cup \mathfrak{R}_1^2 \cup \mathfrak{R}_1^3 \ldots$ is a subgroup of $\mathfrak{G}$ which lies in every subgroup which contains $\mathfrak{R}$. The subgroup is called the subgroup generated by $\mathfrak{R}$ and is denoted by $\{\mathfrak{R}\}$. We set $\{0\} = e$.

Then the following rules hold:

$$\{\mathfrak{R}_1 \cap \mathfrak{R}_2\} \subseteq \{\mathfrak{R}_1\} \cap \{\mathfrak{R}_2\},$$

$$\{\mathfrak{R}_1 \cup \mathfrak{R}_2\} = \big\{\{\mathfrak{R}_1\} \cup \{\mathfrak{R}_2\}\big\}.$$

If $\mathfrak{k} \subseteq \mathfrak{R}$ then $\{\mathfrak{k}\} \subseteq \{\mathfrak{R}\}$; furthermore $\{\mathfrak{R}^{-1}\} = \{\mathfrak{R}\}$.

The following useful rule of the calculus of subgroups can be proven.

If $\mathfrak{u} \subseteq \mathfrak{U}$ and $\mathfrak{v} \subseteq \mathfrak{V}$, then

$$\mathfrak{U} \cap \mathfrak{u}\mathfrak{v} \cap \mathfrak{V} = (\mathfrak{u} \cap \mathfrak{V}) \cdot (\mathfrak{U} \cap \mathfrak{v}).$$

PROOF: It is immediate that $\mathfrak{U} \cap \mathfrak{u}\mathfrak{v} \cap \mathfrak{V} \supset (\mathfrak{u} \cap \mathfrak{V}) \cdot (\mathfrak{U} \cap \mathfrak{v})$. Moreover let $x \in \mathfrak{U} \cap \mathfrak{u}\mathfrak{v} \cap \mathfrak{V}$. Then x is of the form uv where $u \in \mathfrak{u}$, $v \in \mathfrak{v}$. Since $x \in \mathfrak{U}$, it follows that $v \in \mathfrak{U}$. Since $x \in \mathfrak{V}$, $u \in \mathfrak{V}$. Consequently x is in $(\mathfrak{u} \cap \mathfrak{V}) \cdot (\mathfrak{U} \cap \mathfrak{v})$, whence the rule follows.

If we set $\mathfrak{V} = \mathfrak{G}$ in the rule, we obtain:

If $\mathfrak{u} \subseteq \mathfrak{U}$ and $\mathfrak{v}$ is arbitrary then $\mathfrak{u} \cdot (\mathfrak{U} \cap \mathfrak{v}) = \mathfrak{U} \cap \mathfrak{u}\mathfrak{v}$.

We consider an ordered ascending chain of subgroups of a group:

$$\mathfrak{U}_1 \subseteq \mathfrak{U}_2 \subseteq \cdots \subseteq \mathfrak{U}_\omega \subseteq \mathfrak{U}_{\omega+1} \cdots$$

The sum of all $\mathfrak{U}$ in this subgroup chain, which has an arbitrary cardinal number of members, is itself a subgroup which we denote by $\mathfrak{V}$.

If a complex $\mathfrak{R}$ has no element in common with any member of the chain, then the intersection of $\mathfrak{V}$ and $\mathfrak{R}$ is empty.

We prove the following existence theorem on maximal subgroups.

THEOREM 5: *If $\mathfrak{R}$ is an arbitrary complex in $\mathfrak{G}$ and $\mathfrak{U}$ is a subgroup disjoint from $\mathfrak{R}$, then among the subgroups which contain $\mathfrak{U}$ and are disjoint from $\mathfrak{R}$, there exists a maximal one $\mathfrak{V}$.* Thus $\mathfrak{V}$ is defined as a subgroup of $\mathfrak{G}$ such that:

1. $\mathfrak{U} \subseteq \mathfrak{V}$,
2. $\mathfrak{V} \cap \mathfrak{R} = 0$.
3. $\{\mathfrak{V}, x\} \cap \mathfrak{R} = 0$ implies $x \in \mathfrak{V}$.

We consider the elements of $\mathfrak{G}$ as well ordered: $e < \nu_2 < \nu_3 \ldots$. We define an ascending chain of subgroups $\mathfrak{U}_e \leq \mathfrak{U}_{\nu_2} \ldots$ by means of transfinite induction: $\mathfrak{U}_e = \mathfrak{U}$. Assume that the subgroup $\mathfrak{U}_\nu$ has already been defined for all $\nu < \omega$ and that it has been shown that $\mathfrak{U}_\nu \leq \mathfrak{U}_\mu$ for $\nu \leqq \mu < \omega$ and that $\mathfrak{U}_\nu \cap \mathfrak{R} = 0$. Then let $\mathfrak{U}_\omega$ be the union Σ_ω of all $\mathfrak{U}_\nu$ for $\nu < \omega$ if $\{\Sigma_\omega, \omega\} \cap \mathfrak{R} \neq 0$, but let $\mathfrak{U}_\omega = \{\Sigma_\omega, \omega\}$ if $\{\Sigma_\omega, \omega\} \cap \mathfrak{R} = 0$. Since Σ_ω is a subgroup, $\mathfrak{U}_\omega$ is also a subgroup and $\mathfrak{U}_\nu \leq \mathfrak{U}_\omega$ for $\nu \leqq \omega$. Furthermore $\Sigma_\omega \cap \mathfrak{R} = 0$ by the construction of Σ_ω; therefore $\mathfrak{U}_\omega \cap \mathfrak{R} = 0$.

The union $\mathfrak{V}$ of all the $\mathfrak{U}_\omega$ is the maximal subgroup the existence of which was to be proven.

§ 8. The Concept of Normal Subgroup

What condition must a subgroup $\mathfrak{U}$ of a group $\mathfrak{G}$ satisfy in order that left congruency shall be equivalent to right congruency?

From $au \equiv a(\mathfrak{U}r)$ where $u \in \mathfrak{U}$ it should follow that

$$au \equiv a(\mathfrak{U}l),$$

and therefore

$$aua^{-1} \equiv e(\mathfrak{U}l).$$

If, conversely,

$$aua^{-1} \equiv e(\mathfrak{U}l),$$

then

$$au \equiv a$$

for both left and right congruency.

We come upon the *normality condition*

$$a\mathfrak{U}a^{-1} \leq \mathfrak{U}.$$

We arrive at this same condition if we ask when congruences can be multiplied. Then it should follow from $a \equiv a(\mathfrak{U}l)$ and $u \equiv e(\mathfrak{U}l)$ that: $au \equiv a(\mathfrak{U}l)$ and this implies $a\mathfrak{U}a^{-1} \leq \mathfrak{U}$ If conversely $x\mathfrak{U}x^{-1} \leq \mathfrak{U}$ for all x in $\mathfrak{G}$, then we can drop the l, r-symbols from the congruences and it follows from

$$a \equiv b$$

$$c \equiv d,$$

that

$$ac \equiv bc$$

$$bc \equiv bd,$$

and therefore

$$ac \equiv bd.$$

DEFINITION: *A subgroup $\mathfrak{N}$ of $\mathfrak{G}$ for which $x\mathfrak{N}x^{-1} \leq \mathfrak{N}$ holds for all x in $\mathfrak{G}$ is called a* ***normal subgroup.***

Left congruency is equivalent to right congruency if both are with respect to the same normal subgroup. Congruences with respect to a normal subgroup may be multiplied together.

From $x\mathfrak{N}x^{-1} \leq \mathfrak{N}$ and $x^{-1}\mathfrak{N}x \leq \mathfrak{N}$, it follows that

$$\mathfrak{N} = xx^{-1}\mathfrak{N}xx^{-1} \leq x\mathfrak{N}x^{-1},$$

and therefore $x\mathfrak{N}x^{-1} = \mathfrak{N}$,

$$x\mathfrak{N} = \mathfrak{N}x.$$

A normal subgroup commutes with every complex.

If conversely a subgroup commutes with every complex, then it is a normal subgroup, since $x\mathfrak{U} = \mathfrak{U}x$ implies $x\mathfrak{U}x^{-1} = \mathfrak{U}$.

The product of a normal subgroup and a subgroup $\mathfrak{U}$ is a subgroup.

DEFINITION: *A group with no non-trivial normal subgroups is said to be* ***simple.*** *Any other group is called* ***composite.***

A group without a non-trivial subgroup is simple. Moreover,

THEOREM 6: *A group with no non-trivial subgroups is cyclic of prime order, or consists of merely the unit element e.*

Proof: *If* $\mathfrak{G} \neq e$, then there is an element $a \neq e$ in $\mathfrak{G}$. By hypothesis $\mathfrak{G} = (a)$. If $\mathfrak{G}$ were infinite then $(a) \neq (a^2) \neq e$, and consequently $\mathfrak{G}$ is finite. If p is a prime dividing $\mathfrak{G}:1$ then $(a) \neq (a^p)$ and therefore $a^p = e$ and $\mathfrak{G}:1 = p$.

The converse was seen earlier.

A congruence relation in a multiplicative domain is said to be *multiplicative* if $a \equiv b$, $c \equiv d$ implies $ac \equiv bd$.

Example: In the multiplicative group of positive real numbers the relation:

a is congruent to b, if $a \geqq b$,

a is not congruent to b, if $a < b$,

is a multiplicative congruence relation.

Exercise: A multiplicative normal congruence relation in a group is the congruence relation of the group of elements with respect to the normal subgroup consisting of all the elements congruent to e.

§ 9. Normalizer, Class Equation

The following investigation shows the meaning of the concepts of subgroup and of right congruence.

Let $\mathfrak{P}$ be a group of permutations of the objects of a given set $\mathfrak{M}$.

DEFINITION: *Two objects in the set* $\mathfrak{M}$ *are said to be conjugate under the permutation group* $\mathfrak{P}$ ($\mathfrak{P}$*-conjugate) if there is a permutation in* $\mathfrak{P}$ *which maps one of the two objects onto the other.*

The relation "a is conjugate to b" fulfills our three requirements:

1. a is $\mathfrak{P}$-conjugate to itself since the identity permutation in $\mathfrak{P}$ maps a on itself.

2. If a is $\mathfrak{P}$-conjugate to b, then there is a permutation in $\mathfrak{P}$ which maps a onto b. The permutation which is the inverse of the latter lies likewise in $\mathfrak{P}$ and maps b onto a. Thus b is conjugate to a.

3. If $b = \pi a$, $c = \varrho b$, then $\varrho\pi$ as well as π, ϱ lies in $\mathfrak{P}$, and $\varrho\pi a = \varrho b = c$; therefore a is $\mathfrak{P}$-conjugate to c.

Under the action of a permutation group a set splits into disjoint classes of $\mathfrak{P}$-conjugate elements.

We call a class of $\mathfrak{P}$-conjugate objects of a set $\mathfrak{M}$ a *system of transitivity* for the permutation group $\mathfrak{P}$. The system of transitivity in which a lies consists of all πa with $\pi \in \mathfrak{P}$.

How many objects lie in a system of transitivity? The answer is given by THEOREM 7: *All the permutations of a permutation group* $\mathfrak{P}$ *which leave an object* a *of the permuted set* $\mathfrak{M}$ *fixed, form the subgroup* $\mathfrak{P}_a$ *of* $\mathfrak{P}$ *belonging to* a. *All the objects* $\mathfrak{P}$*-conjugate to* a *can be found as images of* a, *each once, under the permutations of a right representative system of* $\mathfrak{P}$ *with respect to* $\mathfrak{P}_a$. *Therefore the number of objects which are* $\mathfrak{P}$*-conjugate to* a *is equal to the index of* $\mathfrak{P}_a$ *in* $\mathfrak{P}$.

Proof: Let $\mathfrak{P}_a$ be the set of permutations in $\mathfrak{P}$ which leave a fixed. 1 belongs to $\mathfrak{P}_a$. If π belongs to $\mathfrak{P}_a$, then π^{-1} is in $\mathfrak{P}$ and $\pi^{-1}a = \pi^{-1}(\pi a) = a$, and therefore π^{-1} also belongs to $\mathfrak{P}_a$. If ϱ and π are in $\mathfrak{P}_a$ then $\varrho\pi$ is in $\mathfrak{P}$ and $\varrho\pi a = \varrho(\pi a) = \varrho a = a$; therefore $\varrho\pi$ is also in $\mathfrak{P}_a$.

$\mathfrak{P}_a$ is a subgroup of $\mathfrak{P}$.

If the permutations ϱ and π in $\mathfrak{P}$ have the same effect on a then they are right congruent with respect to $\mathfrak{P}_a$ since $\pi a = \varrho a$ implies $\varrho^{-1}\pi a = a$, $\varrho^{-1}\pi \in \mathfrak{P}_a$, $\varrho \equiv \pi(\mathfrak{P}_a r)$, and conversely. If, then, $\pi \to \bar{\pi}$ is a right representative function of $\mathfrak{P}$ with respect to $\mathfrak{P}_a$, then every conjugate πa of a is equal to $\bar{\pi}a$ and $\bar{\pi}a = \bar{\varrho}a$ implies $\bar{\pi} = \bar{\varrho} = \bar{\pi} = \bar{\varrho}$, as was to be shown.

DEFINITION: *We say that two subsets of the set* $\mathfrak{M}$ *are* ***conjugate under the permutation group*** $\mathfrak{P}$ *if there is a permutation in* $\mathfrak{P}$ *which maps one subset onto the other.*

Since $\mathfrak{P}$ also permutes the subsets of $\mathfrak{M}$, the above statements remain valid if "object" is replaced by "subset".

However, we denote by $\mathfrak{P}_{(\mathfrak{m})}$ the subgroup of permutations in $\mathfrak{P}$ which map a subset $\mathfrak{m}$ of $\mathfrak{M}$ onto itself, whereas $\mathfrak{P}_{\mathfrak{m}}$ will denote the subgroup of all permutations in $\mathfrak{P}$ which leave each element of $\mathfrak{m}$ fixed.

We now take the set of all elements of a group $\mathfrak{G}$ as an example of a permuted set.

For every element x in $\mathfrak{G}$, we define the "*x-transformation*" as the single-valued mapping $\binom{a}{xax^{-1}}$. xax^{-1} is called the x-transform of a. The x-transformations of $\mathfrak{G}$ form a permutation group, since $\binom{a}{eae^{-1}}=\binom{a}{a}$ is the identity permutation $\underline{1}$:

$$\binom{a}{xax^{-1}}\binom{a}{yay^{-1}}=\binom{a}{xya(xy)^{-1}}, \text{ and in particular} \tag{1}$$

$$\binom{a}{xax^{-1}}\cdot\binom{a}{x^{-1}ax}=\binom{a}{a}=\underline{1}. \tag{2}$$

The group of transformations of $\mathfrak{G}$ is denoted by $J_{\mathfrak{G}}$ or simply by J.

DEFINITION: Two complexes in $\mathfrak{G}$ are said to be *conjugate* (*under* $\mathfrak{G}$) if one complex is the transform of the other: $\mathfrak{K}_2 = x\mathfrak{K}_1x^{-1}$, or equivalently, $x\mathfrak{K}_1 = \mathfrak{K}_2x$.

From equations (1), (2) we immediately see that in $\mathfrak{G}$, all elements x whose corresponding transformations lie in a given subgroup of J form a subgroup of $\mathfrak{G}$. We can therefore define, in accordance with Theorem 7:

The *normalizer* $N_{\mathfrak{K}}$ of the complex $\mathfrak{K}$ is the subgroup consisting of all elements x of $\mathfrak{G}$ which transform $\mathfrak{K}$ into itself: $x\mathfrak{K}x^{-1}=\mathfrak{K}$, or equivalently $x\mathfrak{K}=\mathfrak{K}x$.

If $x_1, x_2, \ldots$ is a representative system of $\mathfrak{G}$ with respect to $N_{\mathfrak{K}}$, then $x_1\mathfrak{K}x_1^{-1}, x_2\mathfrak{K}x_2^{-1}, \ldots$ are the complexes conjugate to $\mathfrak{K}$, each occurring exactly once; and conversely. Thus

The number of complexes conjugate to a given complex is equal to the index of its normalizer.

The group $\mathfrak{G}$ falls into classes of conjugate elements relative to the transformations in J, giving the direct decomposition $\mathfrak{G}=\mathfrak{C}_1+\mathfrak{C}_2+\cdots$ The number of classes of conjugate elements of a group is called the *class-number* of the group. The direct decomposition

$$\mathfrak{G}=\mathfrak{C}_1+\mathfrak{C}_2+\cdots+\mathfrak{C}_r$$

of the group $\mathfrak{G}$ into classes of conjugate elements corresponds to the equation

$$\mathfrak{G}:1=h_1+h_2+\ldots+h_r \qquad (\textit{class equation}) \tag{3}$$

where h_i is the number of elements in $\mathfrak{C}_i$.

DEFINITION: All the elements of a group $\mathfrak{G}$ which transform each

element of $\mathfrak{G}$ into itself, i.e., those which commute with every element of $\mathfrak{G}$, form a subgroup called the *center* $\mathfrak{z}(\mathfrak{G})$ of $\mathfrak{G}$. $\mathfrak{z}$ is obviously the intersection of all the normalizers of elements in $\mathfrak{G}$.

It follows from the definition that the center is an abelian normal subgroup. The center is just that domain of all elements which are transformed into themselves by every element in $\mathfrak{G}$. Therefore we may write the class-equation as follows:

$$(4)\quad \mathfrak{G}:1 = \mathfrak{z}:1 + \sum_{h_i > 1} h_i .$$

It is important in the above to note that the summation is performed over all the *group indices* different from 1.

The subgroups which are transformed into themselves by every element in $\mathfrak{G}$ are precisely the normal subgroups of $\mathfrak{G}$.

The *normalizer* of an arbitrary subgroup $\mathfrak{U}$ of $\mathfrak{G}$ is the (uniquely determined) maximal subgroup containing $\mathfrak{U}$ as normal subgroup.

We wish to determine the classes of conjugate elements in the symmetric and alternating permutation groups of n ciphers.

Let π and ϱ be two permutations in $\mathfrak{S}_n$; then $\varrho\pi\varrho^{-1}(\varrho x) = \varrho\pi x$, and therefore $\varrho\pi\varrho^{-1} = \begin{pmatrix} \varrho x \\ \varrho\pi x \end{pmatrix}$, i.e.: *The ϱ-transform of π originates from π by replacing the cipher x by ϱx in the functional symbol for π. The same also holds for the cycle symbol.*

Two permutations are conjugate under $\mathfrak{S}_n$ if and only if they have cycle decompositions with like groupings.

Let π be a product of a_1 1-cycles, a_2 2-cycles, ..., a_n n-cycles. Then the number of permutations that commute with π is just as large as the number of formally different ways that π can be written as a product of first a_1 1-cycles, then a_2 2-cycles, and finally a_n n-cycles, and this is $a_1!\,1^{a_1}\cdot a_2!\,2^{a_2}, \ldots, a_n!\,n^{a_n}$. Consequently the class $\mathfrak{C}_\pi$ of elements conjugate to π under $\mathfrak{S}_n$ contains $\dfrac{n!}{a_1!\,1^{a_1}\ldots a_n!\,n^{a_n}}$ permutations.

Now let $n > 1$, $\pi_1 = (12)\pi(12)^{-1}$. Every permutation in $\mathfrak{C}_\pi$ is conjugate either to π or π_1 under $\mathfrak{A}_n$, the alternating group. Therefore $\mathfrak{C}_\pi$ decomposes into two classes under $\mathfrak{A}_n$, each with an equal number of elements, or it does not decompose. The latter takes place if and only if π commutes with an odd permutation. This last is equivalent to the condition: There is an $a_{2i} > 0$ or an $a_{2i+1} > 1$.

§ 10. A Theorem of Frobenius

The following theorem is not yet fitted into a wider context in a satisfactory way.

THEOREM OF FROBENIUS: *The number of solutions of* $x^n = c$, *where* c *belongs to a fixed class* $\mathfrak{C}$ *of* h *elements conjugate under a finite group* $\mathfrak{G}$ *of order* N, *is divisible by the greatest common divisor of* hn *and* N.

Proof: The complex consisting of those elements in $\mathfrak{G}$ whose n-th powers lie in the complex $\mathfrak{R}$ is denoted by $\mathfrak{A}_{\mathfrak{R},n}$. Let $A_{\mathfrak{R},n}$ be the number of elements in $\mathfrak{A}_{\mathfrak{R},n}$. If $N=1$, then the theorem is true. Now let $N>1$ and let the theorem be proven for groups whose order is less than N. If $n=1$, then $A_{\mathfrak{C},n}=h$. Therefore the statement is true. Now let $n>1$ and let the statement be proven for all smaller n. (We are using induction twice). Since the elements in $\mathfrak{C}$ are conjugate under $\mathfrak{G}$, $A_{\mathfrak{C},n}=h\cdot A_{c,n}$. $\mathfrak{A}_{c,n}$ lies in the normalizer N_c of c. If $h>1$, then, applying the induction hypothesis to N_c, we find* that $\left(n,\frac{N}{h}\right)/A_{c,n}$, and therefore $(hn, N)/A_{\mathfrak{C},n}$.

Now let $h=1$. If $n=n_1 n_2$, $(n_1, n_2)=1$, $n_1, n_2 \neq 1$ and if $\mathfrak{D}=\mathfrak{A}_{\mathfrak{C},n_1}$ then $\mathfrak{A}_{\mathfrak{C},n}=\mathfrak{A}_{\mathfrak{D},n_1}$. By the induction hypothesis (n_1, N) is a divisor of $A_{\mathfrak{D},n_1}$, and therefore also a divisor of $A_{\mathfrak{C},n}$. Similarly it follows that (n_2, N) is a divisor of $A_{\mathfrak{C},n}$ and since n_1 is relatively prime to n_2, we have (n, N) as divisor of $A_{\mathfrak{C},n}$.

It can now be assumed that $n=p^a$ is the a-th power of a prime number p with $a>0$. If p divides the order ϱ of c, then an element x in $\mathfrak{A}_{c,n}$ has the order $n\cdot\varrho$. Then exactly n elements of $\mathfrak{A}_{c,n}$ lie in (x), and all these n elements generate the same subgroup, namely (x). The number of elements in $\mathfrak{A}_{c,n}$ is consequently divisible by n.

Finally we may assume that n is relatively prime to the order of the center element c. All the elements of the center whose order is prime to n form a subgroup $\mathfrak{g}$ of $\mathfrak{G}$ of order g prime to n.[1] Since every element in $\mathfrak{g}$ is an n-th power[2], the equation $c_1=c_2 x^n$ is solvable in $\mathfrak{g}$ for every pair of elements c_1, c_2, and since $\mathfrak{g}$ lies in the center of $\mathfrak{G}$, we have $A_{c_1,n}=A_{c_2,n}$. It now follows from the class equation that

$$N=\sum_{\mathfrak{C}\nmid\mathfrak{g}} A_{\mathfrak{C},n}+g\cdot A_{c,n}.$$

In the above, N and all the $A_{\mathfrak{C},n}$ with $\mathfrak{C}\nmid\mathfrak{g}$ are divisible by (n, N). Therefore $g\cdot A_{\mathfrak{C},n}$ is divisible by (n, N). Since $(g, n)=1$, we have

$$(n, N)/A_{c,n}, \qquad \text{Q.E.D.}$$

* Since the index of N_c equals h. (*Ed.*)

[1] See Exercises 2, 3 at the end of the Chapter.

[2] See Exercise 3 at the end of the Chapter.

Exercises

1. The complex of all n-th powers of elements of a complex $\mathfrak{K}$ in a group is denoted by $\mathfrak{K}^{(n)}$. The complex of all elements in $\mathfrak{K}$ whose n-th power is equal to e is denoted by $\mathfrak{K}_{(n)}$.

We have

$$\mathfrak{K}^{(1)} = \mathfrak{K}, \quad \mathfrak{K}^{(-1)} = \mathfrak{K}^{-1}, \quad \mathfrak{K}^{(nm)} = (\mathfrak{K}^{(n)})^{(m)}, \quad \mathfrak{K}_{(n)} \cap \mathfrak{K}_{(m)} = \mathfrak{K}_{((n,m))}.$$

2. If a commutes with b then

$$(ab)^n = a^n b^n$$

and the order of ab is a divisor of the least common multiple of the orders of a and b.

3. If the rational integer n is relatively prime to the order of $\mathfrak{G}$ then $\mathfrak{G}^{(n)} = \mathfrak{G}$.

(Exercises 4-6 in Burnside.)

4. In a group $\mathfrak{G}$ if the equation

$$(ab)^n = a^n b^n$$

holds for every pair a, b of group elements, then $\mathfrak{G}^{(n)}$ and $\mathfrak{G}_{(n)}$ are subgroups of $\mathfrak{G}$.

Then, moreover, $\mathfrak{G} : \mathfrak{G}^{(n)} = \mathfrak{G}_{(n)} : 1$.

(Hint: The elements of $\mathfrak{G}$ whose n-th power is a fixed element of $\mathfrak{G}$ form a (right) coset of $\mathfrak{G}$ with respect to $\mathfrak{G}_{(n)}$.,

$\mathfrak{G}^{(n-1)}$ commutes elementwise with $\mathfrak{G}^{(n)}$. (Young.)

5. If $\mathfrak{U}$ and $\mathfrak{V}$ are finite subgroups of the group $\mathfrak{G}$., then $\mathfrak{U}\mathfrak{V}$ contains exactly $\frac{(\mathfrak{U}:1)\,(\mathfrak{V}:1)}{(\mathfrak{U} \cap \mathfrak{V}:1)}$ elements.

6. If the index of the normal subgroup $\mathfrak{N}$ of a finite group $\mathfrak{G}$ is relatively prime to the order n of $\mathfrak{N}$, then $\mathfrak{N}$ contains every subgroup of $\mathfrak{G}$ whose order is a divisor of n. (Use Exercise 5.)

7. The alternating permutation group of $n > 2$ ciphers can be generated by (123), (124), . . . , (12n).

8. A well known puzzle requires that 15 numbered stones on a board divided into 16 squares be moved horizontally and vertically until we obtain the situation of Fig. 1, p. 30.

We may assume that in the initial position the lower right corner of the board is vacant, so that the initial position can be described uniquely, with the use of Fig. 1, by a permutation of the fifteen ciphers. It is to be shown that Fig. 1 is attainable precisely when the permutation for the initial position is even. (Generalization?)

9. If $\mathfrak{N}$ is a normal subgroup of the finite group $\mathfrak{G}$, then a normal multiplication table of $\mathfrak{G}$ can be constructed so that it is possible to divide the table into squares having the following properties:

1). Each square contains the same number of compartments. (The number of squares is $(\mathfrak{G} : \mathfrak{N})^2$.

2). The rows of each square are the same to within the order of elements.

3). The square in the upper left corner contains exactly the elements of $\mathfrak{N}$ (Example, Fig. 2).

What sort of elements are in a square?

Conversely if it is possible to divide a normal multiplication table of $\mathfrak{G}$ into squares, such that 1., 2. hold and e is in the upper left corner of a square, then it is to be shown that we have a division into squares with respect to a normal subgroup.

What divisions of $\mathfrak{G}$ occur if we omit the condition that the multiplication table be normal?

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

Fig. 1.

$e\ a$ $a\ e$	$b\ c$ $c\ b$
$b\ c$ $c\ b$	$e\ a$ $a\ e$

Fig. 2

10. If $\mathfrak{F}$ is a set of complexes of a given group with the properties:
1). Every element in $\mathfrak{G}$ is in at least one of the complexes of $\mathfrak{F}$.
2). No complex in $\mathfrak{F}$ is a proper subset of any other complex of $\mathfrak{F}$.
3). The product of two complexes in $\mathfrak{F}$ is contained in a third complex of $\mathfrak{F}$, then $\mathfrak{F}$ is the set of cosets of $\mathfrak{G}$, with respect to a normal subgroup, and $\mathfrak{F}$ is a group.

II. THE CONCEPT OF HOMOMORPHY AND GROUPS WITH OPERATORS

§ 1. Homomorphisms

1. *The Concept of Homomorphy.*

Let $\mathfrak{G}$ and $\mathfrak{G}^*$ be sets in which a multiplication is uniquely defined (multiplicative domains).

DEFINITION: A single valued mapping of the elements in $\mathfrak{G}$ onto a certain subset of $\mathfrak{G}^*$ is called a *homomorphy*, if the product of two elements is mapped onto the product of the image elements.

Example: The mapping, defined on page 8, of $\mathfrak{S}_n$ into the group consisting of ± 1 is a homomorphy.

If the image of x is denoted by σx then σ must satify the functional equation:

$$\sigma(xy) = \sigma x \cdot \sigma y \ .$$

The homomorphy is said to be a *homomorphic mapping* or a *homomorphism* if every element of $\mathfrak{G}^*$ is an image element. $\mathfrak{G}^*$ is said to be homomorphic to $\mathfrak{G}$. We denote this by: $\mathfrak{G} \sim \mathfrak{G}^*$.

A homomorphy is a mapping *into* $\mathfrak{G}^*$ while a homomorphism is a mapping *onto* $\mathfrak{G}^*$.

Example: From Chapter I. § 6 we see that the mapping of the group of surface rotations of a regular tetrahedron into $\mathfrak{S}_4$ is a homomorphy, but onto $\mathfrak{A}_4$ the mapping is a homomorphism.

Under every homomorphy the set $\overline{\mathfrak{G}}$ of image elements is homomorphic to $\mathfrak{G}$.

The relation of homomorphy is transitive. If $x \to \sigma x$ is a homomorphy of $\mathfrak{G}$ into $\mathfrak{G}^*$ *and* $x^* \to \tau x^*$ a homomorphy of $\mathfrak{G}^*$ into $\mathfrak{G}^{**}$, then the product of τ by σ is defined by means of the equation:

$$\tau\sigma x = \tau(\sigma x) \ .$$

$\tau\sigma$ is a single-valued mapping of the elements of $\mathfrak{G}$ onto a certain subset of $\mathfrak{G}^{**}$.

Since

$$(\tau\sigma)(xy) = \tau(\sigma(xy)) = \tau(\sigma x \cdot \sigma y) = \tau(\sigma x) \cdot \tau(\sigma y) = \tau\sigma x \cdot \tau\sigma y,$$

$\tau\sigma$ is a homomorphy of $\mathfrak{G}$ into $\mathfrak{G}^{**}$. We have the following rule for calculation with homomorphies:

If $\tau\sigma$ *and* $\varrho\tau$ *are defined, then* $\varrho(\tau\sigma)$ *and* $(\varrho\tau)\sigma$ *are also defined and*

$$\varrho(\tau\sigma) = (\varrho\tau)\sigma = \varrho\tau\sigma.$$

The defining equation $(\sigma\tau)x = \sigma(\tau x)$ shows that $\sigma\tau x$ can be written instead of $(\sigma\tau)x$ without misunderstanding. *Thus the homomorphy relation is transitive.*

From $\mathfrak{G} \sim \mathfrak{G}^*$, $\mathfrak{G}^* \sim \mathfrak{G}^{**}$ it follows that $\mathfrak{G} \sim \mathfrak{G}^{**}$.

The homomorphy relation is reflexive. That is, the identity mapping $\underline{1}_{\mathfrak{G}}$ of $\mathfrak{G}$, defined by $\underline{1}_{\mathfrak{G}}\, x = x$, has $\mathfrak{G}$ as its set of images.

If we speak of the product of two homomorphies, then it will be assumed at the same time that it is definable in terms of the above relations.

In this sense

$$\sigma \underline{1}_{\mathfrak{G}^*} = \sigma \quad \text{and} \quad \underline{1}_{\mathfrak{G}}\sigma = \sigma.$$

The image of the complex $\mathfrak{K}$ in $\mathfrak{G}$ under the homomorphy σ is denoted by $\sigma\mathfrak{K}$. If $\mathfrak{K}$ is a multiplicative subdomain, then $\mathfrak{K}$ is mapped homomorphically onto $\sigma\mathfrak{K}$ by σ.

We say σ *induces* a homomorphy of $\mathfrak{K}$ into $\mathfrak{G}^*$.

The homomorphic image of a group $\mathfrak{U}$ *in* $\mathfrak{G}$ *is a group:*

If $\mathfrak{U}$ is a subgroup of $\mathfrak{G}$, then it follows from $y \in \mathfrak{U}$ that $xy \in \mathfrak{U}$; therefore $\sigma x \cdot \sigma y = \sigma(xy) \in \sigma\mathfrak{U}$.

Furthermore $ex = xe = x$, $\sigma e \cdot \sigma x = \sigma x \cdot \sigma e = \sigma x$, therefore σe is the unit element of $\sigma\mathfrak{U}$. We have $\sigma(x x^{-1}) = \sigma x \cdot \sigma(x^{-1}) = \sigma e$ and therefore $\sigma(x^{-1})$ is the inverse of σx. Therefore $\sigma\mathfrak{U}$ is a group.

If $\overline{\mathfrak{U}}$ *is a subgroup of the image domain* $\mathfrak{G}$, *then the set of all the elements of* $\mathfrak{G}$ *whose image is in* $\overline{\mathfrak{U}}$ *forms a subgroup* $\mathfrak{U}$ *of* $\mathfrak{G}$, *and*

$$\overline{\mathfrak{U}} = \sigma\mathfrak{U}.$$

Every element in $\overline{\mathfrak{U}}$ is of the form σx for x in $\mathfrak{U}$; if $x, y \in \mathfrak{U}$, then $\sigma(xy) = \sigma x \cdot \sigma y \in \overline{\mathfrak{U}}$, $xy \in \mathfrak{U}$, $\sigma(x^{-1}) = (\sigma x)^{-1} \in \overline{\mathfrak{U}}$, $x^{-1} \in \mathfrak{U}$.

2. *The Isomorphy Concept.*

If a group $\mathfrak{G}$ is mapped onto the group $\overline{\mathfrak{G}}$ homomorphically, then multiplication in $\mathfrak{G}$ parallels that in $\mathfrak{G}$. However, we consider two groups as the same in abstract group theory only if their tables differ merely in notation, order of rows and columns: Homomorphic groups are not always equivalent in the abstract sense. If, for example, the group $\mathfrak{G}$ contains more than one element, then there is a homomorphism of $\mathfrak{G}$ which maps every element of $\mathfrak{G}$ onto the unit element, but the tables of $\mathfrak{G}$ and e have a different number of rows.

Those homomorphic mappings under which the table of the group is preserved are called *isomorphic mappings*. That the homomorphic mapping is *one-one* is necessary and sufficient for the latter.

DEFINITION: A homomorphy σ of the multiplicative domain $\mathfrak{G}$ into the multiplicative domain $\mathfrak{G}^*$ is called an *isomorphy*, if $\mathfrak{G}$ is mapped onto the set $\overline{\mathfrak{G}}$ of image elements in a one-one manner, i.e., if $\sigma x = \sigma y$ implies $x = y$.

An isomorphy which is a also homomorphic mapping is called an *isomorphic mapping* (*isomorphism*). $\mathfrak{G}$ is isomorphic to $\overline{\mathfrak{G}}$ under every isomorphy.

Example: The group of rotations of an equilateral triangle is isomorphic to $\mathfrak{S}_3$; the group of rotations of a regular tetrahedron is isomorphic to $\mathfrak{A}_4$ (§ 6 of the previous chapter).

The existence of an isomorphic mapping of $\mathfrak{G}$ onto $\overline{\mathfrak{G}}$ is denoted by $\mathfrak{G} \simeq \overline{\mathfrak{G}}$.

The three well-known rules hold for isomorphism:

1) The identity isomorphism maps $\mathfrak{G}$ onto itself.

2) If $\mathfrak{G} \simeq \overline{\mathfrak{G}}$, $\overline{\mathfrak{G}} \simeq \overline{\overline{\mathfrak{G}}}$, then $\mathfrak{G} \simeq \overline{\overline{\mathfrak{G}}}$, since $\sigma\tau x = \sigma\tau y$ implies $\tau x = \tau y$ and $x = y$.

3) If $\mathfrak{G} \simeq \overline{\mathfrak{G}}$, then every element y in $\overline{\mathfrak{G}}$ can be written uniquely in the form $y = \sigma x$. $\sigma^{-1} y = x$ now defines an isomorphic mapping of $\overline{\mathfrak{G}}$ onto $\mathfrak{G}$: Let $y_1 = \sigma x_1$, $y_2 = \sigma x_2$; then

$$\sigma^{-1}(y_1 y_2) = \sigma^{-1}(\sigma x_1 \cdot \sigma x_2) = \sigma^{-1}(\sigma(x_1 x_2)) = x_1 x_2 = \sigma^{-1} y_1 \cdot \sigma^{-1} y_2.$$

Moreover, the mapping σ^{-1} is one-one, since σ is one-one. Therefore it follows from $\mathfrak{G} \simeq \overline{\mathfrak{G}}$ that $\overline{\mathfrak{G}} \simeq \mathfrak{G}$. Calculation with inverse mappings satisfies the following rules:

If the equation $\tau\sigma = \underline{1}_{\mathfrak{G}}$ is solvable for a homomorphy σ, then σ is an isomorphy, since $\sigma x = \sigma y$ implies $\tau\sigma x = \tau\sigma y$ and therefore $x = y$.

An isomorphic mapping can also be defined as a homomorphy for which $\tau\sigma = \underline{1}_{\mathfrak{G}}$ and $\sigma\varrho = \underline{1}_{\mathfrak{G}^*}$ are solvable. Then for all $y \in \mathfrak{G}^*$: $y = \sigma\varrho y$ and therefore $\mathfrak{G}^* = \overline{\mathfrak{G}}$. Moreover $\tau = \varrho = \sigma^{-1}$.

3. *Factor Group, Isomorphy Theorems.*

Under what circumstances it is possible to read off the multiplication table of a homomorphic image of a given group $\mathfrak{G}$ from the multiplication table of $\mathfrak{G}$ itself?

We have first the following theorem:

If $\mathfrak{N}$ is a normal subrgroup of $\mathfrak{G}$, then there is a homomorphism σ of $\mathfrak{G}$ under which the set of elements of $\mathfrak{G}$ mapped onto σe is precisely $\mathfrak{N}$.

We set $$\sigma a = a\mathfrak{N},$$

Then $\sigma(ab) = ab\mathfrak{N} = a(b\mathfrak{N})\mathfrak{N} = a\mathfrak{N} \cdot b\mathfrak{N} = \sigma a \cdot \sigma b.$

From the above we realize that the set of cosets of $\mathfrak{G}$ with respect to a normal subgroup of $\mathfrak{G}$ form a group homomorphic to $\mathfrak{G}$. The group of residue classes of a group $\mathfrak{G}$ with respect to a normal subgroup $\mathfrak{N}$ is called a *factor group* and is denoted by $\mathfrak{G}/\mathfrak{N}$. The order of a factor group is equal to $\mathfrak{G}:\mathfrak{N}$. The unit element of the factor group is the normal subgroup $\mathfrak{N}$.

If, conversely, the left cosets, formed with respect to a subgroup, form a group under the usual complex multiplication, then the subgroup is a normal subgroup, as we saw previously.

FIRST ISOMORHISM THEOREM: *Under a homomorphism* σ *of a given group* $\mathfrak{G}$ *onto a group* $\overline{\mathfrak{G}}$, *all the elements of* $\mathfrak{G}$ *which are mapped onto the unit element of* $\overline{\mathfrak{G}}$ *form a normal subgroup* $\mathfrak{E}$ *of* $\mathfrak{G}$, *and the factor group of* $\mathfrak{G}$ *with respect to* $\mathfrak{E}$ *is isomorphic to* $\overline{\mathfrak{G}}$.

Proof: All the elements of $\mathfrak{G}$ which are mapped on the unit element $\bar{e}$ of $\mathfrak{G}$ under σ form a subgroup $\mathfrak{E}$.

$\sigma(a\mathfrak{E}) = \sigma a$ gives a one-valued mapping .

$$\sigma(a\mathfrak{E} \cdot b\mathfrak{E}) = \sigma(ab\mathfrak{E}) = \sigma(ab) = \sigma a \cdot \sigma b = \sigma(a\mathfrak{E}) \cdot \sigma(b\mathfrak{E}).$$

From $\sigma(a\mathfrak{E}) = \sigma(\mathfrak{E}) = \sigma e$ it follows that $\sigma a = \sigma e$; and therefore

$a \in \mathfrak{E}$, $a\mathfrak{E} = \mathfrak{E}$.

Therefore $a\mathfrak{E} \cdot b\mathfrak{E} = ab\mathfrak{E}$,

$\mathfrak{E}$ is a normal subgroup, and from the isomorphism it follows that the homomorphic image of $\mathfrak{G}$ has the same table as the factor group $\mathfrak{G}/\mathfrak{E}$. Therefore the question of the multiplication tables of homomorphic images will be resolved if we can give all the normal subgroups of the original group. (See Exercises 9, 10 at the end of Chap. I.)

SECOND ISOMORPHISM THEOREM: *If* $\mathfrak{U}$ *is a subgroup and* $\mathfrak{N}$ *is a normal subgroup of the group* $\mathfrak{G}$, *then the intersection* $\mathfrak{U} \cap \mathfrak{N}$ *is a normal subgroup of* $\mathfrak{U}$ *and*

$$\mathfrak{U}/\mathfrak{U} \cap \mathfrak{N} \simeq \mathfrak{U}\mathfrak{N}/\mathfrak{N}.$$

The isomorphism is obtained by means of the mapping:

$$U(\mathfrak{U} \cap \mathfrak{N}) \rightarrow U(\mathfrak{U} \cap \mathfrak{N}) \cdot \mathfrak{N} = U\mathfrak{N}.$$

Proof: The homomorphism $a \rightarrow a\mathfrak{N}$ of $\mathfrak{G}$ onto $\mathfrak{G}/\mathfrak{N}$ is again denoted by σ . Then $\mathfrak{U} \sim \sigma\mathfrak{U}$. Under the mapping of $\mathfrak{U}$ onto $\sigma\mathfrak{U}$, precisely the elements of $\mathfrak{U} \cap \mathfrak{N}$ map onto e; therefore $\mathfrak{U} \cap \mathfrak{N}$ is a normal subgroup

of $\mathfrak{U}$, and $\mathfrak{U}/\mathfrak{U} \cap \mathfrak{N} \simeq \sigma\mathfrak{U}$. If we replace $\mathfrak{U}$ by $\mathfrak{U}\mathfrak{N}$ then the same argument shows that $\mathfrak{U}\mathfrak{N}/\mathfrak{N} \simeq \sigma\mathfrak{U}$. The theorem follows from both isomorphisms.

If $\mathfrak{H}$ is a normal subgroup of the group $\mathfrak{G}$, then for every homomorphism σ, the group $\overline{\mathfrak{H}} = \sigma\mathfrak{H}$ is a normal subgroup of $\overline{\mathfrak{G}} = \sigma\mathfrak{G}$ since $\sigma x \cdot \overline{\mathfrak{H}}(\sigma x)^{-1} = \sigma(x\mathfrak{H}x^{-1}) = \sigma\mathfrak{H} = \overline{\mathfrak{H}}$. If, conversely, $\overline{\mathfrak{H}}$ is a normal sugroup of $\overline{\mathfrak{G}}$, then all the elements of $\mathfrak{G}$ whose image is in $\overline{\mathfrak{H}}$ form a normal subgroup $\mathfrak{H}$ of $\mathfrak{G}$, since

$$\sigma(x\mathfrak{H}x^{-1}) = \sigma(x)\overline{\mathfrak{H}}(\sigma x)^{-1} = \overline{\mathfrak{H}},$$

and therefore $x\mathfrak{H}x^{-1} \leq \mathfrak{H}$. Information on the relation between the factor groups is given by the

THIRD ISOMORPHISM THEOREM: *Let σ be a homomorphic mapping of $\mathfrak{G}$ onto $\overline{\mathfrak{G}}$. Let $\mathfrak{E}$ be the normal subgroup composed of the elements of $\mathfrak{G}$ which map onto the unit element of $\overline{\mathfrak{G}}$; let $\overline{\mathfrak{H}}$ be a normal subgroup of $\overline{\mathfrak{G}}$, let $\mathfrak{H}$ be the group of elements in $\mathfrak{G}$ whose image falls in $\overline{\mathfrak{H}}$.*

Then $\mathfrak{H}$ is a normal subgroup of $\mathfrak{G}$, and

$$\mathfrak{G}/\mathfrak{H} \simeq \overline{\mathfrak{G}}/\overline{\mathfrak{H}} \simeq \mathfrak{G}/\mathfrak{E}/\mathfrak{H}/\mathfrak{E}.$$

Proof: We have $\mathfrak{G} \sim \overline{\mathfrak{G}}$ and $\overline{\mathfrak{G}} \sim \overline{\mathfrak{G}}/\overline{\mathfrak{H}}$. Under the second homomorphism exactly the elements of $\overline{\mathfrak{H}}$ map onto the identity coset $\overline{\mathfrak{H}}$. Under the first homomorphism precisely the elements of $\mathfrak{H}$ map onto $\overline{\mathfrak{H}}$. Therefore $\mathfrak{G}/\mathfrak{H} \simeq \overline{\mathfrak{G}}/\overline{\mathfrak{H}}$. If we set $\overline{\mathfrak{G}} = \mathfrak{G}/\mathfrak{E}$, then $\mathfrak{G}/\mathfrak{H} \simeq \mathfrak{G}/\mathfrak{E}/\mathfrak{H}/\mathfrak{E}$.

§ 2. Representation of Groups by Means of Permutations

We want to find homomorphism of given abstract groups onto permutation groups.

DEFINITION: A single-valued mapping $x \to \pi_x$ of the elements x of a group $\mathfrak{G}$ onto the permutations π_x of ω ciphers is called a *representation of $\mathfrak{G}$ (as a permutation group) of degree ω* if

$$\pi_{xy} = \pi_x \cdot \pi_y.$$

All permutations π_x form a group $\mathfrak{P}$, the *representation group.*

A representation is said to be *faithful* if the homomorphy induced by the representation is an isomorphy.

Two representations Δ, Δ' by means of ciphers from $\mathfrak{M}_1$, $\mathfrak{M}_2$ respectively, are said to be *equivalent* if there is a 1-1 mapping $a \to a'$ of the ciphers of $\mathfrak{M}_1$ onto those of $\mathfrak{M}_2$, such that $(\pi_x a)' = \pi_x' a'$ for all x; in short if the representations are the same except for the naming of the ciphers.

If the permuted ciphers form a system of transitivity under $\mathfrak{P}$, then

the permutation group $\mathfrak{P}$ *and* the representation of $\mathfrak{G}$ by $\mathfrak{P}$ are called *transitive*, otherwise they are called *intransitive*.

If $\mathfrak{T}$ is a system of transitivity of $\mathfrak{P}$, then $\pi_x' = \binom{t}{\pi_x t}$, where $t \in \mathfrak{T}$, is a permutation of ciphers in $\mathfrak{T}$, and the mapping $x \to \pi_x'$ gives a transitive representation $\Delta_{\mathfrak{T}}$ of $\mathfrak{G}$. The representation group belonging to $\Delta_{\mathfrak{T}}$ is called a *transitive component* of the original representation.

Since, clearly, every representation can be constructed from the transitive sub-representations, *it is sufficient to investigate the transitive* representations of a given group $\mathfrak{G}$.

Let a transitive representation Δ of degree ω of the group $\mathfrak{G}$ be given. We choose a cipher a and consider two elements of $\mathfrak{G}$ to be in the same class if the corresponding permutations have the same effect on the cipher a. With the help of this decomposition into classes, a normal congruence relation is definable. Moreover, $x \equiv y$ implies $\pi_x a = \pi_y a$, which implies $\pi_{zx} a = \pi_z \pi_x a = \pi_z \pi_y a = \pi_{zy} a$, and thus $zx \equiv zy$; therefore we have a right congruence with respect to the subgroup $\mathfrak{G}_a$ which consists of all elements of $\mathfrak{G}$ whose corresponding permutation leaves the cipher a fixed. If we call the left coset consisting of all elements x for which $\pi_x a = b$, R_b, then

$$y R_b = R_{\pi_y b} \quad \text{or also} \quad \pi_y = \binom{R_b}{y R_b}.$$

The subgroups $\mathfrak{G}_a, \mathfrak{G}_b, \ldots$ form a family of conjugate subgroups of $\mathfrak{G}$, since $x \mathfrak{G}_a x^{-1} = \mathfrak{G}_{\pi_x a}$. The same family of conjugate subgroups belongs to all equivalent transitive representations of $\mathfrak{G}$.

Conversely we assert: *If* $\mathfrak{U}$ *is a subgroup of* $\mathfrak{G}$ *and* $\mathfrak{G} = \sum_1^\omega R_i$ *is the decomposition of* $\mathfrak{G}$ *into left cosets with respect to* $\mathfrak{U}$, *then the mapping*

$$x \to \pi_x = \binom{R_i}{x R_i}$$

is a transitive representation of degree ω *of* $\mathfrak{G}$ *as a permutation group of left cosets.*

In fact $x R_i$ is also a coset, moreover

$$\pi_{xy} = \binom{R_i}{xy R_i} = \binom{R_i}{x R_i}\binom{R_i}{y R_i} = \pi_x \pi_y$$

and $\pi_e = \binom{R_i}{R_i} = \underline{1}$; therefore the π_x are permutations and the mapping $x \to \pi_x$ is a homomorphy. Transitivity follows from the remark that for every index pair i, k the equation $x R_i = R_k$ is solvable. The transitive representation just found is called *the representation belonging*

to $\mathfrak{U}$. Equivalent representations belong to conjugate subgroups and to them only.

The degree of the representation belonging to $\mathfrak{U}$ is equal to the index of $\mathfrak{U}$ in $\mathfrak{G}$.

Under the representation belonging to $\mathfrak{U}$, exactly those elements in the intersection $\mathfrak{N}$ of all the subgroups conjugate to $\mathfrak{U}$ are mapped onto $\underline{1}$. Consequently the representation group is isomorphic to $\mathfrak{G}/\mathfrak{N}$ and the representation is faithful only when $\mathfrak{N} = e$.

We denote the corresponding representation group by $\mathfrak{G}_u$ and the image of a subset $\mathfrak{R}$ of $\mathfrak{G}$ by $\mathfrak{R}_u$.

If the subgroup $\mathfrak{U}$ is of finite index in $\mathfrak{G}$, then the representation group is finite, and conversely.

The left and right representative systems of $\mathfrak{G}$ with respect to $\mathfrak{U}$ go into left and right representative systems of $\mathfrak{G}_u$ with respect to $\mathfrak{U}_u$ and conversely; therefore Theorem 3 of Chap. I. holds for infinite groups $\mathfrak{G}$.

If we set $\mathfrak{U} = e$, we obtain the regular representation of $\mathfrak{G}$ known from Chap. I., Theorem 2. The degree of the regular representation is equal to the order of $\mathfrak{G}$.

The representation group $\mathfrak{G}_e$ is transitive and every permutation in $\mathfrak{G}_e$ either leaves every cipher fixed, or leaves none fixed.

Permutation groups with the two preceding properties are called *regular permutation groups*. Regular permutation groups are their own regular representations. *Moreover, every transitive representation group of an abelian group is regular* (since every subgroup is a normal subgroup.)

The permutations π of a regular permutation group have the property that $\pi^i a = a$ implies $\pi^i = \underline{1}$.

Permutations with this last property are said to be *regular. A permutation of a finite number of ciphers is regular if and only if all its cycles are of the same length.*

A transitive permutation group consisting of regular permutations only is a regular permutation group.

How does the representation of a group $\mathfrak{H}$, properly between $\mathfrak{U}$ and $\mathfrak{G}$, look in the transitive representation group $\mathfrak{P} = \mathfrak{G}_u$?

We decompose $\mathfrak{G} = \sum_1^r G_i \mathfrak{H}$ and $\mathfrak{H} = \sum_1^s H_k \mathfrak{U}$ into left cosets and notice that the multiplication of left cosets of $\mathfrak{G}$ (with respect to $\mathfrak{U}$) by any x in $\mathfrak{G}$ permutes them in bundles: Either the cosets of $\mathfrak{G}(\mathfrak{U}r)$ in a

complex $G_i\mathfrak{H}$ are left there or they are mapped onto a complex $G_k\mathfrak{H}$ disjoint from it.

Therefore there is a decomposition of the aggregate $\mathfrak{M}$ *of the permuted objects into mutually disjoint systems* $\mathfrak{J}_1, \ldots, \mathfrak{J}_r$, *each containing* s *elements and such that the permutations in* $\mathfrak{P}$ *permute the systems* $\mathfrak{J}_1, \ldots, \mathfrak{J}_r$ *and* $r>1$, $s>1$.

We call the system $\mathfrak{J}_1, \ldots, \mathfrak{J}_r$ a family of (conjugate) *systems of imprimitivity.*

If the ciphers permuted by a transitive permutation group $\mathfrak{P}$ can be decomposed into a family of systems of imprimitivity, then $\mathfrak{P}$ is said to be imprimitive. Otherwise $\mathfrak{P}$ is said to be *primitive.*

Correspondingly, the representation of $\mathfrak{G}$ by $\mathfrak{U}$ is said to be primitive or imprimitive according as the representation group $\mathfrak{G}_\mathfrak{u}$ is primitive or imprimitive.

To a decomposition of the totality $\mathfrak{M}$ *of permuted objects of a transitive representation group* $\mathfrak{P}=\mathfrak{G}_\mathfrak{u}$ *of the group* $\mathfrak{G}$ *into a family of systems* $\mathfrak{J}_1, \ldots, \mathfrak{J}_r$ *of imprimitivity, there belongs a group* $\mathfrak{H}$ *properly between* $\mathfrak{G}$ *and* $\mathfrak{U}$ *such that the left cosets of* $\mathfrak{G}(\mathfrak{U}r)$ *in* $\mathfrak{J}_i$ *form a left coset of* $\mathfrak{G}$ *with respect to* $\mathfrak{H}$.

Let us suppose that the left coset $\mathfrak{U}$ of $\mathfrak{G}(\mathfrak{U}r)$ is in $\mathfrak{J}_1$. Then we say two *elements* of $\mathfrak{G}$ are congruent if their corresponding permutations map $\mathfrak{J}_1$ onto the same $\mathfrak{J}_j$. This is a normal congruence relation. Furthermore it follows from $\pi \equiv \varrho$ that $\sigma\pi \equiv \sigma\varrho$, and therefore that we are considering a right congruence of $\mathfrak{G}$ with respect to a group $\mathfrak{H}$ which contains $\mathfrak{U}$ in any case. From the definition of imprimitivity and transitivity of $\mathfrak{P}$ it follows that $\mathfrak{H}$ is a group properly between $\mathfrak{U}$ and $\mathfrak{G}$, thus the theorem is proven.

The transitive representation $\mathfrak{G}_\mathfrak{u}$ *is primitive if and only if* $\mathfrak{U}$ *is a maximal subgroup of* $\mathfrak{G}$. For example transitive representations of prime order are primitive.

When is a cipher system $\mathfrak{J}$ a system of imprimitivity? As a criterion for this we have: *If* $\mathfrak{J}$ *contains more than one, but not all, the permuted ciphers and if* $\pi\mathfrak{J} \subseteq \mathfrak{J}$ *whenever a permutation* π *in* $\mathfrak{P}$ *leaves a cipher of* $\mathfrak{J}$ *in* $\mathfrak{J}$, *then* $\mathfrak{J}$ *is a system of imprimitivity.*

In any case the condition is necessary. If the condition is fulfilled, then two ciphers a and b are called congruent if there is a permutation π in $\mathfrak{P}$ which maps a and b into $\mathfrak{J}$. The symmetry of the congruence is clear. Since $\mathfrak{P}$ is transitive, the congruence is reflexive. If, moreover, $\pi a, \pi b, \varrho b, \varrho c$ are contained in $\mathfrak{J}$, then $\pi\varrho^{-1}(\varrho b) \in \mathfrak{J}$, and therefore by assumption $(\pi\varrho^{-1})\varrho c \in \mathfrak{J}$, $\pi c \in \mathfrak{J}$, so that the congruence

relation is also transitive. Consequently the totality of permuted ciphers is decomposed into disjoint classes of congruent ciphers. Among these cipher systems we find $\mathfrak{J}$, since two elements in $\mathfrak{J}$ are congruent and if, on the other hand, $a \in \mathfrak{J}$, πa, $\pi b \in \mathfrak{J}$, then it follows that $\pi^{-1}(\pi a) \in \mathfrak{J}$, and therefore by assumption $\pi^{-1}(\pi b) \in \mathfrak{J}$, $b \in \mathfrak{J}$. Obviously the cipher systems found in this way are conjugate under $\mathfrak{P}$. It follows from the assumption that $\mathfrak{J}$ is a system of imprimitivity.

A cipher system $\mathfrak{J}$ of a finite number of ciphers is a system of imprimitivity if it contains more than one, but not all of the permuted ciphers, and if for a fixed cipher a_o in $\mathfrak{J}$ and all permutations π in $\mathfrak{P}$, $\pi a_0 \in \mathfrak{J}$ implies $\pi \mathfrak{J} \subseteq \mathfrak{J}$.

Proof: For every cipher a in $\mathfrak{J}$, there is a permutation ϱ in $\mathfrak{P}$ which maps a_o onto a. It follows from the assumption that $\varrho \mathfrak{J} \subseteq \mathfrak{J}$, and, since $\mathfrak{J}$ is finite, $\varrho \mathfrak{J} = \mathfrak{J}$. If $\pi a \in \mathfrak{J}$ holds for a permutation π in $\mathfrak{P}$, then $\pi \varrho a_0 \in \mathfrak{J}$, $\pi \varrho \mathfrak{J} = \pi \mathfrak{J} \subseteq \mathfrak{J}$. Now we need merely to apply the previous criterion.

THEOREM 1: *A normal subgroup $\mathfrak{N} \neq \mathfrak{1}$ of a primitive permutation group $\mathfrak{P}$ is transitive.*

Proof: Let $\mathfrak{T}$ be a system of transitivity of $\mathfrak{N}$ having at least two ciphers and let a_o be a cipher in $\mathfrak{T}$. If the permutation π in $\mathfrak{P}$ leaves the cipher a_o in $\mathfrak{T}$, then for any permutation ν in $\mathfrak{N}$, $\pi \nu \pi^{-1} = \binom{\pi a}{\pi \nu a}$ lies in $\mathfrak{N}$ and therefore whenever πa_0 lies in $\mathfrak{T}$, $\pi \nu a_0$ lies in $\mathfrak{T}$ also. Since $\mathfrak{N} a_0 = \mathfrak{T}$, we have $\pi \mathfrak{T} \subseteq \mathfrak{T}$. Since this conclusion holds for every cipher a_o in $\mathfrak{T}$, $\mathfrak{T}$ is either a system of imprimitivity of $\mathfrak{P}$, or $\mathfrak{T}$ contains all the ciphers. It follows from the assumptions that $\mathfrak{N}$ is transitive.

As examples of primitive groups we have the *multiply transitive* permutation groups.

DEFINITION: A permutation group $\mathfrak{P}$ is said to be *k-tuply transitive* if the number of permuted ciphers is at least k and for any two (ordered) k-tuples of ciphers $(a_1, \ldots, a_k)$ and $(b_1, \ldots, b_k)$ there is a permutation π in $\mathfrak{P}$ which maps a_1 onto b_1, a_2 onto b_2, $\ldots$, a_k onto b_k.

$\mathfrak{P}$ is called exactly k-tuply transitive if $\mathfrak{P}$ is k-tuply but not $k+1$-tuply transitive.

Every k-tuply transitive permutation group is transitive.

A permutation group $\mathfrak{P}$ is k-tuply transitive if for a fixed k-tuple $(1, \ldots, k)$ and every k-tuple $(a_1, \ldots, a_k)$ there is a permutation π in $\mathfrak{P}$ which maps 1 onto a_1, 2 onto a_2, $\ldots$, k onto a_k. Then for any other k-tuple $(b_1, b_2, \ldots, b_k)$, there is a permutation ϱ in $\mathfrak{P}$ which maps 1 onto b_1,

2 onto $b_2, \ldots, k$ onto b_k, and therefore $\varrho\pi^{-1}$ maps a_1 onto b_1, a_2 onto $b_2, \ldots, a_k$ onto b_k.

For example, the symmetric permutation group is the only n-tuply transitive permutation group of n ciphers.

An $(n-1)$-tuply transitive permutation group of $n \geq 2$ ciphers is also n-tuply transitive and therefore symmetric.

The alternating permutation group of $n > 2$ ciphers is exactly $(n-2)$-tuply transitive, for one of the two permutations

$$\begin{pmatrix} 1 & 2 & \ldots & n-2 & n-1 & n \\ a_1 & a_2 & \ldots & a_{n-2} & a_{n-1} & a_n \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & \ldots & n-2 & n-1 & n \\ a_1 & a_2 & \ldots & a_{n-2} & a_n & a_{n-1} \end{pmatrix}$$

is always even.

A doubly transitive permutation group $\mathfrak{P}$ is also said to be *multiply transitive* and is primitive. Since a permutation can be found in $\mathfrak{P}$ which leaves a cipher a fixed but maps a cipher b different from a onto any cipher $\neq a$, a lies in no system of imprimitivity.

A transitive permutation group $\mathfrak{P}$ is k-tuply transitive with $k > 1$ if the subgroup $\mathfrak{U}_a$ of all permutations which leave a fixed permutes the remaining ciphers in a $(k-1)$-tuply transitive manner. There is a permutation π in $\mathfrak{P}$ which maps a_1 onto a, a permutation ϱ which maps b_1 onto a and a permutation σ which leaves a fixed and maps πa_2 onto ϱb_2, πa_3 onto $\varrho b_3, \ldots,$ πa_k onto ϱb_k. But then $\varrho^{-1}\sigma\pi$ maps the cipher a_1 onto b_1, a_2 onto $b_2, \ldots, a_k$ onto b_k.

There is a conjecture that any sextuply transitive permutation group of n-th degree (and, apart from a finite number of exceptions, even any quadruply transitive permutation group of n-th degree) contains the alternating permutation group of n-th degree.

The construction of all finite multiply transitive permutation groups is an interesting but still unsolved problem.

§ 3. Operators and Operator Homomorphies

DEFINITION: *A homomorphy of a multiplicative domain into itself is called an operator (or endomorphism).*

If the image of x is denoted by x^Θ, then an operator Θ is defined as a single-valued mapping of $\mathfrak{G}$ into itself with the properties

$$x^\Theta \in \mathfrak{G}, \quad (xy)^\Theta = x^\Theta \cdot y^\Theta \text{ for all } \quad x, y \in \mathfrak{G}$$

and the product of two operators Θ_1 and Θ_2 is defined by the equation

$$x^{\Theta_1 \Theta_2} = (x^{\Theta_2})^{\Theta_1}.$$

The identity mapping of $\mathfrak{G}$ onto itself is an operator with the property

$$\underline{1}\Theta = \Theta\underline{1} = \Theta$$

for all operators Θ.

All operators of a multiplicative domain form a semi-group with a unit element.

A semi-group with unit element denoted by $\{\Omega\}$ is generated by a complex Ω of operators by adjoining a unit element and forming all possible products of elements of Ω. Every semi-group of operators which contains $\underline{1}$ and Ω also contains the domain $\{\Omega\}$ of operators generated by Ω.

DEFINITION: *The multiplicative domains* $\mathfrak{G}_1, \mathfrak{G}_2, \ldots$ *have a common operator domain* Ω *if*

1) *a multiplication is defined in* Ω,

2) *to every element* Θ *in* Ω, *there corresponds an operator* Θ *of* $\mathfrak{G}_i$,

3) *to the product* $\Theta_1\Theta_2$ *of two elements in* Ω, *there corresponds the product of the operators* Θ_1 *and* Θ_2 *in* $\mathfrak{G}_i$.

In all the following considerations a fixed common operator domain is assumed unless something else is explicitly stated.

DEFINITION: A homomorphy σ of $\mathfrak{G}$ into $\mathfrak{G}^*$ is said to be an *operator homomorphy* if

$$\sigma(x^\Theta) = (\sigma x)^\Theta$$

for all x in $\mathfrak{G}$ and for all operators Θ in the common operator domain Ω.

This relation is transitive and reflexive.

If we talk of a homomorphy we shall, if nothing is said to the contrary, mean an operator homomorphy over Ω [1]. If other homomorphies are also considered, then we shall explicitly give an operator domain belonging to them. For example a $\underline{1}$-homomorphy means an ordinary homomorphy.

DEFINITION: For a given operator domain, a multiplicative sub-domain $\mathfrak{U}$ of $\mathfrak{G}$ is said to be *admissible*[2] if for all Θ in Ω: $\mathfrak{U}^\Theta \subseteq \mathfrak{U}$.

Given two admissible multiplicative sub-domains, their intersection and the multiplicative sub-domain generated by them are also admissible.

An operator in Ω maps an admissible subdomain onto an admissible subdomain. Moreover, for an arbitrary complex $\mathfrak{R}$, the multiplicative subdomain $\{\mathfrak{R}^{\Theta_1} \cup \mathfrak{R}^{\Theta_2}, \ldots\}$, generated by the union of all $\mathfrak{R}^{\Theta_i}$ with $\Theta_i \in \Omega$ forms an admissible subdomain which contains $\mathfrak{R}$. It is called

[1] Also called an Ω-homomorphism. See JACOBSON, *Theory of Rings* (Amer. Math Soc.)
[2] Also called an Ω-subdomain. (*Ed.*)

the subdomain generated by $\mathfrak{R}$ over Ω and is denoted by $\{\mathfrak{R}\}_\Omega$. Every admissible subdomain which contains $\mathfrak{R}$ also contains $\{\mathfrak{R}\}_\Omega$.

We assume now that $\mathfrak{G}$ is a group.

Subgroups which are mapped into themselves by all operators of the entire group, are said to be *fully invariant subgroups.*

The unit element and the entire group are fully invariant subgroups.

An admissible subgroup is mapped homomorphically onto an admissible subgroup by an operator homomorphy.

This is because, for all x in $\mathfrak{U}$: $(\sigma x)^\Theta = \sigma(x^\Theta) \in \sigma\mathfrak{U}$, since $x^\Theta \in \mathfrak{U}$.

If $\bar{\mathfrak{U}}$ *is an admissible subgroup of the image domain* $\bar{\mathfrak{G}}$, *then all the elements in* $\mathfrak{G}$ *whose images lie in* $\bar{\mathfrak{U}}$ *form an admissible subgroup* $\mathfrak{U}$ *of* $\mathfrak{G}$ and $\bar{\mathfrak{U}} = \sigma\mathfrak{U}$.

Every element in $\bar{\mathfrak{U}}$ is of the form σx with x in $\mathfrak{U}$; from $x \in \mathfrak{U}, \Theta \in \Omega$ it follows that

$$\sigma x \in \bar{\mathfrak{U}} \ni (\sigma x)^\Theta = \sigma(x^\Theta),\ x^\Theta \in \mathfrak{U}.$$

In the following investigations it will be assumed that the subgroups used are admissible, if another operator domain is not explicitly assigned to the subgroup in question. For example a $\underline{1}$-group is an ordinary subgroup.

Let $\mathfrak{G}$ be a group with operator domain Ω. Given a homomorphism σ of $\mathfrak{G}$ we wish to consider the operator domain also as the operator domain of $\sigma\mathfrak{G}$ so that σ becomes an operator homomorphism.

Then $\sigma(x^\Theta) = (\sigma x)^\Theta$ for all Θ in Ω. In order that this mapping Θ be single-valued in $\sigma\mathfrak{G}$, the normal subgroup $\mathfrak{E}$ of all elements of $\mathfrak{G}$ which are mapped by σ onto σe must be admissible with respect to Ω.

If conversely the normal subgroup $\mathfrak{E}$ of all elements in the group $\mathfrak{G}$ which map onto σe under the homomorphism σ is admissible with respect to the operator domain Ω, then we define the *extension* of Ω to $\sigma\mathfrak{G}$ by the condition

$$(\sigma x)^\Theta = \sigma(x^\Theta)$$

for all Θ in Ω. Then Θ is an operator of $\sigma\mathfrak{G}$.

For it follows from $\sigma x = \sigma y$ that $x = ay$, where $a \in \mathfrak{E}$.

By assumption $a^\Theta \in \mathfrak{E}$, $(\sigma x)^\Theta = \sigma(x^\Theta) = \sigma(a^\Theta \cdot y^\Theta) = \sigma(y^\Theta)$. Moreover, $(\sigma x \cdot \sigma y)^\Theta = (\sigma(xy))^\Theta = \sigma((xy)^\Theta) = \sigma(x^\Theta \cdot y^\Theta) = \sigma(x^\Theta) \cdot \sigma(y^\Theta) = (\sigma x)^\Theta \cdot (\sigma y)^\Theta$.

Ω is a common operator domain of $\mathfrak{G}$ and $\sigma\mathfrak{G}$ since $\Theta_1\Theta_2 = \Theta_3$ in Ω over $\mathfrak{G}$ implies $(\sigma x^{\Theta_2})^{\Theta_1} = \sigma(x^{\Theta_2})^{\Theta_1} = \sigma((x^{\Theta_2})^{\Theta_1}) = \sigma x^{\Theta_3}$, and there-

fore $\Theta_3 = \Theta_1 \Theta_2$ in $\sigma\mathfrak{G}$. From the definition of Ω over $\sigma\mathfrak{G}$ it follows that σ is an operator homomorphism.

The operator domain Ω of $\mathfrak{G}$ is extended to the factor group of $\mathfrak{G}$ with respect to the admissible normal subgroup $\mathfrak{N}$ by the condition

$$(a\mathfrak{N})^{\Theta} = a^{\Theta}\mathfrak{N}$$

for all Θ in Ω.

If we regard $(a\mathfrak{N})^{\Theta}$ as a coset mod $\mathfrak{N}$ we can delete the dash without misunderstanding.

We apply the new concepts to a cyclic group $\mathfrak{G} = (A)$. *The homomorphic image of a cyclic group is cyclic.*

From $\sigma A^m = (\sigma A)^m$, it follows that $\sigma\mathfrak{G} = (\sigma A)$ and the above statement is proven. *Every subgroup of a cyclic group is admissible.*

This is because $A^{\Theta} = A^t$, and therefore

$$(A^m)^{\Theta} = (A^{\Theta})^m = A^{tm} \subseteq (A^m).$$

Every cyclic group has as many operators as it has elements.

This follows from the fact that an operator Θ is uniquely determined by its effect on A:

$$(A^m)^{\Theta} = (A^{\Theta})^m = A^{mt}.$$

Conversely, the mapping $(A^m)^{\Theta} = A^{mt}$ is an operator.

§ 4. On the Automorphisms of a Group

DEFINITIONS: An isomorphy of a group with itself is called a *meromorphy.*

As isomorphic mapping of a group onto itself is called an *automorphic mapping* (*automorphism*).

An isomorphic mapping of a group onto a subgroup is called a *meromorphic mapping* (*meromorphism*). The mapping is called a *proper* meromorphism if the subgroup is a proper subgroup.

If a group $\mathfrak{G}$ has a proper meromorphism σ, then $\mathfrak{G}$ contains the infinite and decreasing sequence of subgroups:

$$\mathfrak{G} \supset \sigma\mathfrak{G} \supset \sigma^2\mathfrak{G}, \ldots$$

A finite group, therefore, has no proper meromorphism. Every operator of the infinite cyclic group which is different from 0, ± 1, is a proper meromorphism.

The product of two proper meromorphisms is also a proper meromorphism.

All the automorphisms of a group $\mathfrak{G}$ *form a group.*

The group of automorphisms of a group $\mathfrak{G}$ without operators is denoted by $A_{\mathfrak{G}}$.

The group of automorphisms admissible over an operator domain Ω is denoted by $(A_{\mathfrak{G}})_{\Omega}$.

1. *Inner Automorphisms.*

The "transformation" of the elements of a group $\mathfrak{G}$ by a fixed element x is an automorphism. First we have the simple but important rule: $xax^{-1} \cdot xbx^{-1} = xabx^{-1}$; secondly, the transformations form a group with the identity automorphism as unit element.

We call the automorphism $\begin{pmatrix} a \\ xax^{-1} \end{pmatrix} = \begin{pmatrix} a \\ a^{\underline{x}} \end{pmatrix}$ an *inner automorphism* of the group. All the inner automorphisms of $\mathfrak{G}$ form a group $J_{\mathfrak{G}}$.

We saw previously that the mapping $x \to \underline{x}$ defines a homomorphism between $\mathfrak{G}$ and $J_{\mathfrak{G}}$. Precisely those elements in the center of $\mathfrak{G}$ are mapped onto the identity automorphism, so that we have the isomorphy

$$\mathfrak{G}/\mathfrak{z} \simeq J_{\mathfrak{G}} \tag{1}$$

The group of inner automorphisms is a normal subgroup of the group of all automorphisms. This is because for every operator Θ

$$(a^{\underline{x}})^{\Theta} = (xax^{-1})^{\Theta} = x^{\Theta} a^{\Theta} (x^{\Theta})^{-1}, \tag{2}$$

and therefore $\Theta \underline{x} = \underline{x^{\Theta}} \Theta$; and if Θ is an automorphism, then

$$\Theta \underline{x} \Theta^{-1} = \underline{x^{\Theta}}. \tag{3}$$

The factor group of $A_{\mathfrak{G}}$ over $J_{\mathfrak{G}}$ is called the group of *outer automorphisms.*

From formula (2) we see that:

An automorphism maps a series of complexes which are conjugate under $\mathfrak{G}$ onto a series of complexes which are again conjugate under $\mathfrak{G}$.

In particular, classes of conjugate elements go into classes of conjugate elements. Whether every automorphism of a finite group which maps every class of conjugate elements onto itself is an inner automorphism, is a problem which is as yet unsolved.

2. *Complete groups.*

A group is said to be complete if its center is e and every automorphism is an inner automorphism.

THEOREM 2: *The automorphism group of a simple non-abelian group is complete.*

Proof: Let $\mathfrak{G}$ be simple but non-abelian. Since the center of $\mathfrak{G}$ is a

normal abelian subgroup, it must be e. Therefore $\mathfrak{G}$ is isomorphic to the group J of inner automorphisms. We may even identify $\mathfrak{G}$ with J so that in the full automorphism group A of $\mathfrak{G}$: $\alpha x \alpha^{-1} = x^{\alpha}$ for all x in J, and $x^{\alpha} = x$ for all x implies $\alpha = 1$. Therefore the center of A is 1,and the only element in A with which all the elements of J commute is 1.

An automorphism σ of A onto itself maps J onto a normal subgroup J^{σ} of A. J^{σ} is isomorphic to J and therefore simple. The intersection of J and J^{σ} is a normal subgroup of J ,and therefore $J = J^{\sigma}$ or $J \cap J^{\sigma} = 1$.

But in the latter case J and J^{σ} commute elementwise, since $\alpha \in J$, $\beta \in J^{\sigma}$ imply:

$$\alpha\beta\alpha^{-1} \in J^{\sigma},\ \beta\alpha^{-1}\beta^{-1} \in J,$$
$$\alpha\beta\alpha^{-1}\beta^{-1} \in J \cap J^{\sigma},\ \alpha\beta\alpha^{-1}\beta^{-1} = 1,$$
$$\alpha\beta = \beta\alpha.$$

Since $J \neq 1$, we must have $J = J^{\sigma}$. Consequently the mapping $x \to x^{\sigma}$ for all x in J is a certain automorphism σ' of J. We want to prove that the automorphism σ of A is an inner automorphism and may, for this purpose, replace σ by the automorphism $\tau = \sigma'^{-1}\sigma$ of A. Now $x^{\tau} = x$ for all x in J. Therefore, $\alpha x \alpha^{-1} = x^{\alpha} \in J$ implies $\alpha^{\tau} x (\alpha^{\tau})^{-1} = (x^{\alpha})^{\tau} = x^{\alpha}$, and therefore $\alpha^{\tau} = \alpha$. Thus τ is the identity automorphism of A, Q.E.D.

Are there any simple non-abelian groups? Since every subgroup of an abelian group is a normal subgroup, it follows that:

A simple abelian group $\neq e$ is cyclic of prime order.

Conversely a group of prime order is cyclic and simple.

Thus "*simple and non-abelian*" is equivalent to "*simple of composite order.*"

THEOREM 3: *The alternating permutation group on five ciphers is simple.*

Proof: A normal subgroup of $\mathfrak{A}_5$ can be divided into classes of elements conjugate under $\mathfrak{A}_5$ among which 1 must occur, and its order divides the order of $\mathfrak{A}_5$. The classes of $\mathfrak{A}_5$, as previously shown, are: (1) The identity permutation, (2) The 15 double transpositions ,(3) The 20 3-cycles, (4) and (5) 12 5-cycles each. But no sum of two or more integers from the set 1, 15, 20, 12, 12 is a proper divisor of 60. Therefore $\mathfrak{A}_5$ contains no proper normal subgroup, as was to be proved.

Whether it is possible, starting with a finite group having e as center, to construct a complete group by repeatedly, but only a finite number of

times, constructing the automorphism group of the automorphism group previously constructed, is a problem still unsolved.

3. *Characteristic Subgroups. Centralizers.*

A subgroup of a group $\mathfrak{G}$ which is mapped into itself by all automorphisms of $\mathfrak{G}$ is said to be a *characteristic subgroup*. $\mathfrak{G}$ and e are characteristic subgroups. The subgroups admissible under all inner automorphisms are precisely the normal subgroups. Consequently, characteristic subgroups are always normal subgroups.

The center of a group is a characteristic subgroup.

Proof: Since $\mathfrak{G}^\alpha = \mathfrak{G}$ for an automorphism α and $xz = zx$ for all x implies that $x^\alpha z^\alpha = z^\alpha x^\alpha$ for all x, we have z^α in the center for each z in the center.

The factor group over the center is likewise characteristic. We can even form a series of characteristic subgroups, the *ascending central series*, by defining recursively: $\mathfrak{z}_0 = e$, $\mathfrak{z}_1 = \mathfrak{z}(\mathfrak{G})$; if $\mathfrak{z}_i$ has already been defined as a characteristic subgroup, then $\mathfrak{z}_{i+1}/\mathfrak{z}_i$ will be the center of $\mathfrak{G}/\mathfrak{z}_i$.

A group is said to be *characteristically simple* if it does not contain any proper characteristic subgroup. The investigation of the structure of the finite characteristically simple groups will later be reduced to the investigation of the structure of simple groups.

If $\mathfrak{A}$ is a group of automorphisms of the group $\mathfrak{G}$, and $\mathfrak{N}$ is a normal subgroup admissible under $\mathfrak{A}$, then we can derive the structure of $\mathfrak{A}$ from the structure of certain groups of automorphisms of $\mathfrak{G}/\mathfrak{N}$ and $\mathfrak{N}$ in the following way: All the automorphisms of $\mathfrak{A}$ which leave the elements of $\mathfrak{N}$ fixed form a normal subgroup $\mathfrak{A}_1$ of $\mathfrak{A}$. All the automorphisms of $\mathfrak{A}$ which leave the elements of $\mathfrak{G}/\mathfrak{N}$ fixed form a normal sugroup $\mathfrak{A}_2$ of $\mathfrak{A}$. By the first isomorphy theorem, $\mathfrak{A}/\mathfrak{A}_1$ is isomorphic to a group of automorphisms of $\mathfrak{N}$ and $\mathfrak{A}/\mathfrak{A}_2$ is isomorphic to a group of automorphisms of $\mathfrak{G}/\mathfrak{N}$. $\mathfrak{A}_1 \cap \mathfrak{A}_2$ consists of all the automorphisms α in $\mathfrak{A}$ such that

1) $v^\alpha = v$ for all v in $\mathfrak{N}$,

2) $x^\alpha x^{-1} \in \mathfrak{N}$ for all x in $\mathfrak{G}$.

See exercise 6 at the end of the chapter concerning this point.

Now we apply the first isomorphy theorem to the normalizer $N_{\mathfrak{U}}$ of a subgroup $\mathfrak{U}$.

The mapping $x \to \begin{pmatrix} U \\ x\,U\,x^{-1} \end{pmatrix}$ of the elements x in $N_{\mathfrak{U}}$ is a homomorphism onto a group of automorphisms of $\mathfrak{U}$.

Consequently all the elements of $\mathfrak{G}$ which commute with *every element* of $\mathfrak{U}$ form a subgroup $Z_{\mathfrak{U}}$. $Z_{\mathfrak{U}}$ is called the *centralizer* of $\mathfrak{U}$. *The centralizer of a subgroup is a normal subgroup of its normalizer and the factor group is isomorphic to a group of automorphisms of the subgroup.*

The centralizer of the whole group $\mathfrak{G}$ is equal to its center.

4. *The Φ - subgroup.*

An automorphism of the group $\mathfrak{G}$ is uniquely determined by its effect on the elements of a system of generators of $\mathfrak{G}$. In order to state this circumstance more sharply, we introduce the following concept.

DEFINITION: The set Φ of all the elements which may be deleted from every system of generators of a non-trivial group is a subgroup, *the Φ- subgroup of* $\mathfrak{G}$:

1) Since $\mathfrak{G} \neq e$, e is a member of Φ;

2) If $x \in \Phi$ and $y \in \Phi$, then it follows from $\mathfrak{G} = \{xy, \mathfrak{R}\}$ that $\mathfrak{G} = \{x, y, \mathfrak{R}\}$ and therefore $\mathfrak{G} = \{y, \mathfrak{R}\}$; therefore $\mathfrak{G} = \{\mathfrak{R}\}$; xy also belongs to Φ;

3) If $x \in \Phi$ then it follows from $\mathfrak{G} = \{x^{-1}, \mathfrak{R}\}$ that $\mathfrak{G} = \{x, \mathfrak{R}\}$ and therefore $\mathfrak{G} = \{\mathfrak{R}\}$; x^{-1} also belongs to Φ.

The Φ-subgroup is a characteristic subgroup (since every automorphism maps a system of generators onto a system of generators), hence also normal.

The Φ-subgroup is the intersection of the whole group with all of its maximal subgroups.

If $\mathfrak{D}$ is this intersection then we shall show 1) $\Phi \subseteq \mathfrak{D}$, in other words: If x does not lie in the maximal subgroup $\mathfrak{U}$ then it is not in Φ either. This is because $\{x, \mathfrak{U}\} = \mathfrak{G} \neq \mathfrak{U}$. 2) $\mathfrak{D} \subseteq \Phi$; in other words: If x does not lie in Φ, then neither does it lie in every maximal subgroup of $\mathfrak{G}$. If $\{x, \mathfrak{R}\} = \mathfrak{G} \neq \{\mathfrak{R}\}$, then x is not in $\{\mathfrak{R}\}$. By the theorem on maximal subgroups[1], there is a largest possible subgroup $\mathfrak{U}$ which contains $\mathfrak{R}$ but not x. $\mathfrak{U}$ is moreover a maximal subgroup of $\mathfrak{G}$, since any larger subgroup would contain x and $\mathfrak{R}$ and therefore also the group

$$\{x, \mathfrak{R}\} = \mathfrak{G}.$$

If every proper subgroup can be embedded in a maximal (proper) subgroup, then we have the

[1] Theorem 5, Chap. I.

BASIS THEOREM: *If a complex* $\mathfrak{K}$ *together with* Φ *generates* $\mathfrak{G}$, *then* $\mathfrak{K}$ *alone generates* $\mathfrak{G}$.

If $\{\mathfrak{K}\} \neq \mathfrak{G}$, then $\{\mathfrak{K}\}$ could be embedded in a maximal subgroup $\mathfrak{U}$. But then Φ would also lie in $\mathfrak{U}$. Therefore the group $\mathfrak{G}$ generated by $\mathfrak{K}$ and Φ would lie in $\mathfrak{U}$, which is a contradiction.

Now let $\mathfrak{G}$ be finite, $A_{\mathfrak{G}}$ the automorphism group of $\mathfrak{G}$, $\mathfrak{B}$ the normal subgroup consisting of all automorphisms which leave every coset of $\mathfrak{G}$ with respect to Φ fixed. Then $A_{\mathfrak{G}} : \mathfrak{B}$ is isomorphic to a group of automorphisms of $\mathfrak{G}/\Phi$. The factor group $\mathfrak{G}/\Phi$ has a finite number of generators $R_1, \ldots, R_d$. Since, by the basis theorem, a representative system $S_1, \ldots, S_d$ generates the whole group $\mathfrak{G}$, there are as many different systems conjugate to $S_1, \ldots, S_d$ under $\mathfrak{B}$ as there are elements in $\mathfrak{B}$. The $(\Phi : 1)^d$ representative systems decompose, therefore, into a certain number of classes of systems conjugate under $\mathfrak{B}$, such that the classes each contain $\mathfrak{B}:1$ elements. Thus we obtain the divisibility condition

$$(A_{\mathfrak{G}} : 1) \mid (\Phi : 1)^d \cdot (A_{\mathfrak{G}/\Phi} : 1). \tag{4}$$

5. *Normal and Central Operators.*

An operator is said to be a *normal operator* if

$$x\, y^{\Theta}\, x^{-1} = (x\, y\, x^{-1})^{\Theta}$$

for all x, y in $\mathfrak{G}$, i.e.:

An operator is normal if it commutes with all the inner automorphisms.

Therefore a normal operator maps a normal subgroup onto a normal subgroup.

If α is a normal automorphism, then $x^{\alpha}\, y^{\alpha}\, x^{-\alpha} = x\, y^{\alpha}\, x^{-1}$ or

$$x^{-1}\, x^{\alpha}\, y^{\alpha} = y^{\alpha}\, x^{-1}\, x^{\alpha}$$

for all x, y and, since $\mathfrak{G}^{\alpha} = \mathfrak{G}$, $x^{-1}\, x^{\alpha}$ is in the center of $\mathfrak{G}$, and conversely. An automorphism is normal if and only if it multiplies every element of $\mathfrak{G}$ by an element of the center.[1]

The mapping $x \longrightarrow x^{-1}\, x^{\alpha}$ is an operator $-1 + \alpha$, since

$$(x\, y)^{-1+\alpha} = (x\, y)^{-1}\, (x\, y)^{\alpha} = y^{-1}\, x^{-1}\, x^{\alpha}\, y^{\alpha} = x^{-1}\, x^{\alpha}\, y^{-1}\, y^{\alpha} = x^{-1+\alpha}\, y^{-1+\alpha}.$$

An operator which maps every element of the group onto a center element is said to be a *central operator*. Every central operator is normal.

6. *The Holomorph of a Group.*

[1] Because of this property a normal automorphism is also called a *center automorphism.*

Is it possible to extend a given group $\mathfrak{G}$ to a group $\mathfrak{H}$ so that every automorphism of $\mathfrak{G}$ can be induced by a transformation by an element in $\mathfrak{H}$?

Let $\mathfrak{M}$ be any group of automorphisms of $\mathfrak{G}$, and consider the set $\mathfrak{H}$ of permutations $\begin{pmatrix} x \\ y\, x^{\alpha} \end{pmatrix}$ with $x, y \in \mathfrak{G}$, $\alpha \in \mathfrak{M}$.

Then

$$\begin{pmatrix} x \\ y\, x^{\alpha} \end{pmatrix} \begin{pmatrix} x \\ z\, x^{\beta} \end{pmatrix} = \begin{pmatrix} x \\ y\, z^{\alpha} x^{\alpha\beta} \end{pmatrix}.$$

The permutations $\pi_y = \begin{pmatrix} x \\ y\, x \end{pmatrix}$ form a group $\overline{\mathfrak{G}}$ of permutations in $\mathfrak{H}$, and by I, Theorem 2, the mapping $y \to \pi_y$ gives the regular representation of $\mathfrak{G}$. $\overline{\mathfrak{G}}$ is therefore a regular permutation group which we may identify with $\mathfrak{G}$.

The permutations $\begin{pmatrix} x \\ x^{\alpha} \end{pmatrix}$ form a permutation group $\overline{\mathfrak{M}}$ in $\mathfrak{H}$ isomorphic to $\mathfrak{M}$ and we identify $\overline{\mathfrak{M}}$ with $\mathfrak{M}$.

We can verify easily that

$$\begin{pmatrix} x \\ x^{\alpha} \end{pmatrix} \begin{pmatrix} x \\ y\, x \end{pmatrix} = \begin{pmatrix} x \\ y^{\alpha}\, x \end{pmatrix} \begin{pmatrix} x \\ x^{\alpha} \end{pmatrix}, \tag{5}$$

and consequently $\mathfrak{H} = \mathfrak{G}\overline{\mathfrak{M}} = \overline{\mathfrak{M}}\mathfrak{G}$ is a group of permutations.

According to (5), transforming by $\begin{pmatrix} x \\ x^{\alpha} \end{pmatrix}$ in $\mathfrak{H}$ induces the automorphism α in $\mathfrak{G}$.

The permutation group just constructed is called the *holomorph of the automorphism group* $\mathfrak{M}$ *over* $\mathfrak{G}$. The holomorph of the group of all automorphisms over $\mathfrak{G}$ is called simply the *holomorph of* $\mathfrak{G}$.

Now we wish to start, in the reverse order, with a transitive permutation group $\mathfrak{G}$, andwe form the group $\mathfrak{H}$ of all permutations which transform $\mathfrak{G}$ onto itself.

Which automorphisms of the astract group can be induced by transformation with elements of $\mathfrak{H}$?

Let $\mathfrak{G}_i$ be the subgroup of all permutations in $\mathfrak{G}$ which leave the cipher i fixed. For a permutation π in $\mathfrak{H}$ it follows that

$$\pi \mathfrak{G}_i \pi^{-1} \leq \mathfrak{G},\ \pi \mathfrak{G}_i \pi^{-1}(\pi i) = \pi i,$$

and therefore $$\pi \mathfrak{G}_i \pi^{-1} \leq \mathfrak{G}_{\pi i},$$

likewise $$\pi^{-1} \mathfrak{G}_{\pi i} \pi \leq \mathfrak{G}_i$$

$$\mathfrak{G}_{\pi i} \leq \pi \mathfrak{G}_i \pi^{-1},$$

therefore

$$\pi \mathfrak{G}_i \pi^{-1} = \mathfrak{G}_{\pi i}.$$

Conversely, let α be an automorphism of $\mathfrak{G}$ which maps $\mathfrak{G}_1$ onto $\mathfrak{G}_i$. We wish to show that there is a permutation π in $\mathfrak{H}$ such that

$$\pi x \pi^{-1} = x^{\alpha}$$

for all x in $\mathfrak{G}$. In order to prove this we look for a permutation y in $\mathfrak{G}$ which maps i onto 1. (There are such, since $\mathfrak{G}$ is transitive.) Then $\mathfrak{G}_1^{y\alpha} = \mathfrak{G}_1$, and so without loss of generality we may replace $y\alpha$ by a new α with

$$\mathfrak{G}_1^{\alpha} = \mathfrak{G}_1$$

Let R_i be the left coset of $\mathfrak{G}$ over $\mathfrak{G}_1$ consisting of all permutations which map 1 onto i. The mapping $\begin{pmatrix} R_i \\ R_i^{\alpha} \end{pmatrix}$ is a permutation $\begin{pmatrix} R_i \\ R_{\pi i} \end{pmatrix}$ of the left cosets since $\mathfrak{G}_1^{\alpha} = \mathfrak{G}_1$.

Then

$$\begin{pmatrix} R_i \\ (x R_i)^{\alpha} \end{pmatrix} = \begin{pmatrix} R_i \\ x^{\alpha} R_i^{\alpha} \end{pmatrix} = \begin{pmatrix} R_i \\ x^{\alpha} R_{\pi i} \end{pmatrix},$$

and therefore

$$\pi x i = x^{\alpha} \pi i,$$

$$\pi x \pi^{-1} = x^{\alpha}.$$

We have as a result:

THEOREM 4: *Let $\mathfrak{H}$ be the group of all automorphisms of a transitive group $\mathfrak{G}$ which permute the subgroups $\mathfrak{G}_i$ (previously described and belonging to the given transitive representation of $\mathfrak{G}$). Then this group $\mathfrak{H}$ is precisely that induced by all transformations of $\mathfrak{G}$ by the elements of the normalizer of $\mathfrak{G}$ in the group of all permutations on the ciphers of $\mathfrak{G}$.*

We determine which permutations π in $\mathfrak{H}$ are elementwise commutative with $\mathfrak{G}$. Let $\pi^{-1} 1 = i$. By assumption $\pi R_i = R_i \pi$ and also $\pi R_i 1 = 1$; therefore $1 = R_i \pi 1$. If we set $R_i = x \mathfrak{G}_1$, then it follows that

$$\begin{aligned} x \mathfrak{G}_1 x^{-1} 1 &= x \mathfrak{G}_1 x^{-1} \cdot x \pi 1 \\ &= R_i \pi 1 = 1, \end{aligned}$$

therefore

$$\mathfrak{G}_i = x \mathfrak{G}_1 x^{-1} \leq \mathfrak{G}_1.$$

Since $\pi i = 1$, we find through similar considerations that: $\mathfrak{G}_1 \leq \mathfrak{G}_i$, and therefore $\mathfrak{G}_i = \mathfrak{G}_1$.

Conversely, let $\mathfrak{G}_i = x\,\mathfrak{G}_1 x^{-1} = \mathfrak{G}_1$ with $x \in R_i$. Since $\mathfrak{G}_1 x = x\,\mathfrak{G}_1$, the mapping $\begin{pmatrix} R_i \\ R_i x \end{pmatrix}$ is a permutation $\begin{pmatrix} R_i \\ R_{\bar{x}i} \end{pmatrix}$ of the left cosets of $\mathfrak{G}$ over $\mathfrak{G}_1$.

Since

$$\begin{pmatrix} R_i \\ y\,R_i \end{pmatrix} \cdot \begin{pmatrix} R_i \\ R_i x \end{pmatrix} = \begin{pmatrix} R_i \\ R_i x \end{pmatrix} \begin{pmatrix} R_i \\ y\,R_i \end{pmatrix} = \begin{pmatrix} R_i \\ y\,R_i x \end{pmatrix} ,$$

$\bar{x}$ commutes with all the permutations in $\mathfrak{G}$. The mapping $x \to \bar{x}^{-1}$ gives a homomorphy, between the normalizer of $\mathfrak{G}_1$ in $\mathfrak{G}$ and the group of all permutations commuting elementwise with $\mathfrak{G}$, under which $\mathfrak{G}_1$ is mapped onto $\underline{1}$.

If however π commutes with $\mathfrak{G}$ elementwise, and $\pi 1 = 1$, then

$$\pi i = \pi R_i 1 = R_i \pi 1 = R_i 1 = i,$$

and therefore $\pi = \underline{1}$.

We obtain as the result:

THEOREM 5: *The centralizer of a transitive permutation group $\mathfrak{G}$ in the group of all permutations is isomorphic to the factor group $N_{\mathfrak{G}_1}/\mathfrak{G}_1$ of the normalizer $N_{\mathfrak{G}_1}$ in $\mathfrak{G}$ of a subgroup $\mathfrak{G}_1$ which belongs to the transitive representation of $\mathfrak{G}$. It consists wholly of regular permutations.*

As a special case we obtain the THEOREM OF JORDAN: *The centralizer of a group $\mathfrak{G}$ in its holomorph consists of the permutations*

$$\varrho_y = \begin{pmatrix} x \\ x\,y^{-1} \end{pmatrix} = \begin{pmatrix} x \\ y^{-1}\,x^y \end{pmatrix},$$

which form a regular permutation group isomorphic to $\mathfrak{G}$.

Moreover it follows that the center of a primitive permutation group is $\underline{1}$, or the group consists of the powers of a cycle whose length is a prime.

A transitive permutation group $\mathfrak{H}$ which contains a regular normal subgroup $\mathfrak{G}$ is, by what has just been proven, the holomorph of the group $\mathfrak{M}$ of all permutations in $\mathfrak{H}$ which leave a cipher fixed over the group $\mathfrak{G}$.

Thus the holomorph of a group $\mathfrak{G}$ is primitive if and only if the group is characteristically simple[1], since a system of imprimitivity which contains e consists of the elements of a non-trivial characteristic subgroup of $\mathfrak{G}$.

THEOREM 6: *If the holomorph of a finite group is doubly transitive, then $\mathfrak{G}$ is abelian and there is a prime integer p such that the p-th power of every element in $\mathfrak{G}$ is equal to e.*

[1] i.e., has no proper characteristic subgroups.

Proof: It follows from the hypothesis that the automorphisms of $\mathfrak{G}$ permute transitively all the elements $\neq e$, of $\mathfrak{G}$. Therefore all the elements $\neq e$ of $\mathfrak{G}$ have the same order p. Since $\mathfrak{G} \neq e$, there are elements of prime order in $\mathfrak{G}$ and therefore p is a prime. Moreover all the normalizers of elements $\neq e$ in $\mathfrak{G}$ have the same order $\frac{\mathfrak{G}:1}{h}$. Thus there are h elements in each class of conjugate elements $\neq e$ in $\mathfrak{G}$. If there are $r+1$ classes it follows that

$$\mathfrak{G}:1 = rh + 1.$$

On the other hand h is a divisor of $\mathfrak{G}:1$; therefore $h = 1$, i.e., $\mathfrak{G}$ is abelian, Q.E.D.

THEOREM 7: *If the holomorph of a group $\mathfrak{G}$ consisting of more than three elements is triply transitive, then $\mathfrak{G}$ is abelian and the square of every element is e.*

Proof: It follows from the hypothesis that the automorphisms of $\mathfrak{G}$ permute the elements $\neq e$ in $\mathfrak{G}$ in a doubly transitive manner. If, for an x in $\mathfrak{G}$, $x^2 \neq e$, $x^3 \neq e$, then there is an automorphism which maps x onto x^2 but leaves x^3 fixed. But then $(x^2)^3 = x^3$ and therefore $x^3 = e$. If, however, $x^2 \neq e$, $x^3 = e$, then by hypothesis there is an element y in $\mathfrak{G}$ which does not lie in (x) and we can find an automorphism of $\mathfrak{G}$ which maps x^2 onto y but leaves x fixed. But then $x^2 = y$ which is a contradiction. Consequently for all x in $\mathfrak{G}$, $x^2 = e$, i.e., $x = x^{-1}$. From this it follows that $xy = x^{-1}y^{-1} = (yx)^{-1} = yx$. Therefore $\mathfrak{G}$ is abelian, Q.E.D.

If the holomorph $\mathfrak{H}$ of a group $\mathfrak{G}$ is quadruply transitive, then $\mathfrak{G}$ must consist of exactly four elements:

By the previous theorem the square of every element in $\mathfrak{G}$ is equal to e. Moreover $\mathfrak{G}$ contains at least four elements e, x, y, xy. If there were a fifth element z in $\mathfrak{G}$ then an automorphism could be found which leaves x and y fixed but maps xy onto z and this is a contradiction, which establishes the above. There does, in fact, exist a group of four elements whose holomorph is quadruply transitive. In the symmetric permutation group of four ciphers, the three double transpositions (12) (34), (13) (24), (14) (23) together with 1 form a regular normal subgroup $\mathfrak{B}_4$ of four elements, as is easily seen. ($\mathfrak{B}_4$ is called the *Klein Four Group*.)

§ 5. Normal Chains and Normal Series

Let $\mathfrak{G}$ be a group with operators.

A *normal chain of length* r is a chain of $(r+1)$ subgroups:

$$\mathfrak{G} = \mathfrak{G}_0 \geq \mathfrak{G}_1 \geq \mathfrak{G}_2 \geq \cdots \geq \mathfrak{G}_r = 1,$$

which begins with $\mathfrak{G}$ and terminates with e, and is such that every member of the chain is a normal subgroup of the preceding member. The factor groups $\mathfrak{G}_i/\mathfrak{G}_{i+1}$ $(i = 0, 1, 2, \ldots, r-1)$ are called the *factors* of the chain.

A normal chain in which successive members are different is said to be a *normal chain without repetitions.*

A normal chain is said to be a *refinement* of a given normal chain if the members of the given chain are among the members of the new chain.

THEOREM 8 (Jordan - Hölder - Schreier) : *Two given normal chains can be refined so that the series of factors of the two new chains are identical up to order and isomorphism.*

In order to carry out the proof, we ask not only if a refinement process can be found, but still more, namely :

Are there convenient methods for constructing the refinement?

Let the two given chains be:

$$\mathfrak{G} = \mathfrak{G}_0 \geq \mathfrak{G}_1 \geq \mathfrak{G}_2 \geq \cdots \geq \mathfrak{G}_r = e$$

and

$$\mathfrak{G} = \mathfrak{H}_0 \geq \mathfrak{H}_1 \geq \mathfrak{H}_2 \geq \cdots \geq \mathfrak{H}_s = e.$$

The following example shows that in general at least s–1 groups must be inserted between adjacent members of the first chain and similarly that at least r–1 groups must be inserted between adjacent members of the second chain.

Let p_{ik} $(i=1, 2, \ldots, r;\ k=1, 2, \ldots, s)$ be $r.s$ distinct prime numbers. Let $\mathfrak{G}$ be the cyclic group of order $n = \prod_{i,k} p_{ik}$. Then set

$$d_i = \prod_{k=1}^{s} p_{ik}, \qquad e_k = \prod_{i=1}^{r} p_{ik},$$

and $\mathfrak{G}_0 = \mathfrak{G}$; let $\mathfrak{G}_i$ be the subgroup of order $n/\prod_{1}^{i} d_\nu$ $(i=1, \ldots, r)$; similarly let $\mathfrak{H}_0 = \mathfrak{G}$ and let $\mathfrak{H}_k$ be the subgroup of order $n/\prod_{1}^{k} e_\mu$ $(k = 1, 2, \ldots, s)$. By inserting s–1 groups and r–1 between the adjacent members of the first and second chain respectively, both given chains can be refined so that the orders of the new factors run through all the primes p_{ik}. Since there is only one group of a given prime

order, the resulting refinements are isomorphic. On the other hand isomorphic refinements between $\mathfrak{G}_{i-1}$ and $\mathfrak{G}_i$ (or $\mathfrak{H}_{k-1}$ and $\mathfrak{H}_k$) can not contain a factor whose order is divisible by two primes, since only common factor groups of order p_{ik} or 1 can lie between $\mathfrak{G}_{i-1}, \ldots, \mathfrak{G}_i$ (and $\mathfrak{H}_{k-1}, \ldots, \mathfrak{H}_k$). The intersection of two admissible subgroups and the product of an admissible normal subgroup with an admissible subgroup are again admissible subgroups. Consequently, multiplication of an intersection lying in $\mathfrak{G}_{i-1}$ with the normal subgroup $\mathfrak{G}_i$ yields a group between $\mathfrak{G}_{i-1}$ and $\mathfrak{G}_i$. In what follows, it will be shown that the intercalation of the $s-1$ groups

$$\mathfrak{G}_{i,k} = \mathfrak{G}_i \cdot (\mathfrak{G}_{i-1} \cap \mathfrak{H}_k) \qquad (k = 1, 2, \ldots, s-1)$$

between $\mathfrak{G}_{i-1}$ and $\mathfrak{G}_i$, and of the $r-1$ groups

$$\mathfrak{H}_{i,k} = \mathfrak{H}_k \cdot (\mathfrak{H}_{k-1} \cap \mathfrak{G}_i) \qquad (i = 1, 2, \ldots, r-1)$$

between $\mathfrak{H}_{k-1}$ and $\mathfrak{H}_k$, refines the given chains isomorphically.

$\mathfrak{G}_{i,k}$ and $\mathfrak{H}_{i,k}$ are defined for $i = 1, 2, \ldots, r-1$; $k = 1, 2, \ldots, s-1$ by the above formulae. Moreover set

$$\mathfrak{G}_{i,0} = \mathfrak{G}_{i-1}, \ \mathfrak{H}_{0,k} = \mathfrak{H}_{k-1}; \quad \mathfrak{G}_{i,s} = \mathfrak{G}_i, \ \mathfrak{H}_{r,k} = \mathfrak{H}_k .$$

If it is shown that $\mathfrak{G}_{i,k}$ is a normal subgroup of $\mathfrak{G}_{i,k-1}$ $(k = 1, 2, \ldots, s)$, then the $\mathfrak{G}_{i,k}$ form a refinement of $\mathfrak{G}_i$. Correspondingly for the $\mathfrak{H}_{i,k}$. If it is shown that

$$\frac{\mathfrak{G}_{i,k-1}}{\mathfrak{G}_{i,k}} \simeq \frac{\mathfrak{H}_{i-1,k}}{\mathfrak{H}_{i,k}} \qquad \begin{pmatrix} i = 1, 2, \ldots, r \\ k = 1, 2, \ldots, s \end{pmatrix},$$

then the refinements are isomorphic. The desired results are given by the following theorem concerning four groups:

If a subgroup $\mathfrak{u}$ *is a normal subgroup of the subgroup* $\mathfrak{U}$ *of* $\mathfrak{G}$, *and the subgroup* $\mathfrak{v}$ *is a normal subgroup of the subgroup* $\mathfrak{V}$ *of* $\mathfrak{G}$, *then* $\mathfrak{u}(\mathfrak{U} \cap \mathfrak{v})$ *is a normal subgroup of* $\mathfrak{u}(\mathfrak{U} \cap \mathfrak{V})$, *and* $\mathfrak{v}(\mathfrak{V} \cap \mathfrak{u})$ *is a normal subgroup of* $\mathfrak{v}(\mathfrak{V} \cap \mathfrak{U})$; *and*

$$\frac{\mathfrak{u}(\mathfrak{U} \cap \mathfrak{V})}{\mathfrak{u}(\mathfrak{U} \cap \mathfrak{v})} \simeq \frac{\mathfrak{v}(\mathfrak{V} \cap \mathfrak{U})}{\mathfrak{v}(\mathfrak{V} \cap \mathfrak{u})}.$$

Proof: By the second isomorphism theorem $\mathfrak{u} \cap \mathfrak{V}$ is a normal subgroup of $\mathfrak{U} \cap \mathfrak{V}$ and

$$\frac{\mathfrak{U} \cap \mathfrak{V}}{\mathfrak{u} \cap \mathfrak{V}} \simeq \frac{\mathfrak{u}(\mathfrak{U} \cap \mathfrak{V})}{\mathfrak{u}}.$$

Since $\mathfrak{u} \cap \mathfrak{V}$ is a normal subgroup of $\mathfrak{U} \cap \mathfrak{V}$, so is $\mathfrak{v} \cap \mathfrak{U}$, and therefore

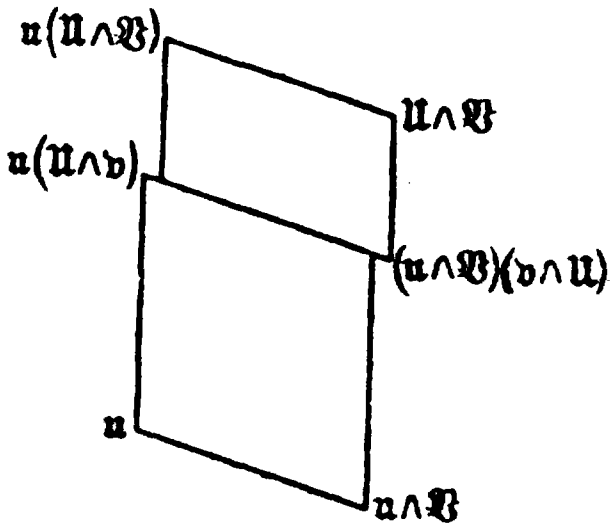
$(\mathfrak{u} \cap \mathfrak{V})\,(\mathfrak{v} \cap \mathfrak{U})$ is also a normal subgroup of $\mathfrak{U} \cap \mathfrak{V}$. Under the above isomorphy, $(\mathfrak{u} \cap \mathfrak{V})(\mathfrak{v} \cap \mathfrak{U})$ is mapped onto $\mathfrak{u}(\mathfrak{u} \cap \mathfrak{V})\,(\mathfrak{v} \cap \mathfrak{U}) = \mathfrak{u}\,(\mathfrak{v} \cap \mathfrak{U})$. Therefore by the third isomorphy theorem $\mathfrak{u}(\mathfrak{U} \cap \mathfrak{v})$ is a normal subgroup of $\mathfrak{u}(\mathfrak{U} \cap \mathfrak{V})$, and

$$\frac{\mathfrak{U} \cap \mathfrak{V}}{(\mathfrak{u} \cap \mathfrak{V})\,(\mathfrak{v} \cap \mathfrak{U})} \simeq \frac{\mathfrak{u}\,(\mathfrak{U} \cap \mathfrak{V})}{\mathfrak{u}\,(\mathfrak{U} \cap \mathfrak{v})}.$$

Since the hypotheses are symmetric, it follows likewise that $\mathfrak{v}(\mathfrak{V} \cap \mathfrak{u})$ is a normal subgroup of $\mathfrak{v}(\mathfrak{V} \cap \mathfrak{U})$ and that

$$\frac{\mathfrak{U} \cap \mathfrak{V}}{(\mathfrak{u} \cap \mathfrak{V})\,(\mathfrak{v} \cap \mathfrak{U})} \simeq \frac{\mathfrak{v}\,(\mathfrak{V} \cap \mathfrak{U})}{\mathfrak{v}\,(\mathfrak{V} \cap \mathfrak{u})},$$

from which we obtain the desired isomorphy.



The method of proof can be made more meaningful by means of a diagram which shows the position of the groups occurring in the proof. In order to do this let a line between two groups, one of which is above the other, mean that the group at the upper end contains the group at the lower end of the line.

The given method of refinement, applied for a second time, gives no new refinement of the first refinement. Nevertheless it may refine isomorphic chains still further.

Example: Let $\mathfrak{G}$ be cyclic of order 12. Let $\mathfrak{G}_1$ be the subgroup of order 6, $\mathfrak{H}_1$ the one of order 2. $\mathfrak{G}_2 = \mathfrak{H}_2 = e$. Then

$$\mathfrak{G}_{2,1} = \mathfrak{H}_1, \quad \mathfrak{H}_{1,1} = \mathfrak{G}_1.$$

A refinement is said to be a *proper refinement* if a new subgroup of $\mathfrak{G}$ actually occurs in the new chain.

A normal chain is said to be a *normal series* if it has no proper refinements.

If $\mathfrak{G}$ has a normal series then by the theorem of Jordan - Hölder - Schreier it follows that every normal chain can be refined so as to give a normal series. The series of factors in different normal series is identical up to sequence and isomorphy.

The existence of a normal series is assured if the *double chain condition of group theory* holds:

[1] Often called a *Hasse diagram*.

1. *Minimal condition*: In every decreasing sequence of subgroups $\mathfrak{U}_1 \geq \mathfrak{U}_2 \geq \ldots$ there is an index after which all the members are equal.

Equivalent to this is:

1. a) In every set of subgroups there is a subgroup which contains no other subgroup of the set.

2. *Maximal condition*: In every increasing sequence of groups $\mathfrak{U}_1 \leq \mathfrak{U}_2 \leq \mathfrak{U}_3 \leq \ldots$ there is an index after which all the members are equal.

2. a) In every set of subgroups there is a subgroup which is contained in no other subgroup of the set.

From the maximal condition it follows that $\mathfrak{G}$ contains a largest normal subgroup $\mathfrak{G}_1$ or is equal to e, that $\mathfrak{G}_1$ contains a largest normal subgroup $\mathfrak{G}_2$ or is equal to e, etc. It follows from the minimal condition that this sequence terminates at e after a finite number of steps. The normal chain thus obtained is a normal series.

If, conversely, every admissible subgroup is a normal subgroup of $\mathfrak{G}$, then the double chain theorem follows from the existence of a normal series.

The normal series in group theory have received different names, depending on the underlying domain of operators:

1. *Composition Series*: Every member of the chain

$$\mathfrak{G} = \mathfrak{G}_0 \geq \mathfrak{G}_1 \geq \cdots \geq \mathfrak{G}_{r-1} \geq \mathfrak{G}_r = e$$

which is different from $\mathfrak{G}$ is a maximal normal subgroup of the previous member.

2. *Principal Series*: Every member of the chain different from $\mathfrak{G}$ is a normal subgroup of $\mathfrak{G}$, maximal in the set of all proper subgroups of the preceding member.

3. *Characteristic Series*: Every member of the chain different from $\mathfrak{G}$ is a characteristic subgroup of $\mathfrak{G}$, maximal in the set of proper subgroups of the preceding member.

As an example we shall determine the *structure of the symmetric and the alternating permutation groups.*

The following theorem is useful when investigating the simplicity of a group.

THEOREM 9: *A transitive and primitive permutation group* $\mathfrak{G}$ *which contains no proper regular normal subgroups, and in which the subgroup of all permutations which leave a cipher fixed is simple, must itself be simple.*

Proof: By Theorem 1 of this chapter, any normal subgroup $\mathfrak{N}$ other than $\underline{1}$, of the primitive permutation group $\mathfrak{G}$ is transitive. Let $\mathfrak{G}_1$ be the group of all permutations of $\mathfrak{G}$ which leave the cipher 1 fixed. Since $\mathfrak{N}$ is assumed not to be regular, the intersection $\mathfrak{N}_1$ of $\mathfrak{N}$ with the group $\mathfrak{G}_1$ is distinct from $\underline{1}$. According to the 2nd isomorphy theorem $\mathfrak{N}_1$ is a normal subgroup of $\mathfrak{G}_1$, and inasmuch as $\mathfrak{G}_1$ is simple by hypothesis, we must have $\mathfrak{N}_1 = \mathfrak{G}_1$. Since $\mathfrak{N}$ is transitive,

$$\mathfrak{G} = \mathfrak{N}\,\mathfrak{G}_1 = \mathfrak{N}\,\mathfrak{N}_1 = \mathfrak{N},$$

as was to be proved.

THEOREM 10:[1] *The alternating permutation group of* $n \neq 4$ *ciphers is simple.*

Proof: $\mathfrak{A}_1$, $\mathfrak{A}_2$, $\mathfrak{A}_3$ are of orders 1, 1, 3, and are therefore simple. By Theorem 3, $\mathfrak{A}_5$ is simple. Now assume that we know that $\mathfrak{A}_{n-1}$ is simple and $n>5$. Then $\mathfrak{A}_n$ is quadruply transitive, therefore primitive, and according to the remark following Theorem 7, $\mathfrak{A}_n$ contains no regular normal subgroups.

The subgroup of all permutations in $\mathfrak{A}_n$ which leave the cipher n fixed permutes the remaining ciphers $1, \ldots, n-1$ as $\mathfrak{A}_{n-1}$ does, and thus is simple by the induction assumption. By the preceding theorem $\mathfrak{A}_n$ itself is simple, as was to be shown.

THEOREM 11: *If* $n \neq 4$, $n > 2$, *then the symmetric permutation group* $\mathfrak{S}_n$ *has exactly the one composition series.*

$$\mathfrak{S}_n > \mathfrak{A}_n > e.^2$$

Proof: If $n > 2$, then $\mathfrak{S}_n$ is doubly transitive and therefore primitive; consequently a proper normal subgroup $\mathfrak{N}$ of $\mathfrak{S}_n$ is transitive. By the second isomorphy theorem $\mathfrak{N} \cap \mathfrak{A}_n$ is a normal subgroup of $\mathfrak{A}_n$, moreover $\mathfrak{N} : \mathfrak{N} \cap \mathfrak{A}_n / 2$, while the transitivity of $\mathfrak{N}$ implies $\mathfrak{N} \cap \mathfrak{A}_n \neq \underline{1}$. If moreover $n \neq 4$, then because of the previously proven simplicity of $\mathfrak{A}_n$

$$\mathfrak{N} \cap \mathfrak{A}_n = \mathfrak{A}_n,$$

and therefore $\mathfrak{N} = \mathfrak{A}_n$, as was to be shown.

By the same method of proof, it follows that for a proper normal subgroup $\mathfrak{N}$ of $\mathfrak{A}_4$, the intersection $\mathfrak{N}_1 = \mathfrak{N} \cap \mathfrak{A}_4$ is a normal subgroup $\neq \underline{1}$ of $\mathfrak{A}_4$. Since $\mathfrak{A}_4$ is doubly transitive, $\mathfrak{N}_1$ is transitive. Therefore the order of $\mathfrak{N}_1$ is divisible by 4. Either $\mathfrak{N}_1$ contains 3-cycles so that $\mathfrak{N}_1 = \mathfrak{A}_4$, or $\mathfrak{N}_1$ consists of double transpositions and $\underline{1}$. $\mathfrak{A}_4$ actually con-

[1] With the help of Exercise 9 at the end of the chapter, the reader can develop the usual proof of Theorem 10.

[2] Naturally this is also the principal series, indeed the characteristic series.

tains the transitive normal subgroup $\mathfrak{B}_4$ which consists of the three double transpositions and $\mathfrak{1}$. The subgroup $\mathfrak{S}_3$ of all permutations which leave the cipher 4 fixed can be taken as a representative system of $\mathfrak{S}_4$ over $\mathfrak{B}_4$ and so we finally obtain: *Every composition series of* $\mathfrak{S}_4$ *begins with* $\mathfrak{S}_4 > \mathfrak{A}_4 > \mathfrak{B}_4$.

Since the abelian group $\mathfrak{B}_4$ contains three proper subgroups, $\mathfrak{S}_4$ has three different compositions series.

§ 6. Commutator Groups and Commutator Forms

We saw on page 9 that there are groups in which the commutative law $ab=ba$ does not hold. If we wish nevertheless to calculate in an arbitrary group $\mathfrak{G}$ in commutative fashion we must create a multiplicative normal congruence relation between its elements for which the condition

$$ab \equiv ba \tag{1}$$

holds. By page 24 the congruence relation sought is the congruence in $\mathfrak{G}$ with respect to a normal subgroup $\mathfrak{G}'$, consisting of all elements which are to be congruent to e. From the proposed congruence, we conclude, upon multiplication by the congruence $(ba)^{-1} \equiv (ba)^{-1}$, that all elements $ab(ba)^{-1}$ must be in $\mathfrak{G}'$.

DEFINITION: The element $ab\,a^{-1}b^{-1}$ is called the *commutator* of the elements a, b and is denoted by (a, b).

According to the defining equation,

$$ab = (a, b)\,ba \tag{2}$$

the commutator indicates the deviation from the commutative law.

The subgroup generated by all the commutators is called the *commutator subgroup* of $\mathfrak{G}$, and is denoted by $D\,\mathfrak{G}$ or by $\mathfrak{G}'$.

If we actually wish to calculate commutatively in $\mathfrak{G}$, then we must look upon two elements as congruent if their quotient lies in the commutator group. However if we do this, we calculate in an abelian manner, since from (2) it follows that

$$ab \equiv ba\ (D\,\mathfrak{G}l)$$

and from $a \equiv b,\ c \equiv d$ it follows that

$$ac \equiv bc \equiv cb \equiv db \equiv bd\ (D\,\mathfrak{G}l).$$

The commutator group is the smallest normal subgroup with an abelian factor group.

The commutator group is invariant under every operator of the given group, since

$$(3) \qquad (a, b)^{\Theta} = (a\,b\,a^{-1}\,b^{-1})^{\Theta} = a^{\Theta}\,b^{\Theta}\,(a^{\Theta})^{-1}(b^{\Theta})^{-1} = (a^{\Theta}, b^{\Theta}),$$

and therefore $\mathfrak{G}'^{\Theta}$ lies in $\mathfrak{G}'$.

We now define higher commutator groups ("higher derivatives") recursively , setting

$$D^0\,\mathfrak{G} = \mathfrak{G}$$

$$D^1\,\mathfrak{G} = D\,\mathfrak{G} = \mathfrak{G}',$$

$$D^2\,\mathfrak{G} = D\,\mathfrak{G}' = \mathfrak{G}'',$$

$$\cdots\cdots\cdots\cdots$$

$$D^r\,\mathfrak{G} = D(D^{r-1}\,\mathfrak{G}).$$

It is clear that the r-th commutator group $D^r\mathfrak{G}$ is a fully invariant ant subgroup of $\mathfrak{G}$ and that the successive factor groups of the normal subgroup chain:

$$\mathfrak{G} = D^0\,\mathfrak{G} \geq \mathfrak{G}' = D^1\,\mathfrak{G} \geq D^2\,\mathfrak{G} \ldots \geq D^r\,\mathfrak{G}$$

are abelian.

For a subgroup $\mathfrak{U}$ of $\mathfrak{G}$ it follows from the definition of the commutator group that

$$D\,\mathfrak{U} \leq D\,\mathfrak{G}$$

and by induction

$$D^r\,\mathfrak{U} \leq D^r\,\mathfrak{G}.$$

For the factor group over a normal subgroup $\mathfrak{N}$ we have

$$D^r\,(\mathfrak{G}/\mathfrak{N}) = (D^r\,\mathfrak{G})\,\mathfrak{N}/\mathfrak{N}.$$

The usefulness of these concepts is obvious from the following

DEFINITION: A group $\mathfrak{G}$ is said to be *solvable*, if the series of higher commutator groups terminates with e.

To a solvable group $\mathfrak{G} \neq e$ there corresponds a uniquely defined number k such that $D^k\,\mathfrak{G} = e$, $D^{k-1}\,\mathfrak{G} \neq e$. Since in the normal chain: $\mathfrak{G} > D^1\,\mathfrak{G} > D^2\,\mathfrak{G} > \ldots > D^k\,\mathfrak{G} = e$ just k abelian factor groups different from e appear, we say that the group $\mathfrak{G}$ is *k-step metabelian*.

The group consisting of only the unity element is said to be 0-step metabelian. The 1-step metabelian groups are exactly the abelian groups $\neq e$.

It follows immediately from our remarks above that *every subgroup and every factor group of a k-step metabelian group is itself at most k-step metabelian.*

If the group $\mathfrak{G}$ has a normal chain

$$\mathfrak{G} = \mathfrak{G}_0 \geq \mathfrak{G}_1 \geq \mathfrak{G}_2 \geq \cdots \geq \mathfrak{G}_k = e$$

which has only abelian factor groups $\mathfrak{G}_i/\mathfrak{G}_{i+1}$, then $\mathfrak{G}$ is at most k-step metabelian since $\mathfrak{G}' \leq \mathfrak{G}_1$, because $\mathfrak{G}/\mathfrak{G}_1$ is abelian, and it follows by induction that $D^r\mathfrak{G} \leq \mathfrak{G}_r$, $D^k\mathfrak{G} = e$.

Since the higher derivatives are fully invariant in $\mathfrak{G}$, and the subgroups and factor groups of an abelian group are themselves abelian, it follows from the Jordan - Hölder - Schreier theorem that the factor groups of a normal series of a solvable group are abelian.

Since an abelian group is simple if and only if it is of prime order, it follows that:

A solvable group has a composition series if and only if it is finite. A finite group is solvable if and only if its composition factors are cyclic of prime order.

The following rules hold for calculation with commutators:

(4) $$(a, b) = e$$

is equivalent to $$ab = ba,$$

and in particular, we have

(4a) $$(e, a) = (a, e) = e$$

(4b) $$(a, a) = e.$$

(5) $$(a, b)\,(b, a) = e,$$

(6) $$aba^{-1} = b^a = (a, b)\,b,$$

$$(a, b) = a^{1-b} = b^{a-1},$$

(7) $$(ab, c) = (b, c)^a\,(a, c)$$

(8) $$(a, bc) = (a, b)\,(a, c)^b.$$

If the commutator group lies in the center, then rules (7) and (8) can be simplified to

(7a) $$(ab, c) = (a, c)\,(b, c)$$

(8a) $$(a, bc) = (a, b)\,(a, c),$$

in particular

(9) $$(a^n, c) = (a, c^n) = (a, c)^n.$$

From this we can derive the useful power rule:

For (a, b) *in the center of the group,*

$$(ab)^n = (b, a)^{\frac{1}{2}n(n-1)} a^n b^n \tag{10}$$

Proof: For $n = 0$ the rule is trivially true. Now let $n > 0$ and assume we have already proven

$$(ab)^{n-1} = (b, a)^{\frac{1}{2}(n-1)(n-2)} a^{n-1} b^{n-1}.$$

Now
$$(ab)^n = (ab)^{n-1} \cdot ab$$
$$a^{n-1} b^{n-1} ab = a^{n-1} (b^{n-1}, a)\, ab^n$$
$$= a^{n-1} (b, a)^{n-1} ab^n \qquad \text{by (9)}$$
$$= (b, a)^{n-1} a^n b^n, \quad \text{since } (b, a) \text{ is in the center}$$

and therefore
$$(ab)^n = (b, a)^{\frac{1}{2}(n-1)(n-2)} (b, a)^{n-1} a^n b^n,$$

from which the rule follows for positive n. For negative exponents the rule follows from the equations

$$(ab)^{-n} = (b^{-1} a^{-1})^n, \quad a^n b^n = (a^n, b^n) b^n a^n$$
$$= (a, b)^{n^2} b^n a^n = (b, a)^{-n^2} b^n a^n.$$

The *mutual commutator group* $(\mathfrak{U}, \mathfrak{V})$ of two complexes $\mathfrak{U}$ and $\mathfrak{V}$ of given group $\mathfrak{G}$ is the subgroup generated by all the commutators (U, V) where $U \in \mathfrak{U}$, $V \in \mathfrak{V}$.[1] $\mathfrak{U}$ commutes with $\mathfrak{V}$ elementwise if and only if $(\mathfrak{U}, \mathfrak{V}) = e$.

From (5) we have

$$(\mathfrak{U}, \mathfrak{V}) = (\mathfrak{V}, \mathfrak{U}). \tag{11}$$

If $\mathfrak{U}$ and $\mathfrak{V}$ are normal subgroups of $\mathfrak{G}$ then it follows from (3) and (6) that $(\mathfrak{U}, \mathfrak{V})$ is a normal subgroup of $\mathfrak{G}$ and is contained in $\mathfrak{U} \cap \mathfrak{V}$. Then by (7) and (8), for an arbitrary complex $\mathfrak{K}$:

$$(\mathfrak{K}\mathfrak{U}, \mathfrak{V}) = (\mathfrak{U}, \mathfrak{V})\,(\mathfrak{K}, \mathfrak{V}), \tag{12}$$

$$(\mathfrak{U}, \mathfrak{K}\mathfrak{V}) = (\mathfrak{U}, \mathfrak{K})\,(\mathfrak{U}, \mathfrak{V}). \tag{13}$$

Let $\mathfrak{K}_1$ and $\mathfrak{K}_2$ be two complexes, $\mathfrak{U}_1$, $\mathfrak{U}_2$ the subgroups generated by them.

THEOREM 12: *The normal subgroup* $\mathfrak{N}$ *of* $\mathfrak{G}$ *generated by* $(\mathfrak{K}_1, \mathfrak{K}_2)$ *is equal to the normal subgroup* $\mathfrak{N}_1$ *of* $\mathfrak{G}$ *generated by* $(\mathfrak{U}_1, \mathfrak{U}_2)$.

Proof: In any case $\mathfrak{N}$ is contained in $\mathfrak{N}_1$. We must show that

[1] If confusion with the commutator is to be feared then we write $\{(\mathfrak{U}, \mathfrak{V})\}$.

$\mathfrak{N}=e$ implies $\mathfrak{N}_1=e$[1]. In fact, then $\mathfrak{K}_1$, $\mathfrak{K}_2$ commute elementwise and from (4), (7), (8) it follows that $\mathfrak{U}_1$, $\mathfrak{U}_2$ commute elementwise, as was to be shown.

It is useful to introduce higher commutators,e.g.,

$$(a, b, c) = (a, (b, c)) \tag{14}$$

$$(a_1, a_2, \ldots, a_n) = (a_1, (a_2, \ldots, a_n)) \tag{15}$$

$$(a, b; c, d) = ((a, b), (c, d)). \tag{16}$$

Rules (7) and (8) can now be written

$$(ab, c) = (a, b, c)\,(b, c)\,(a, c) \tag{7b}$$

$$(a, bc) = (a, b)\,(b, a, c)\,(a, c). \tag{8b}$$

In order to understand these multiple commutators completely we define recursively a "linear expression of weight w and type s", in symbols $x_1, x_2, \ldots, x_w$. The linear expression of weight 1 in x is the symbol x itself. Let this correspond to type 0. As a separating symbol of the first type we use a comma; for the second type, a semi-colon; for the third type, a triple point $\vdots$; and in general for the sth type the symbol $\textcircled{s}$ is used. Now let $w > 1$ and assume that all the linear expressions of weight $< w$ are defined, and let a type correspond to each of them. Then we define expressions $(f_1 \textcircled{s} f_2)$ as linear expressions of weight w and of type $s > 0$ where f_1 is of weight w_1 in $x_1, x_2, \ldots, x_{w_1}$ and of type s_1, and f_2 is of weight w_2 in $x_{w_1+1}, x_{w_1+2}, \ldots, x_{w_1+w_2}$ and of type s_2, such that $w = w_1 + w_2$, $s = \mathbf{Max}\,(s_1 + 1, s_2)$. The weight is therefore simply the number of symbols in the "linear expression" and the type is equal to the highest type of separation symbol.

If $f\ (x_1, \ldots, x_w)$ is a linear expression of weight w and type s, then for arbitrary elements $G_1, \ldots, G_w$ in the group $\mathfrak{G}$ we define:

$f\ (G_1, \ldots, G_w)$ is a *commutator of weight w and type s in the* G_i. Moreover for arbitrary subgroups $\mathfrak{U}_1, \mathfrak{U}_2, \ldots \mathfrak{U}_w$ we define: $f(\mathfrak{U}_1, \mathfrak{U}_2, \ldots, \mathfrak{U}_w)$ is a *commutator form of weight w and of type s in the* $\mathfrak{U}_i$.

In the successive construction of corresponding linear expressions the separation symbols are to indicate commutator formation. E.g.,

$D\mathfrak{G} = (\mathfrak{G}, \mathfrak{G})$ is of weight 2 and type 1,

$D^2\mathfrak{G} = (\mathfrak{G}, \mathfrak{G}; \mathfrak{G}, \mathfrak{G})$ is of weight 4 and type 2,

$D^r\mathfrak{G} = (D^{r-1}\mathfrak{G} \textcircled{r} D^{r-1}\mathfrak{G})$ is of weight 2^r and type r

in the components $\mathfrak{G}, \mathfrak{G}, \ldots, \mathfrak{G}$.

[1] We calculate in the factor group $\mathfrak{G}/\mathfrak{N}$!

If the complexes $\mathfrak{K}_1, \ldots, \mathfrak{K}_w$ are transformed into themselves by every element in $\mathfrak{G}$, then every commutator form formed from them is a normal subgroup of $\mathfrak{G}$, since from (3) it follows, by induction on the weight w, that for each operator Θ of $\mathfrak{G}$:

$$(3\,a) \qquad (f(G_1, G_2, \ldots, G_w))^{\Theta} = f(G_1^{\Theta}, G_2^{\Theta}, \ldots, G_w^{\Theta}).$$

If the subgroup generated by the complex $\mathfrak{K}_i$ is equal to the normal subgroup $\mathfrak{N}_i$ of $\mathfrak{G}$ then we actually have:

THEOREM 13: *The commutator form* $f(\mathfrak{N}_1, \mathfrak{N}_2, \ldots, \mathfrak{N}_w)$ *is equal to the subgroup* $\mathfrak{N}$ *of* $\mathfrak{G}$, $\mathfrak{N}$ *being generated by all the elements* $f(N_1, \ldots, N_w)$ *with* $\mathfrak{N}_i$ *in* $\mathfrak{K}_i$.

Proof: For $w = 1$ the theorem is clear. Let $w > 1$ and assume that the theorem is proven for commutator forms of lower weight.

$f = (f_1 \circledS f_2)$, where the weights w_1, w_2 of f_1, f_2 are lower than w. By the induction hypothesis,

$$f_1(\mathfrak{N}_1, \mathfrak{N}_2, \ldots, \mathfrak{N}_{w_1}) \text{ is generated by all } f_1(N_1, \ldots, N_{w_1}),$$
$$f_2(\mathfrak{N}_{w_1+1}, \mathfrak{N}_{w_1+2}, \ldots, \mathfrak{N}_w) \text{ is generated by all } f_2(N_{w_1+1}, \ldots, N_w).$$

Now the statement of the theorem follows from Theorem 12. From the previous definitions and the last theorem the following "substitution principle" follows immediately:

If $f(y_1, y_2, \ldots, y_\omega)$ *is a linear expression of weight* ω *and if* $\varphi_i(x_1^{(i)}, x_2^{(i)}, \ldots, x_{w_i}^{(i)})$ $(i = 1, 2, \ldots, \omega)$ *are linear expressions of weight* w_i, *then* $f(\varphi_1, \varphi_2, \ldots, \varphi_\omega)$ *is a linear expression* g *of weight* $w = w_1 + w_2 + \ldots + w_\omega$ *in* $x_1^{(1)}, \ldots, x_{w_1}^{(1)}, \ldots, x_{w_\omega}^{(\omega)}$ [1]. *For normal subgroups*

$$\mathfrak{N}_\nu^{(i)} \; (\nu = 1, 2 \ldots w_i;\; i = 1, 2 \ldots \omega)$$

of a group $\mathfrak{G}$, *we have*

$$g(\mathfrak{N}_\nu^{(i)}) = f(\mathfrak{M}_1, \mathfrak{M}_2 \ldots \mathfrak{M}_\omega),$$

where $\mathfrak{M}_i = \varphi_i(\mathfrak{N}_1^{(i)}, \ldots, \mathfrak{N}_{w_i}^{(i)})$.

In a group $\mathfrak{G}$ with abelian commutator group $\mathfrak{G}'$ we have the following important rule:

$$(17) \qquad (a, b, c)\,(b, c, a)\,(c, a, b) = e,$$

which we derive in the following way:

[1] The type of the separating symbols in f may have to be raised by the substitution.

$$c(a,b)c^{-1} = (a,b)^c = (c,a,b)\,(a,b)$$
$$= cac^{-1}\cdot cbc^{-1}\cdot(cbc^{-1}\cdot cac^{-1})^{-1}$$
$$= (c,a)a\cdot(c,b)b\cdot((c,b)b\,(c,a)a)^{-1}$$
$$= (c,a)\,(a,c,b)\,(c,b)ab\,((c,b)\,(b,c,a)\,(c,a)ba)^{-1}.$$

(17a) $(c,a,b)\,(a,b) = (c,a)\,(a,c,b)\,(c,b)\,(a,b)\,(c,a)^{-1}(b,c,a)^{-1}(c,b)^{-1}.$

Since $\mathfrak{G}'$ is abelian we have

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

and moreover by (8) $\quad (a,e) = e = (a,b,c)\,(a,c,b),$

and therefore finally we have (17). Now we can prove the following important theorem.

THEOREM 14: *In a group $\mathfrak{G}$ with the three normal subgroups $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$, each of the three normal subgroups $(\mathfrak{A}, \mathfrak{B}, \mathfrak{C})$, $(\mathfrak{B}, \mathfrak{C}, \mathfrak{A})$, $(\mathfrak{C}, \mathfrak{A}, \mathfrak{B})$ is contained in the product of the two others.*

Proof: We may assume that $(\mathfrak{A}, \mathfrak{B}, \mathfrak{C})\cdot(\mathfrak{B}, \mathfrak{C}, \mathfrak{A}) = e$, and must then prove that $(\mathfrak{C}, \mathfrak{A}, \mathfrak{B}) = e$. By Theorem 13, $(\mathfrak{C}, \mathfrak{A}, \mathfrak{B})$ is generated by all (c, a, b) where $a \in \mathfrak{A}$, $b \in \mathfrak{B}$, $c \in \mathfrak{C}$, so that we must prove $(c, a, b) = e$. In any case $(\mathfrak{A}, \mathfrak{B}, \mathfrak{C}) = (\mathfrak{B}, \mathfrak{C}, \mathfrak{A}) = e$, and therefore also $(\mathfrak{A}, \mathfrak{C}, \mathfrak{B}) = e$. In formula (17a) we may insert $(a, c, b) = (b, c, a) = e$, so that

(18) $$(c,a,b)\,(a,b) = (c,a)\,(c,b)\,(a,b)\,(c,a)^{-1}\,(c,b)^{-1}.$$

Since $\mathfrak{A}$ is a normal subgroup, $(\mathfrak{A}, \mathfrak{B}) \leq \mathfrak{A}$, and therefore, $(\mathfrak{A}, \mathfrak{B}; \mathfrak{B}, \mathfrak{C}) = e$ and $(\mathfrak{A}, \mathfrak{C}; \mathfrak{B}, \mathfrak{C}) = e$. Since $\mathfrak{B}$ is a normal subgroup, $(\mathfrak{A}, \mathfrak{B}) \leq \mathfrak{B}$, $(\mathfrak{A}, \mathfrak{B}; \mathfrak{C}, \mathfrak{A}) = e$. The factors on the right of (18) may be permuted so that we finally obtain $(c, a, b) = e$.

§ 7. On the Groups of an Algebra

In this paragraph we give a short survey of the groups occurring in an algebra and of groups with operators.

1. *Modules.*

A commutative group in which the symbol of combination is written as the $(+)$ symbol, is called a ***module***.

Consequently, the *sum* of two *summands* a and b is denoted by $a+b$. The following laws must then be valid for this *addition*:

I. $a+(b+c) = (a+b)+c$.
II. There is a null element 0 with the property $0+a=a$ for all a.
III. The equation $x+a=b$ is solvable for all pairs a, b.
IV. $a+b=b+a$.

As we saw earlier, it follows from this that in a sum of a finite number of summands the order and parenthesizing can be changed arbitrarily, without altering the value of the sum.

A sum consisting of the n summands $a_1, \ldots, a_n$ is written

$$a_1+a_2+\ldots+a_n \text{ or } \sum_1^n a_i .$$

Addition has a unique inverse, i.e., the equation $x+a=b$ has exactly one solution for each pair a, b. By the commutative law, the equation $a+x=b$ is equivalent to $x+a=b$. Zero has the property: $0+a=a$, $a+0=a$ and it is uniquely defined by any of these equations. The solution of $x+a=0$ is denoted by $-a$ and is uniquely determined. We have

$$a+-a=-a+a=0$$

and therefore $$-(-a)=a$$

The *difference* $a+(-b)$ of a and b will be denoted by $a-b$.

The sum of n equal summands a is denoted by $n\,a$. $0a$ is defined as 0 and $(-n)\,a$ is defined as $-(n\,a)$.

Then we have rules analogous to the power rules:

$$n\,(a+b)=n\,a+n\,b\,, \tag{1}$$

$$(n+m)\,a=n\,a+m\,a\,, \tag{2}$$

$$(n\,m)\,a=n\,(m\,a), \tag{3}$$

for all rational integers n, m. Consequently the mapping $a \to n\,a$ is an operator $\underline{n}$ of the module such that the rules for calculation

$$\underline{n+m}=\underline{n}+\underline{m} \tag{4}$$

$$\underline{n\,m}=\underline{n}\,\underline{m} \tag{5}$$

are valid. $\underline{1}$ leaves each element fixed; $\underline{0}$ maps each element onto 0.

For example, the rational integers $0, \pm 1, \pm 2, \ldots$ form a module $\mathfrak{o}$. $\mathfrak{o}$ is additively generated by 1 and is therefore cyclic; moreover $\mathfrak{o}$ is infinite.

By I § 5, the *submodules* of $\mathfrak{o}$ are exactly the modules (n), consisting of all multiples $m\,n$ of the non-negative rational integer n.

Two numbers are said to be *congruent* mod (n) if their difference is in (n) and therefore divisible by n. The number of residue classes of $\mathfrak{o}$ with respect to (n) is n if $n > 0$. They form a module $\mathfrak{o}(n)$, the *factor-module* of $\mathfrak{o}$ with respect to (n).

For an arbitrary module $\mathfrak{M}$, all the rational integers m for which $m=0$ form a submodule of $\mathfrak{o}$, the so-called *exponential module* of $\mathfrak{M}$. The non-negative rational integer generating the exponential module is

called the *characteristic* of the module. For example, the factor-module $\mathfrak{o}/(n)$ is of characteristic n.

The *sum* $\mathfrak{m}_1+\mathfrak{m}_2$ of two submodules $\mathfrak{m}_1, \mathfrak{m}_2$ of $\mathfrak{M}$ consists of all sums $a_1 + a_2$ with $a_i \in \mathfrak{m}_i$. It is a submodule.

The sum of the two submodules (n) and (m) of $\mathfrak{o}$ is generated by the *greatest common divisor* (g. c. d.) (n, m) of n and m. The intersection of (n) and (m) is generated by the *least common multiple* of n and m (l. c. m.) From the second isomorphy theorem it follows that

$$n.\, m=(n, m).\ (\text{l. c. m. } (n, m))$$

The *maximal submodules* of $\mathfrak{o}$ are exactly the submodules generated by the prime natural numbers.

2. *Rings.*

DEFINITION: A *ring* is a module in which besides addition, a multiplication of elements is defined such that

1. $a\ (b\ c)=(a\ b)\ c$ (associative law)
2. $a\ (b+c)=a\ b+a\ c$ (left distributive law)
   $(b+c)\ a=b\ a+c\ a$ (right distributive law).

Thus a ring is an abelian group in which a right and a left operator is associated with each element.

In particular,

$$a.\ 0=0.\ a=0,\ a.\ -b=-a.\ b=-(a.\ b).$$

DEFINITION: The admissible subgroups of a ring are said to be *ideals.*

A *right ideal* is a submodule in which ϱa is contained in the submodule if ϱ is in the submodule; similarly a left ideal is a submodule which contains $a\lambda$ if it contains λ, where a in each case runs through all the elements of the ring $\mathfrak{S}$.

A submodule which is at the same time a right and left ideal is said to be a *two-sided ideal.*

As the *product* $\mathfrak{m}_1\mathfrak{m}_2$ of two submodules $\mathfrak{m}_1, \mathfrak{m}_2$ of a ring $\mathfrak{S}$ we define the set of all finite sums

$$a_1b_1 + a_2b_2 + \cdots + a_rb_r\ ,$$

where $a_i \in \mathfrak{m}_1$, $b_i \in \mathfrak{m}_2$, r arbitrary.

With this definition, $\mathfrak{m}_1\,\mathfrak{m}_2$ first becomes a submodule of $\mathfrak{S}$.

The sum, intersection and product of two ideals of the same sort are also ideals of this same sort.

The residue classes (cosets) over a right– (left–) ideal have $\mathfrak{S}$ as a right– (left–) domain of operators. The residue classes with respect to a two-sided ideal form a ring, the factor-ring, where the residue class R_{ab} is defined as the product of the residue classes R_a and R_b.

The ring $\mathfrak{f}$ is said to be *homomorphic* to the ring $\mathfrak{S}$ if there is a single-valued mapping σ of $\mathfrak{S}$ on $\mathfrak{f}$ such that $\sigma(a+b)=\sigma a+\sigma b$, $\sigma(ab)=\sigma a\cdot\sigma b$. If the mapping is one-one, then $\mathfrak{f}$ is said to be isomorphic to $\mathfrak{S}$.

Here the first isomorphy theorem reads:

A ring $\mathfrak{f}$ homomorphic to the ring $\mathfrak{S}$ is isomorphic to the residue class ring of $\mathfrak{S}$ with respect to the two-sided ideal consisting of all the elements of $\mathfrak{S}$ which are mapped onto 0 *by the homomorphic mapping of $\mathfrak{S}$ onto $\mathfrak{f}$.*

An example of a ring is the operator domain of a module $\mathfrak{M}$. An operator Θ of $\mathfrak{M}$ is a single-valued mapping of $\mathfrak{M}$ into itself such that $\Theta(a+b)=\Theta a+\Theta b$. The product of two operators is defined by $(\Theta_1\Theta_2)a=\Theta_1(\Theta_2 a)$ which we encountered previously; on the other hand the sum is defined by $(\Theta_1+\Theta_2)a=\Theta_1 a+\Theta_2 a$. One can easily show that the operators of $\mathfrak{M}$ form a ring with the unit element $\underline{1}$.

3. *Division Rings,*[1] *Commutative Rings, and Fields.*

DEFINITION: A ring in which the elements different from zero form a multiplicative group is said to be a *division ring.*

This would follow from the additional conditions:

3. There are at least two different elements;

4. The equations $a.x=b$ and $y.a=b$ are solvable if $a\neq 0$. (If $a\neq 0$, $b\neq 0$, then the equations $ae=a$ and $bx=e$ are solvable and give $abx=ae=a\neq 0$, therefore $ab\neq 0$. Thus the non-zero elements form a semi-group which is actually a group because of 4.)

A ring is said to be a *commutative ring* if the commutative law for multiplication holds in it.

A commutative ring which is at the same time a division ring is called a *field.*

For example all the rational numbers, as well as the domain of all real numbers, form a field.

DEFINITION: The *center* of a ring is the (commutative) ring of all elements which commute with every element of the ring.

The center of a division ring is a field.

[1] Also called skew fields, *s*-fields, non-commutative fields, etc. (*Ed.*)

In a commutative ring with unit element, the residue class ring with respect to an ideal is a field if and only if the ideal is maximal.

For example, the set of all the rational integers form a commutative ring $\mathfrak{o}$. Every submodule of $\mathfrak{o}$ is also an ideal of $\mathfrak{o}$. The residue class ring of $\mathfrak{o}$ with respect to the ideal (n) is a field if and only if n is a prime. Therefore for every prime p we obtain a field k_p of p elements.

In an arbitrary division ring K, all the elements obtainable from 1 by combinations of the four operations form a sub-field k, the *prime field* of K. Either none of the sums $1, 1+1, 1+1+1, \ldots$ is equal to zero in K, in which case k is isomorphic to the field of rational numbers, or a sum $1+1+\ldots+1$ is equal to zero, in which case k is isomorphic to a field k_p of p elements.

The characteristic of a division ring is equal to the characteristic of its prime field and is therefore zero or a natural prime, since from $n\,a=0$, $a\neq 0$ *it follows that* $n=0$.

4. $\mathfrak{S}$-*Modules.*

DEFINITION: A module with a ring $\mathfrak{S}$ as operator domain is said to be an $\mathfrak{S}$-*module.*

We define in greater detail:

The module $\mathfrak{M}$, given a ring $\mathfrak{S}$, is said to be a *left* $\mathfrak{S}$-*module* if a multiplication of elements α in $\mathfrak{S}$ with elements u in $\mathfrak{M}$ is uniquely defined so that

1. $\alpha u \in \mathfrak{M}$,
2. $\alpha(u+v)=\alpha u+\alpha v$,
3. $(\alpha+\beta)u=\alpha u+\beta u$,
4. $(\alpha\beta)u=\alpha(\beta u)$.

We also speak of an $\mathfrak{S}$-module in the case where $\mathfrak{S}$ is only a semi-group in which case requirement 3. becomes meaningless.

$\mathfrak{M}$ is said to be a *proper* $\mathfrak{S}$-module if 5. $\mathfrak{S}\mathfrak{M}=\mathfrak{M}$; 6. $\alpha\mathfrak{M}=0$, $\mathfrak{M}\neq 0$, imply $\alpha=0$.

If $\mathfrak{S}$ contains a unit element 1, then condition 5. is equivalent to condition 5a): $1.\mathfrak{M}=\mathfrak{M}$. 5a) is equivalent to 5b): $1.u=u$ for all u.

If $\mathfrak{S}$ is a division ring, then condition 5. suffices to make $\mathfrak{M}$ a proper $\mathfrak{S}$-module: for from $\alpha\mathfrak{M}=0$ and $\alpha\neq 0$ we would have $\mathfrak{S}\alpha\mathfrak{M}=0$, and since $\mathfrak{S}\alpha=\mathfrak{S}$, then $\mathfrak{S}\mathfrak{M}=0$.

The concept of a right $\mathfrak{S}$-module is defined similarly, the module being multiplied on the right.

An $\mathfrak{S}$-module $\mathfrak{M}$ is said to be a *finite* $\mathfrak{S}$-*module* if $\mathfrak{M}$ can be generated over $\mathfrak{S}$ by a finite number of its elements, and therefore if there are a finite number of elements $u_1, \ldots, u_n$ in $\mathfrak{M}$ such that every element in $\mathfrak{M}$ is of the form

$$u = \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n$$

with $\alpha_i \in \mathfrak{S}$.

Examples of $\mathfrak{S}$-modules are the *n-dimensional* $\mathfrak{S}$-*vector module* consisting of all ordered n-tuples $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ (*vectors*) with *components* α in $\mathfrak{S}$, among which only a finite number are different from zero[1], and with the calculation rules

$$(\alpha_1, \alpha_2, \ldots, \alpha_n) + (\beta_1, \beta_2, \ldots, \beta_n) = (\alpha_1 + \beta_1, \alpha_2 + \beta_2, \ldots, \alpha_n + \beta_n)$$

$$\alpha(\alpha_1, \alpha_2, \ldots, \alpha_n) = (\alpha\alpha_1, \alpha\alpha_2, \ldots, \alpha\alpha_n).$$

If $\mathfrak{S}$ contains a unit element 1, then the n-dimensional $\mathfrak{S}$-vector module over $\mathfrak{S}$ is generated by the n *unit vectors*

$$u_i = (0, \ldots, 0, 1, 0, \ldots, 0) \qquad (i = 1, 2, \ldots, n).$$

The u_i are then called a *basis* of the $\mathfrak{S}$-module.

In an arbitrary $\mathfrak{S}$-module $\mathfrak{M}$, the expression $\alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_r u_r$ is called a *linear combination* of the u_i. The elements $u_1, u_2, \ldots, u_r$ are said to be *linearly independent* if

1. $u_i \neq 0$ $(i = 1, \ldots, r)$
2. $\alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_r u_r = 0$ implies $\alpha_i u_i = 0, i = 1, 2, \ldots, r.$

Now we generalize the definition of basis. A system $\mathfrak{B}$ of elements $u_1, u_2, \ldots, u_\omega$ is said to be an $\mathfrak{S}$-*basis system* if each element of $\mathfrak{M}$ is of the form $u = \alpha_{\nu_1} u_{\nu_1} + \cdots + \alpha_{\nu_r} u_{\nu_r}$ and every finite set of elements $u_{\nu_1}, u_{\nu_2}, \ldots, u_{\nu_r}$ is linearly independent $(\nu_1 < \nu_2 < \cdots < \nu_r)$.

If a module $\mathfrak{M}$ over a division ring K has a finite basis, then it is a vector module:[2]

Since $K\mathfrak{M} = \mathfrak{M}$, $\mathfrak{M}$ is a proper K-module. If, moreover, $u_1, u_2, \ldots, u_n$ is the basis, then it follows from $\alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n = 0$ that $\alpha_i u_i = 0$. If we were to have $\alpha_i \neq 0$ then $\alpha_i^{-1}(\alpha_i u_i) = 1 u_i = u_i = 0$. Therefore we must have $\alpha_i = 0$ $(i = 1, 2, \ldots, n)$. Every element of $\mathfrak{M}$ can be represented in only one way as $\alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n$.

[1] The number n can be any ordinal number whatsoever.

[2] More precisely: is operator-isomorphic to an $\mathfrak{S}$-vector module.

THEOREM 15: *For any division ring K, every proper K-module* $\mathfrak{M} \neq 0$ *has a basis.*

Proof: With the help of transfinite induction we shall give a method of construction only. The reader can carry out the proof himself without difficulty.

We first pick a system of generators $v_1, v_2, \ldots, v_\omega$ of $\mathfrak{M}$ over K, for example, $\mathfrak{M}$ itself, for which we can assume that $v_1 \neq 0$ and that the indices $1, 2, \ldots, \omega$ are well ordered. Let $\mathfrak{M}_\mu$ be the K-module of all linear combinations of the elements $v_1, v_2, \ldots, v_\mu$. We wish to define a basis system $\mathfrak{B}_\mu$ of $\mathfrak{M}_\mu$. In order to do this, let $\mathfrak{B}_1$ be the set consisting of v_1 alone. Moreover let $\nu > 1$ and let $\mathfrak{B}_\mu$ be defined for all $\mu < \nu$. Let Σ_ν be the union of all $\mathfrak{B}_\mu$ with $\mu < \nu$, and let $\mathfrak{m}_\nu$ be the K-module: union of all $\mathfrak{M}_\mu$ with $\mu < \nu$. One can show easily that Σ_ν is a K-basis for $\mathfrak{m}_\nu$. Now we define: $\mathfrak{B}_\nu = \Sigma_\nu$ if $v_\nu \in \mathfrak{m}_\nu$ but $\mathfrak{B}_\nu =$ the union of Σ_ν and v_ν if $v_\nu \notin \mathfrak{m}_\nu$.

Then $\mathfrak{B}_\omega$ is the desired basis system.

It is shown in the theory of linear algebra that for a division ring K the dimension of a finite K-vector module $\mathfrak{M}$ is uniquely determined (also see Chap. III. § 2).

The dimension of $\mathfrak{M}$ over K is denoted by $[\mathfrak{M}/K]$ or simply by $[\mathfrak{M}]$.

The dimension of a K-module in $\mathfrak{M}$ is at most equal to the dimension of $\mathfrak{M}$. If the dimension of $\mathfrak{M}$ is finite then a K-module in $\mathfrak{M}$ is identical with $\mathfrak{M}$ if and only if their dimensions are equal. Consequently, then, the double chain theorem holds in $\mathfrak{M}$ over the operator domain K.

If k is a division subring in K, then K can be conceived of as a proper left k-module. The dimension of K over k is called the *degree* of K over k. If K is a finite k-module, then K is said to be a *finite extension* of k.

In this case, the elements of K can be represented uniquely in the form

$$\Theta = \lambda_1 u_1 + \lambda_2 u_2 + \cdots \lambda_n u_n$$

where $\lambda_i \in k$ and $u_1, u_2, \ldots, u_n$ is a basis of K over k. If k contains q elements, then K contains q^n elements.

5. *$\mathfrak{S}$-Rings, Hypercomplex Systems.*

Let $\mathfrak{S}$ be a ring with unit element, $\mathfrak{M}$ an $\mathfrak{S}$-vector module with the basis $u_1, u_2, \ldots, u_\omega$.

We wish to make $\mathfrak{M}$ into a ring such that

$$(\lambda u) \cdot v = \lambda (u \cdot v), \tag{6}$$

$$u_i \cdot (\lambda v) = \lambda (u_i \cdot v) \qquad (i = 1, 2, \ldots, \omega) \tag{7}$$

$$(\lambda \in \mathfrak{S};\ u, v \in \mathfrak{M}).$$

A ring with this structure is said to be an $\mathfrak{S}$-*ring*.

If we have the $\mathfrak{S}$-ring given, then we shall have

$$u_i u_k = \sum_1^\omega \gamma_{ikv} u_v \tag{8}$$

with only a finite number of γ_{ikv} in $\mathfrak{S}$ different from zero. Every element in $\mathfrak{M}$ is uniquely of the form

$$u = \sum_1^\omega \alpha_i u_i \tag{9}$$

with only a finite number of α_i in $\mathfrak{S}$ different from zero. If v is a second element of the kind, of the form $\sum_1^\omega \beta_i u_i$, then

$$u \cdot v = \sum_{i,k=1}^{\omega} (\alpha_i u_i) \cdot (\beta_k u_k) = \sum_{i,k=1}^{\omega} \alpha_i \beta_k \cdot (u_i u_k)$$

$$\sum_1^\omega \alpha_i u_i \cdot \sum_1^\omega \beta_i u_i = \sum_{v=1}^{\omega} \Big(\sum_{i,k=1}^{\omega} \alpha_i \beta_k \gamma_{ikv}\Big) u_v . \tag{10}$$

Then the equations $(u_i \cdot u_k) \cdot u_l = u_i \cdot (u_k \cdot u_l)$ are equivalent to the *associativity relations*:

$$\sum_{v,\mu=1}^{\omega} \gamma_{ikv}\gamma_{vl\mu} = \sum_{v,\mu=1}^{\omega} \gamma_{klv}\gamma_{iv\mu} \qquad (i,k = 1,2,\ldots,\omega). \tag{11}$$

The equations $(u_i \cdot u_k) \cdot (\lambda u_l) = \lambda (u_i \cdot u_k \cdot u_l)$ are equivalent to the relations

$$\sum_{v,\mu=1}^{\omega} \gamma_{ikv}\lambda\gamma_{vl\mu} = \sum_{v,\mu=1}^{\omega} \lambda\gamma_{ikv}\gamma_{vl\mu} \qquad (i,k = 1,2,\ldots,\omega;\ \lambda \in \mathfrak{S}). \tag{12}$$

If conversely a system of "*combination constants*" γ_{ikv} is given such that the relations (11), (12) are fulfilled, and if we then define multiplication in accordance with (9), (10), we have made $\mathfrak{M}$ into a ring which satisfies the two conditions (6), (7).

Conditions (7) are certainly fulfilled if the γ_{ikv} are in the center of the ring $\mathfrak{S}$. For example, let $\mathfrak{M}$ be the $\mathfrak{S}$-vector module with the basis elements $x^0 = 1$, $x^1 = x$, x^2, x^3, . . . and with the rule of combination $x^n \cdot x^m = x^{n+m}$. The ring defined by this is called the *polynomial domain of one variable* x over $\mathfrak{S}$ and is denoted by $\mathfrak{S}[x]$. Every element of $\mathfrak{S}[x]$ is uniquely of the form

$$f(x) = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \cdots + \alpha_0 , \tag{13}$$

with $\alpha_i \in \mathfrak{S}$ and $\alpha_n \neq 0$, if $n>0$. The number n is called the *degree of the polynomial* $f(x)$ if $f(x) \neq 0$.

The $\mathfrak{S}$-matrix rings are other examples of $\mathfrak{S}$ rings.

Let $\mathfrak{M}$ be the n-dimensional left vector module with basis $u_1, u_2, \ldots, u_n$. We wish to find all the operators σ of $\mathfrak{M}$ which map $\mathfrak{M}$ into itself operator-homomorphically with respect to $\mathfrak{S}$. Accordingly we define: A *linear transformation* σ of $\mathfrak{M}$ is a single-valued mapping $u \to u\sigma$ of $\mathfrak{M}$ into itself such that

$$(u+v)\sigma = u\sigma + v\sigma, \tag{14}$$

$$(\alpha u)\sigma = \alpha(u\sigma). \tag{15}$$

Therefore we have

$$u_i\sigma = \alpha_{i1}u_1 + \alpha_{i2}u_2 + \cdots + \alpha_{in}u_n \tag{16}$$

and for

$$u = \sum_1^n \lambda_i u_i$$

$$u\sigma = \sum_{k=1}^{n} \Big(\sum_{i=1}^{n} \lambda_i \alpha_{ik}\Big) u_k . \tag{17}$$

Conversely, every system of elements α_{ik} $(i, k=1, 2, \ldots, n)$ in $\mathfrak{S}$ defines a linear transformation of $\mathfrak{M}$ uniquely by means of the above formulae.

We order the n^2 elements α_{ik} in a square configuration

$$A = \begin{pmatrix} \alpha_{11}\alpha_{12}\cdots\alpha_{1n} \\ \alpha_{21}\alpha_{22}\cdots\alpha_{2n} \\ \cdots\cdots\cdots \\ \alpha_{n1}\alpha_{n2}\cdots\alpha_{nn} \end{pmatrix} = (\alpha_{ik})$$

and call this configuration *the matrix of n-th degree associated with* σ.

According to the earlier definitions and statements, the linear transformations of $\mathfrak{M}$ form a ring.

If

$$u_i\sigma = \sum_{k=1}^{n} \alpha_{ik}u_k \qquad (i=1,2,\ldots,n)$$

$$u_i\tau = \sum_{k=1}^{n} \beta_{ik}u_k, \qquad (i=1,2,\ldots,n)$$

then we defined

$$u_i(\sigma+\tau) = u_i\sigma + u_i\tau = \sum_{k=1}^{n}(\alpha_{ik}+\beta_{ik})u_k, \quad . \tag{18}$$

$$u_i(\sigma\tau) = (u_i\sigma)\tau = (\sum_{\nu=1}^{n}\alpha_{i\nu}u_\nu)\tau = \sum_{\nu=1}^{n}\alpha_{i\nu}(u_\nu\tau) = \sum_{k=1}^{n}(\sum_{\nu=1}^{n}\alpha_{i\nu}\beta_{\nu k})u_k. \tag{19}$$

Accordingly we define the sum and product of the matrices

$$A = (\alpha_{ik}), \quad B = (\beta_{ik}) \quad :$$

$$A + B = (\alpha_{ik} + \beta_{ik}) \quad ,$$

$$AB = (\sum_{\nu=1}^{n}\alpha_{i\nu}\beta_{\nu k}).$$

All the matrices of the n-th degree with coefficients in the ring $\mathfrak{S}$ *with unit element form a ring* M_n *isomorphic to the ring of all linear transformations of the n-dimensional* $\mathfrak{S}$*-vector module.*

M_n is said to be a *matrix ring of n-th degree over* $\mathfrak{S}$. M_n is an $\mathfrak{S}$-ring.

The basis elements are n^2 *matrix unities* e_{ik} $(i, k=1, 2, \ldots, n)$, where e_{ik} is the matrix which has a 1 at the intersection of the i-th column and k-th row, and otherwise all zeros. The multiplication rules of the matrix unities are

$$e_{ik}e_{rs} = \delta_{kr}e_{is} \tag{20}$$

$$\left(i, k, r, s = 1, 2, \ldots, n; \delta_{kr} = \begin{cases} 1, & \text{if } k = r \\ 0, & \text{if } k \neq r \end{cases}\right).$$

The unit element of M_n is the identity matrix $E = \begin{pmatrix} 1 & & 0 \\ & 1 & \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$

The zero element is the matrix of all zeros.

If the ring $\mathfrak{S}$ of matrix coefficients is commutative, then one usually applies the linear transformation σ of the vector module $\mathfrak{M}$ on the left, so that σ is a single-valued mapping of $\mathfrak{M}$ into itself for which

1. $\sigma(u+v) = \sigma u + \sigma v$,
2. $\sigma(\alpha u) = \alpha\sigma u$.

Moreover we set, differing from (16) above,

$$\sigma u_k = \sum_{1}^{n}\alpha_{ik}u_i, \qquad (k=1, 2, \ldots, n) \tag{21}.$$

but define the associated matrix again as

$$A_\sigma = (\alpha_{ik}). \quad .$$

Since $\mathfrak{S}$ is now a commutative ring, the mapping $\sigma \rightarrow A_\sigma$ is again an isomorphism between the ring of linear transformations of $\mathfrak{M}$ and the matrix ring M_n.

A k-ring over a field k is called a *hypercomplex system.*

An example is the *group ring* of a given finite group $\mathfrak{G}$ over a field k. As a basis of the k-ring we take the finite number of elements of $\mathfrak{G}$, and as a multiplication rule we take the multiplication table of $\mathfrak{G}$.

6. *Galois Fields.*

A field with a finite number of elements is called a *Galois field.*

The number of elements of the prime field k contained in a Galois field K is finite, and is therefore a natural prime p. Since K contains only a finite number of elements, K is a finite extension of k. *The number of elements in a Galois field is thus a prime power* $\mathfrak{p}^n$. *The exponent* n *is equal to the degree of* K *over the prime field consisting of* p *elements.*

In order to investigate the multiplicative group of a Galois field, we need the

LEMMA: *A finite group must be cyclic if, for every natural number* n, *it has at most* n *elements whose* n*-th power is* e.[1]

Proof: Let $\mathfrak{G}$ have the order N; let $\mathfrak{Z}$ be the cyclic group with order N. An element in $\mathfrak{G}$ generates a cyclic subgroup $\mathfrak{U}$ whose order d is a divisor of N. It was shown earlier that $\mathfrak{Z}$ contains exactly one cyclic subgroup $\mathfrak{V}$ of order d. The d-th power of each of the d elements of $\mathfrak{U}$ is e; therefore by hypothesis $\mathfrak{U}$ contains all the elements of $\mathfrak{G}$ whose d-th power is e. Since $\mathfrak{U}$ and $\mathfrak{V}$ have the same structure, $\mathfrak{G}$ contains at most as many elements of order d as $\mathfrak{Z}$ does. This holds for every divisor of N. Since $\mathfrak{G}:1 = \mathfrak{Z}:1$, $\mathfrak{G}$ and $\mathfrak{Z}$ contain the same number of elements of order d. $\mathfrak{Z}$ contains an element of order N and therefore $\mathfrak{G}$ contains one also, Q.E.D.

In a field, according to a familiar theorem, the equation $x^n = 1$ has at most n different solutions. Therefore by the preceding lemma, the multiplicative group of any finite field is cyclic.

The multiplicative group of a Galois field is cyclic.

In the proof of the following theorem some acquaintance with cyclotomic polynomials is assumed.

THEOREM 16: *A finite division ring is a field.*

Witt's Proof: Let K be a division ring with a finite number of elements. If k is a division ring contained in K then K is a finite k-module, and by 4. the number of elements of K is a power of the number of elements of k.

[1] Equivalently: For each given index, or for each given order, there is only one subgroup.

The center of K is (as was shown earlier) a field; say it has q elements. Then K consists of q^n different elements. All the elements of K which commute with an element a form a division ring k_a, which contains the center of K. Therefore k_a contains q^d elements, where d is a positive divisor of n. We decompose the multiplicative group of K into classes of conjugate elements and obtain as the class equation

$$q^n - 1 = (q-1) + \sum_{\substack{\text{some} \\ 0<d<n}}^{d/n} \frac{q^n-1}{q^d-1}.$$

Each summand $\frac{q^n-1}{q^d-1}$ and the number q^n—1 are divisible by $\varphi_n(q)$ where $\varphi_n(x)$ is the n-th cyclotomic polynomial. Therefore q-1 is also divisible by $\varphi_n(q)$. If $n>1$, then in the decomposition $\varphi_n(q) = \prod_1^{\varphi(n)}(q-\zeta_i)$, where the ζ_i are the primitive *n-th* roots of unity, each factor is greater than q-1 in absolute value, and therefore $\varphi_n(q)$ is also greater than q-1 in absolute value. Therefore $n=1$ and K is identical with its center, as was to be shown.

7. *Near-Rings and Near-Fields.*

We wish to add the operators of a given group $\mathfrak{G}$ and investigate the rules of combination which will obtain.

Single-valued mappings $\binom{x}{x^\pi}$ of a group into itself are added in the following way:

$$x^{\pi+\varrho} = x^\pi \cdot x^\varrho.$$

In general this addition is not commutative. All the single-valued mappings of $\mathfrak{G}$ into itself form an additive group. Moreover we know that they form a multiplicative semi-group.

In the domain $\Pi_{\mathfrak{G}}$ of all single-valued mappings of $\mathfrak{G}$ into itself, we also have the right distributive law

$$(\pi+\varrho)\sigma = \pi\sigma + \varrho\sigma,$$

which can be verified immediately. The left distributive holds for all π, ϱ in $\Pi_{\mathfrak{G}}$ if and only if σ is an operator belonging to $\mathfrak{G}$.

Under what conditions is the sum of two operators an operator?

When, therefore, is

$$(xy)^{\Theta_1+\Theta_2} = x^{\Theta_1+\Theta_2} \cdot y^{\Theta_1+\Theta_2}$$

for two operators Θ_1, Θ_2 ?

Since by definition

$$(x\,y)^{\Theta_1+\Theta_2} = (x\,y)^{\Theta_1}\,(x\,y)^{\Theta_2} = x^{\Theta_1}\,y^{\Theta_1}\,x^{\Theta_2}\,y^{\Theta_2},$$

we have

$$x^{\Theta_2}\cdot y^{\Theta_1} = y^{\Theta_1}\cdot x^{\Theta_2}$$

as a necessary and sufficient condition.

DEFINITION: Two operators Θ_1, Θ_2 are said to be *additive* if $\mathfrak{G}^{\Theta_1}$ commutes with $\mathfrak{G}^{\Theta_2}$ elementwise.

The sum of two operators is an operator if and only if the summands are additive. For additive operators Θ_1, Θ_2, addition is commutative: $\Theta_1+\Theta_2=\Theta_2+\Theta_1$, as is immediately seen. The sum of n operators is certainly additive if the summands are pairwise additive. The sum of pairwise additive operators is independent of order or parenthesizing.

It is precisely the center operators that are additive with respect to any operator. (If Θ is additive with respect to $\underline{1}$, then x^{Θ} is in the center of $\mathfrak{G}$). Two automorphisms are additive if and only if $\mathfrak{G}$ is abelian.

In the domain $\Pi_{\mathfrak{G}}$ with operators of $\mathfrak{G}$ as multipliers, almost all the ring axioms are fulfilled. We call such a domain a *near-ring*.

The axioms which must be fulfilled in a (left-) near-ring are:

I. A near-ring F is an additive group, not necessarily commutative.

II. There is a multiplier domain $\mathfrak{M}$ in F, such that for every element μ in $\mathfrak{M}$ and α in F the product $\mu\alpha$ is defined uniquely as an element in F. The following rules hold:

$$(\mu\mu')\alpha = \mu(\mu'\alpha) \qquad (\mu, \mu' \in \mathfrak{M})$$

$$\mu(\alpha+\beta) = \mu\alpha + \mu\beta \qquad (\alpha, \beta \in F).$$

The *near-fields* are special near-rings. A near-field is a near-ring whose multiplier domain forms a group. If 1 is the identity element of $\mathfrak{M}$, then we should have $1\cdot\alpha=\alpha$ for all $\alpha\in F$, and we should have the cancellation law:

$$\mu\alpha = \mu'\alpha,\ \alpha \neq 0$$

implies

$$\mu = \mu'.$$

The multiplicative group $\mathfrak{M}$ of a near-field F is mapped isomorphically onto a group of automorphisms of the additive groups of F by the mapping $\mu \to \begin{pmatrix} \alpha \\ \mu\alpha \end{pmatrix}$. Because of the cancellation law we have a group of regular automorphisms.[1]

[1] An automorphism is said to be *regular* if it permutes regularly the group elements different from the identity. A *regular automorphism group* is a group consisting entirely of regular automorphisms.

If conversely a regular automorphism group $\mathfrak{M}$ of a group $\mathfrak{G}$, which contains at least two elements, is given, then we consider $\mathfrak{G}$ as an additive group, find a non-zero element, denote it by 1, and introduce the notation $\mu = \mu(1)$ for all μ in $\mathfrak{M}$. Since $\mathfrak{M}$ is regular, the notation is single-valued. Now we define multiplication by the statement $\mu\alpha = \mu(\alpha)$ for all μ in $\mathfrak{M}$. Then we have found a near-field F with the additive group $\mathfrak{G}$ and the multiplicative group $\mathfrak{M}$.

The holomorph of $\mathfrak{M}$ over $\mathfrak{G}$ is the group of all permutations $\begin{pmatrix} \alpha \\ \mu\alpha+\beta \end{pmatrix}$ of elements of F.

This permutation group can be formed for every near-field F and is denoted by $\mathfrak{P}_F$. $\mathfrak{P}_F$ is transitive and each permutation in $\mathfrak{P}_F$ either leaves all of the elements of F fixed or leaves at most one element of F fixed. In order to prove the last property we must show that

$$\mu\alpha+\beta=\alpha,\ \mu\alpha'+\beta=\alpha',\ \alpha \neq \alpha',$$

implies $\mu = 1, \beta = 0$. In fact

$$\alpha-\alpha' = \mu\alpha-\mu\alpha' = \mu(\alpha-\alpha'),$$

and since $\alpha-\alpha' \neq 0$, we find $\mu = 1$. Since $\alpha+\beta=\alpha$, we have $\beta = 0$.

The permutations $\begin{pmatrix} \alpha \\ \alpha+\beta \end{pmatrix}$ form a regular normal subgroup of $\mathfrak{P}_F$ isomorphic to the additive group of F.

If conversely the permutation group $\mathfrak{P}$ contains a regular normal subgroup $\mathfrak{G}$ and each permutation leaves either all or at most one cipher fixed, then we can consider the group $\mathfrak{P}$ as a holomorph of a certain automorphism group $\mathfrak{M}$ over $\mathfrak{G}$ because of a remark in § 4, 6. Because of the second assumption, $\mathfrak{M}$ is a group of regular automorphisms. Consequently we can construct a near-field F with additive group $\mathfrak{G}$ and with $\mathfrak{M}$ as multiplier group, so that $\mathfrak{P} = \mathfrak{P}_F$.

A near-ring in which every element is a multiplier is said to be a *complete near-ring* or in accordance with a suggestion of Mr. Wieland a *stem*. For example, the previously constructed near-ring $\Pi_{\mathfrak{G}}$ is a *right stem*.

A near-field is said to be a *complete near-field* if the group of multipliers consists of all non-zero elements. For example every division ring is a complete near field.

The determination of all the types of complete near-fields which contain a finite number of elements is an interesting problem which will be solved later.

Exercises

1. We have lost the first row and first column of a group table. Show that the associated abstract group is still uniquely determined by the incomplete table.

2a. All rational integers a, for which $X^a = e$ for all elements X of a group $\mathfrak{G}$, form a module—the *exponential module.*

2b. The non-negative rational integer generating the exponential module is called the *exponent.* The exponent is the least common multiple of the orders of all the elements of $\mathfrak{G}$.

3. The exponent is the smallest natural number a such that $X^a = e$ for all X, if there are any rational integers different from zero with this property.

The exponent is a divisor of the group order. The exponent of a cyclic group is equal to its order. Is the converse true for finite groups?

A finite abelian group whose exponent is equal to its order is cyclic. More generally, show that in a finite abelian group every divisor of the exponent occurs as the order of an element.

Hint: Prove and use the fact that the product of two elements which have relatively prime orders and which commute has an order equal to the product of the orders of the factors.

4. The exponent of a subgroup is a divisor of the exponent of the whole group. The same holds true for a homomorphic image of $\mathfrak{G}$; in particular, the exponent of a factor group is a divisor of the exponent of $\mathfrak{G}$.

5. The greatest common divisor of all rational integers n with the property: $X^n = e$ implies $X^{p^n} = e$, is called the p-exponent (p is a natural prime). Set up and prove statements analogous to those made in exercises 2 - 4.

6. An automorphism α of a group $\mathfrak{G}$ which leaves both the normal subgroup $\mathfrak{N}$ and the factor group $\mathfrak{G}/\mathfrak{N}$ elementwise fixed multiplies each element in $\mathfrak{G}$ by an element of the center $\mathfrak{z}$ of $\mathfrak{N}$. Its order is a divisor of the exponent of $\mathfrak{z}$. All such automorphisms α form an abelian group.

7. A finite group has a non-zero central operator precisely when the order of the factor commutator group and the order of the center have a common prime factor. (Use Exercise 3 of Chap. 1).

8. A normal subgroup of a finite group contains every subgroup whose order is relatively prime to the index of the normal subgroup.

9. Prove the simplicity of $\mathfrak{A}_n$ for $n>4$ by the following method.

a) If the permutation π moves (does not leave fixed) more than 3 ciphers, then there is a three-cycle ϱ, such that $\varrho\pi\varrho^{-1}\pi^{-1}$ leaves more ciphers fixed than π but is not the identity permutation.

b) In any normal subgroup of $\mathfrak{A}_n$ which is different from $\underline{1}$ there is a three-cycle.

c) Apply Exercise 7 of Chapter I (following v.d. Waerden, *Modern Algebra I.*)

III. THE STRUCTURE AND CONSTRUCTION OF COMPOSITE GROUPS

§ 1. Direct Products

By the second isomorphy theorem, in a group $\mathfrak{G}$ which is the product of two normal subgroups $\mathfrak{N}_1$ and $\mathfrak{N}_2$, the factor groups are isomorphic to the factor groups of the $\mathfrak{N}_i$ with respect to their intersection $\mathfrak{D}$; that is,

$$\mathfrak{G}/\mathfrak{N}_1 \simeq \mathfrak{N}_2/\mathfrak{D}, \quad \mathfrak{G}/\mathfrak{N}_2 \simeq \mathfrak{N}_1/\mathfrak{D}.$$

We ask to what extent the structure of $\mathfrak{G}/\mathfrak{D}$ is uniquely determined by the structures of $\mathfrak{N}_1/\mathfrak{D}$ and $\mathfrak{N}_2/\mathfrak{D}$.

To do this we can and will assume that $\mathfrak{G}$ is the product of the two normal subgroups $\mathfrak{N}_1$ and $\mathfrak{N}_2$ with e as their intersection:

$$\mathfrak{G} = \mathfrak{N}_1\mathfrak{N}_2, \ \mathfrak{N}_1 \cap \mathfrak{N}_2 = e.$$

THEOREM 1. *Every element in $\mathfrak{G}$ can be represented as the product of an element from $\mathfrak{N}_1$ and one from $\mathfrak{N}_2$ in one and only one way.*

The multiplication rule is

$$(a_1a_2)\cdot(b_1b_2) = (a_1b_1)\cdot(a_2b_2),$$

where a_i, b_i are in $\mathfrak{N}_i$.

Proof: Since $\mathfrak{G}=\mathfrak{N}_1.\mathfrak{N}_2$, every element in $\mathfrak{G}$ is of the form $a_1.a_2$ with a_i in $\mathfrak{N}_i$.

From $a_1a_2=b_1b_2$ with b_i in $\mathfrak{N}_i$, it follows that

$$b_1^{-1}a_1 = b_2a_2^{-1} = d.$$

Since $\mathfrak{N}_1 \cap \mathfrak{N}_2 = e$,

$$d = e, \ b_1 = a_1, \ b_2 = a_2.$$

Next,

$$a_1a_2a_1^{-1}a_2^{-1} = a_1(a_2a_1^{-1}a_2^{-1}) \in \mathfrak{N}_1$$
$$= (a_1a_2a_1^{-1})a_2^{-1} \in \mathfrak{N}_2 \ ,$$

because $\mathfrak{N}_1$ and $\mathfrak{N}_2$ are normal subgroups, and therefore it follows from $\mathfrak{N}_1 \cap \mathfrak{N}_2 = e$ that $a_1.a_2=a_2.a_1$. It follows from this that we have the multiplication rule, as was to be proved.

Conversely we now form a group $\mathfrak{G}$ with given normal subgroups $\mathfrak{N}_1$ and $\mathfrak{N}_2$ by defining it as follows: $\mathfrak{G}$ consists of all ordered pairs (a_1, a_2) with a_i in $\mathfrak{N}_i$.

We define multiplication by

$$(a_1, a_2)\cdot(b_1, b_2) = (a_1b_1, a_2b_2).$$

We immediately verify the validity of the group axioms. The identity element is $e=(e_1, e_2)$.

The mappings $a_1 \to (a_1, e_2)$ and $a_2 \to (e_1, a_2)$ are, respectively, isomorphisms of $\mathfrak{N}_1$ and $\mathfrak{N}_2$ with normal subgroups $\overline{\mathfrak{N}}_1$ and $\overline{\mathfrak{N}}_2$ of $\mathfrak{G}$ and

$$\overline{\mathfrak{N}}_1 \overline{\mathfrak{N}}_2 = \mathfrak{G};\ \overline{\mathfrak{N}}_1 \cap \overline{\mathfrak{N}}_2 = e.$$

The group $\mathfrak{G}$ just constructed is called the *direct product* of the groups $\mathfrak{N}_1$ and $\mathfrak{N}_2$; in symbols:

$$\mathfrak{G} = \mathfrak{N}_1 \times \mathfrak{N}_2.$$

We restate the previous theorem as follows:

If $\mathfrak{G}$ is the product of the normal subgroups $\mathfrak{N}_1$ and $\mathfrak{N}_2$ with intersection $\mathfrak{D}$, then the factor group $\mathfrak{G}/\mathfrak{D}$ is the direct product of the factor groups $\mathfrak{N}_1/\mathfrak{D}$ and $\mathfrak{N}_2/\mathfrak{D}$.

As the direct product of three groups $\mathfrak{H}_i$, $i=1, 2, 3$, we define

$$\mathfrak{H}_1 \times \mathfrak{H}_2 \times \mathfrak{H}_3 = (\mathfrak{H}_1 \times \mathfrak{H}_2) \times \mathfrak{H}_3.$$

It it obvious that there is a simple isomorphism between

$$(\mathfrak{H}_1 \times \mathfrak{H}_2) \times \mathfrak{H}_3 \quad \text{and} \quad \mathfrak{H}_1 \times (\mathfrak{H}_2 \times \mathfrak{H}_3),$$

and likewise between

$$\mathfrak{H}_1 \times \mathfrak{H}_2 \quad \text{and} \quad \mathfrak{H}_2 \times \mathfrak{H}_1.$$

Accordingly $\mathfrak{H}_1 \times \mathfrak{H}_2 \times \cdots \times \mathfrak{H}_n$ is *uniquely* defined as the direct product of the $\mathfrak{H}_i$ in any order and with any parenthesizing; and indeed we may define $\mathfrak{G} = \mathfrak{H}_1 \times \mathfrak{H}_2 \times \cdots \times \mathfrak{H}_n$ as the set of all ordered n-tuples $x=(x_1, \ldots, x_n)$ of elements x_i in $\mathfrak{H}_i$ with the multiplication rule

$$(x_1, x_2, \ldots, x_n) \cdot (y_1, y_2, \ldots, y_n) = (x_1 y_1, x_2 y_2, \ldots, x_n y_n).$$

After we have identified x_i with the element $(e_1, \ldots, e_{i-1}, x_i, e_{i+1}, \ldots, e_n)$, $\mathfrak{G}$ becomes the direct product of its normal subgroups $\mathfrak{H}_i$.

Necessary and sufficient conditions that a group $\mathfrak{G}$ with normal subgroups $\mathfrak{H}_1, \ldots, \mathfrak{H}_n$ be the direct product of these normal subgroups, are:

1. $$\mathfrak{G} = \mathfrak{H}_1 \cdot \mathfrak{H}_2 \cdot \ldots \cdot \mathfrak{H}_n,$$

2. $$\mathfrak{H}_i \cap (\mathfrak{H}_1, \ldots, \mathfrak{H}_{i-1}, \mathfrak{H}_{i+1}, \ldots, \mathfrak{H}_n) = e \qquad (i=1, 2, \ldots, n).$$

Condition 2. can be replaced by

2 a. $$\mathfrak{H}_i \cap (\mathfrak{H}_{i+1}, \mathfrak{H}_{i+2}, \ldots, \mathfrak{H}_n) = e \qquad (i=1, 2, \ldots, n-1)$$

or

2b. The representation $e = e_1 \cdot e_2 \cdot \ldots \cdot e_n$ with e_i in $\mathfrak{H}_i$, of the identity element of $\mathfrak{G}$ is unique.

We say that the x_i are the $\mathfrak{H}_i$-components of an element x of $\mathfrak{G}$. The

mapping $x \to x_i$ is an operator H_i of $\mathfrak{G}$. H_i is said to be the i-th *decomposition operator* of $\mathfrak{G} = \mathfrak{H}_1 \times \mathfrak{H}_2 \times \cdots \times \mathfrak{H}_n$. The H_i are additive operators and $x = x^{H_1} \cdot x^{H_2} \cdot \ldots \cdot x^{H_n}$; hence

$$H_1 + H_2 + \cdots + H_n = \underline{1}.$$

Moreover $H_i H_k = 0$ if $i \neq k$ and $H_i^2 = H_i$.

If, conversely, we are given additive operators H_i with the properties $\sum_1^n H_i = \underline{1}$, $H_i H_k = 0$ for $i \neq k$, then they are associated with the direct decomposition

$$\mathfrak{G} = \mathfrak{G}^{H_1} \times \mathfrak{G}^{H_2} \times \cdots \times \mathfrak{G}^{H_n}.$$

H_i is a normal operator over $\mathfrak{G}$ since for all b in $\mathfrak{G}^{H_i}$, x in $\mathfrak{G}$, we have $b^x = b^{xH_i} = b^{xH_i}$, and therefore for all a in G, $a^{xH_i} = a^{xH_iH_i} = a^{H_ix}$ The order of a direct product is equal to the product of the orders of its factors, as the component representation shows.

The center, the commutator group and the comutator form of a direct product are the direct products of the centers, the commutator groups and the commutator forms of the factors, respectively.

If $\mathfrak{G}$ is decomposed into the direct product of characteristic factors, then the automorphism group of $\mathfrak{G}$ is the direct product of the automorphism groups of the factors.

Every group is the direct product of the identity element and itself. A group which has only this direct decomposition is said to be *directly indecomposable.*

Direct products occur in the investigation of factors of a principal series of a given group. These factors are simple over a certain automorphism domain, and therefore are characteristically simple.

THEOREM 2: *If the group $\mathfrak{G} \neq e$ is characteristically simple and the double chain law holds for normal subgroups, then it is the direct product of (merely) simple groups which are isomorphic to each other*

Proof: Since the minimal chain law holds, there is a minimal normal subgroup $\mathfrak{N}$ in $\mathfrak{G}$. The automorphisms α of $\mathfrak{G}$ map $\mathfrak{N}$ onto the minimal normal subgroups $\mathfrak{N}^\alpha$ of $\mathfrak{G}$, all isomorphic to $\mathfrak{N}$. We wish to form the largest possible direct product of these. By the maximal chain law, there is certainly a largest direct product $\mathfrak{M} = \mathfrak{N}^{\alpha_1} \times \mathfrak{N}^{\alpha_2} \times \cdots \times \mathfrak{N}^{\alpha_r}$. If $\mathfrak{M}$ were not equal to $\mathfrak{G}$, then by hypothesis $\mathfrak{M}$ would not be mapped into itself under all automorphisms of $\mathfrak{G}$; therefore there is an automorphism α of $\mathfrak{G}$ such that $\mathfrak{N}^\alpha$ does not lie in $\mathfrak{M}$. However we would then have

$\mathfrak{N}^\alpha \cap \mathfrak{M} = e$, since $\mathfrak{N}^\alpha$ is a smallest normal subgroup of $\mathfrak{G}$, and therefore $\mathfrak{N}^\alpha \times \mathfrak{N}^{\alpha_1} \times \cdots \times \mathfrak{N}^{\alpha_r}$ is greater than $\mathfrak{M}$. Consequently

$$\mathfrak{G} = \mathfrak{N}^{\alpha_1} \times \mathfrak{N}^{\alpha_2} \times \cdots \times \mathfrak{N}^{\alpha_r}.$$

The factors of this direct decomposition are the minimal normal subgroups of $\mathfrak{G}$ and therefore simple, as can easily be seen.

Remark: Every factor of a principal series (or of a characteristic series) of a finite solvable group is the direct product of cyclic groups of equal prime order.

§ 2. Theorems on Direct Products[1]

The following theorems also hold for groups with an operator domain Ω.

From the first isomorphism theorem we derive:

THEOREM 3: *If a homomorphism of a group $\mathfrak{G}$ onto a multiplicative system $\mathfrak{H}$ induces an isomorphism with $\mathfrak{H}$ of a normal subgroup $\mathfrak{N}_2$ of $\mathfrak{G}$, then $\mathfrak{G}$ is the direct product of the normal subgroup $\mathfrak{N}_1$ of $\mathfrak{G}$, consisting of all elements of $\mathfrak{G}$ which map onto $\bar{e}$, with the normal subgroup $\mathfrak{N}_2$.*

Proof: From the hypothesis, $\mathfrak{N}_1 \mathfrak{N}_2 = \mathfrak{G}$, $\mathfrak{N}_1 \cap \mathfrak{N}_2 = e$.

THEOREM 4: *If σ is a homomorphism of the group $\mathfrak{G}$ which is different from e, onto the normal subgroup $\overline{\mathfrak{G}}$ of the indecomposable group $\mathfrak{H}$, τ a homomorphy of $\mathfrak{H}$ onto $\mathfrak{J}$, $\tau\sigma$ a $\mathfrak{G}\mathfrak{J}$-isomorphism, then σ is a $\mathfrak{G}\mathfrak{H}$-isomorphism and τ an $\mathfrak{H}\mathfrak{J}$-isomorphism.*

Proof: One can show easily that σ is a $\mathfrak{G}\mathfrak{H}$-isomorphy and that τ is a $\overline{\mathfrak{G}}\mathfrak{J}$-isomorphy. Since $\tau\overline{\mathfrak{G}} = \tau\sigma\mathfrak{G} = \mathfrak{J}$, τ is a $\overline{\mathfrak{G}}\mathfrak{J}$-isomorphism. Since $\mathfrak{G} \neq e$, $\overline{\mathfrak{G}}$ is a normal subgroup of $\mathfrak{H}$ that is distinct from e. From the indecomposability of $\mathfrak{H}$ it follows, by Theorem 3, that $\overline{\mathfrak{G}} = \mathfrak{H}$, and therefore σ is a $\mathfrak{G}\mathfrak{H}$-isomorphism and τ is an $\mathfrak{H}\mathfrak{J}$-isomorphism, Q.E.D.

If ω is an operator of $\mathfrak{G}$, then all the elements of $\mathfrak{G}$ for which $x^\omega = e$ form a normal subgroup $\mathfrak{n}_\omega$ of $\mathfrak{G}$. All the elements of $\mathfrak{G}$ for which $x^{\omega^m} = e$ is solvable likewise form a normal subgroup of $\mathfrak{G}$, which is denoted by $\mathfrak{N}_\omega$. . $\mathfrak{N}_\omega$ is the union of all $\mathfrak{n}_{\omega^m}$. ω is a meromorphism of $\mathfrak{G}/\mathfrak{N}_\omega$, and every normal subgroup of $\mathfrak{G}$ for which ω induces a meromorphism in its factor group, contains $\mathfrak{N}_\omega$.

If the minimal chain condition holds in $\mathfrak{G}$, then ω is actually an automorphism of $\mathfrak{G}/\mathfrak{N}_\omega$. It follows from this that $\mathfrak{G} = \mathfrak{N}_\omega \cdot \mathfrak{G}^{\omega^m}$ for all m. If the maximal chain condition also holds in $\mathfrak{G}$, then the chain

[1] Following Fitting, *Math. Zeitschr. 39 (1934)*; one will find further bibliographical material there.

$\mathfrak{n}_\omega, \mathfrak{n}_{\omega^2}, \mathfrak{n}_{\omega^3}, \ldots$ terminates, and $\mathfrak{N}_\omega = \mathfrak{n}_{\omega^n}$ is solvable. The intersection of $\mathfrak{G}^{\omega^n}$ with $\mathfrak{N}_\omega$ is e, since an element x of this intersection satisfies the equation $x^{\omega^n} = e$ and is of the form $x = y^{\omega^n}$ but $y^{\omega^{2n}} = x^{\omega^n} = e$ implies $y^{\omega^n} = x = e$. If, conversely, $\mathfrak{G} = \mathfrak{N}_\omega \cdot \mathfrak{U}$, where $\mathfrak{U}$ is a subgroup of $\mathfrak{G}$ with the properties $\mathfrak{N}_\omega \cap \mathfrak{U} = e$, $\mathfrak{U}^\omega \leq \mathfrak{U}$, then ω induces a meromorphism of $\mathfrak{U}$, and from the minimal chain condition of $\mathfrak{G}/\mathfrak{N}_\omega$ it follows that $\mathfrak{U}^\omega = \mathfrak{U}$, and therefore $\mathfrak{U} = \mathfrak{U}^{\omega^n} = \mathfrak{N}^{\omega^n}\mathfrak{U}^{\omega^n} = \mathfrak{G}^{\omega^n}$. We specialize to the case for which the operator domain Ω of $\mathfrak{G}$ contains the inner automorphisms of $\mathfrak{G}$, and thus obtain

THEOREM 5.[1] *With a normal operator ω of a group, in which the double chain theorem for normal subgroups is fulfilled, is associated a direct decomposition $\mathfrak{G} = \mathfrak{N}_\omega \times \mathfrak{G}^{\omega^n}$. The second factor of the decomposition is uniquely determined by having $\mathfrak{N}_\omega$ as the first factor.*

Hereafter we shall assume that the double chain condition for the normal subgroups holds in $\mathfrak{G}$.

THEOREM 6: *If the sum of additive normal operators of a directly indecomposable $\mathfrak{G}$ is an automorphism, then the same is true of one of the summands.*

Proof: We can assume immediately that the sum contains only two summands.

If $\omega_1 + \omega_2 = \omega$ is an automorphism then $\omega^{-1}\omega_1 + \omega^{-1}\omega_2 = \underline{1}$, and if we prove the theorem for this sum, it follows for the other. Therefore let $\omega_1 + \omega_2 = \underline{1}$ be the sum of additive normal operators ω_1 and ω_2. From $\omega_1 = \omega_1(\omega_1 + \omega_2) = (\omega_1 + \omega_2)\omega_1$ it follows that $\omega_1\omega_2 = \omega_2\omega_1$. If we had both $\omega_1^n = \underline{0}$ and $\omega_2^n = \underline{0}$, then

$$\underline{1} = (\omega_1 + \omega_2)^{2n} = \sum_0^{2n} c_i \omega_1^i \omega_2^{2n-i} = \underline{0}$$

i.e., $\mathfrak{G} = e$. In this case the theorem is trivial. If $\mathfrak{G} \neq e$ then for at least one of the two operators ω_i, let us say ω_1, every power is different from zero. From Theorem 5 and the indecomposability of $\mathfrak{G}$, it follows that $\mathfrak{N}_{\omega_1} = e$. ω_1 is a meromorphism, and, because of the minimal chain condition for normal subgroups, it is an automorphism, Q.E.D.

DEFINITION: A direct decomposition of a group into directly indecomposable factors not equal to e is said to be a *Remak decomposition.* If the group is directly indecomposable, then it is itself the only factor of its Remak decomposition.

[1] This is known as Fittings Lemma. (See Jacobson, *Theory of Rings.*) (*Ed.*)

THEOREM 7: a) *Every group (satisfying the double chain condition for normal subgroups) has a Remak decomposition .*

b) If $$\mathfrak{G} = \mathfrak{H}_1 \times \mathfrak{H}_2 \times \cdots \times \mathfrak{H}_n$$

and $$\mathfrak{G} = \mathfrak{J}_1 \times \mathfrak{J}_2 \times \cdots \times \mathfrak{J}_m$$

are two Remak decompositions with decomposition operators $H_1, H_2, \ldots, H_n$ *and* $J_1, J_2, \ldots, J_m$, *respectively, then* $n=m$, *and the* $\mathfrak{J}_i$ *can be renumbered so that*

$$\omega = J_1H_1 + J_2H_2 + \cdots + J_nH_n$$

is a normal automorphism of $\mathfrak{G}$ *which maps the* $\mathfrak{H}$*-decomposition on to the* $\mathfrak{J}$*-decomposition.*

c) *For the appropriate ordering of the* $\mathfrak{J}_i$ *we have the exchange equations*

$$\mathfrak{G} = \mathfrak{J}_1 \times \mathfrak{J}_2 \times \cdots \times \mathfrak{J}_k \times \mathfrak{H}_{k+1} \times \mathfrak{H}_{k+2} \times \cdots \times \mathfrak{H}_n.$$

Proof: a) Associated with a direct decomposition $\mathfrak{G}=\mathfrak{H}_1 \times \cdots \times \mathfrak{H}_n$ into factors $\neq e$ is the normal chain without repetitions

$$\mathfrak{G} > \mathfrak{H}_1 \times \mathfrak{H}_2 \times \cdots \times \mathfrak{H}_{n-1} > \cdots > \mathfrak{H}_1 > e$$

of length n. The n are bounded. We choose the decomposition so that the number of factors is as large as possible, and then the further decomposition of any factor into factors unequal to e is impossible.

b) We remark that the additivity of two operators ω_1 and ω_2 implies the additivity of $\omega_1 J_i$ and ω_2, and of $J_k\omega_1$ and ω_2. Therefore

$$\sum_1^m H_1J_k = H_1 \cdot \sum_1^m J_k = H_1,$$

and, by Theorem 6, at least one of the operators H_1J_k induces an automorphism in $\mathfrak{H}_1$.

The J_k can be re-indexed so that it is H_1J_1 that induces an automorphism in $\mathfrak{H}_1$. By Theorem 4, J_1 induces an $\mathfrak{H}_1\mathfrak{J}_1$-isomorphism. By the remark made above,

$$\omega_1 = J_1H_1 + \sum_2^n H_i$$

is a normal operator. An equation $x^{\omega_1} = e$ implies $e = x^{H_1\omega_1} = x^{H_1J_1H_1}$, and since H_1J_1 induces an automorphism of $\mathfrak{H}_1$, we have $x^{H_1} = e$. But then $x^{\omega_1} = x^{\omega_1 H_2} \ldots x^{\omega_1 H_n} = x^{H_2} \cdot x^{H_3} \ldots x^{H_n} = e$, and therefore

$$x^{H_i} = e, \quad x = e.$$

The normal operator ω_1 is a meromorphism, and by the double chain

condition it is, in fact, an automorphism of $\mathfrak{G}$ which maps the $\mathfrak{H}$-decomposition onto the Remak decomposition

$$\mathfrak{G} = \mathfrak{J}_1 \times \mathfrak{H}_2 \times \mathfrak{H}_3 \times \cdots \times \mathfrak{H}_n .$$

If $n=1$, then the theorem is now complete. We apply induction with respect to n and assume $n>1$. $\mathfrak{G}/\mathfrak{J}_1$ has $\mathfrak{H}_2 \times \mathfrak{H}_3 \times \cdots \times \mathfrak{H}_n$ as well as $\mathfrak{J}_2 \times \mathfrak{J}_3 \times \cdots \times \mathfrak{J}_m$ as representative groups. Since the $\mathfrak{H}_i$, $\mathfrak{J}_i$, for $i>1$, remain indecomposable in $\mathfrak{G}/\mathfrak{J}_1$, by the induction hypothesis $n=m$, and the $\mathfrak{J}_i$ with $i>0$, can be reindexed so that $\bar{\omega} = \sum_2^n \bar{J}_i \bar{H}_i$ transforms the $\mathfrak{H}$-decomposition of $\mathfrak{G}/\mathfrak{J}_1$ into the $\mathfrak{J}$-decomposition. Here $\bar{H}_i$ and $\bar{J}_i$ are the decomposition operators in $\mathfrak{G}/\mathfrak{J}_1 \simeq \mathfrak{H}_2 \times \mathfrak{H}_3 \times \cdots \times \mathfrak{H}_n$ and $\mathfrak{G}/\mathfrak{J}_1 \simeq \mathfrak{J}_2 \times \mathfrak{J}_3 \times \cdots \times \mathfrak{J}_n$ respectively. From this it follows that $\sum_2^n J_i H_i$ maps the decomposition $\mathfrak{H}_2 \times \mathfrak{H}_3 \times \cdots \times \mathfrak{H}_n$ isomorphically onto the decomposition $\mathfrak{J}_2 \times \mathfrak{J}_3 \times \cdots \times \mathfrak{J}_n$, and hence $\omega = \sum_1^n J_i H_i$ is the normal automorphism of $\mathfrak{G}$ which was sought.

c) Moreover it also follows from the induction hypothesis that, after appropriate reindexing of the $\mathfrak{J}_i$ for $i>1$,

$$\mathfrak{J}_2 \times \mathfrak{J}_3 \times \cdots \times \mathfrak{J}_h \times \mathfrak{H}_{h+1} \times \cdots \times \mathfrak{H}_n$$

is a representative system of $\mathfrak{G}$ over $\mathfrak{J}_1$. Therefore the exchange equations

$$\mathfrak{G} = \mathfrak{J}_1 \times \mathfrak{J}_2 \times \cdots \times \mathfrak{J}_h \times \mathfrak{H}_{h+1} \times \cdots \times \mathfrak{H}_n .$$

follow.

THEOREM 8: *If* $\mathfrak{G} = \mathfrak{H}_1 \times \mathfrak{H}_2$, *then a homomorphism* σ *of* $\mathfrak{H}_1$ *onto* $\mathfrak{H}_2$ *is normal*[1] *if and only if* $\mathfrak{H}_1{}^\sigma$ *is in the center of* $\mathfrak{G}$.

Proof: 1. Let σ be normal, $a \in \mathfrak{H}_1$, $b \in \mathfrak{H}_2$. Then $a^{b\sigma} = a^{\sigma b} = a^\sigma$. a^σ is in the center of $\mathfrak{H}_2$ and therefore of $\mathfrak{G}$.

2. Let $\mathfrak{H}_1{}^\sigma$ be in the center of $\mathfrak{H}_2$. Then it follows that for all b in $\mathfrak{H}_2$: $a^{b\sigma} = a^{\sigma b}$. If b is in $\mathfrak{H}_1$, then $a^\sigma \cdot b^\sigma = b^\sigma \cdot a^\sigma$. Therefore $(a^b)^\sigma = a^\sigma$, $a^{\sigma b} = a^\sigma = (a^\sigma)^b = a^{b\sigma}$, and therefore σ is normal in $\mathfrak{G}$.

From Theorem 8 follows, with the notation of Theorem 7,

THEOREM 9: *A non-abelian factor of the* $\mathfrak{H}$*-decomposition is normally isomorphic in* $\mathfrak{G}$ *to one and only one factor of the* $\mathfrak{J}$*-decomposition.*

Proof: If $\mathfrak{H}_1$ is normally isomorphic to $\mathfrak{J}_1$, $\mathfrak{J}_2$, then it is also normally isomorphic to $\mathfrak{H}_2$, and by Theorem 8, $\mathfrak{H}_1$ is then abelian.

[1] The mapping σ of $\mathfrak{H}_1$ onto $\mathfrak{H}_2$ is said to be normal in $\mathfrak{G}$ if $a^{b\sigma} = a^{\sigma b}$ for all $a \in \mathfrak{H}_1$, $b \in \mathfrak{G}$.

THEOREM 10: *The Remak decomposition is uniquely determined if and only if all of its factors are invariant under normal operators of* $\mathfrak{G}$.

Proof: We need only prove the second part of the statement. Therefore, let ω be a normal operator of $\mathfrak{G}$ which does not transform the factor $\mathfrak{H}_1$ of the Remak decomposition $\mathfrak{G} = \mathfrak{H}_1 \times \mathfrak{H}_2 \times \cdots \times \mathfrak{H}_n$ into itself. ω is the sum of the normal operators $\omega_{ik} = H_i \omega H_k$. By Theorem 8 the operators ω_{ik} with $i \neq k$ are central operators.

If, for all $i>1$, $\omega_{i1} = 0$, then we would have

$$\mathfrak{H}_1{}^{\omega} = \mathfrak{H}_1{}^{\Sigma \omega_{ik}} = \mathfrak{H}_1{}^{\Sigma \omega_{i1}} = \mathfrak{H}_1{}^{\omega_{11}} \leq \mathfrak{H}_1,$$

and therefore there would be an $i>1$, say $i=2$, such that $\omega_{21} \neq 0$. Since the operator ω_{21} is central, $\pi = \omega_{21} + \underline{1}$ is an operator. It does not map $\mathfrak{H}_1$ into itself.

Since $\omega_{21}{}^2 = 0$, then

$$(\omega_{21} + \underline{1}) \cdot (-\omega_{21} + \underline{1}) = \underline{1}, \quad (-\omega_{21} + \underline{1}) \cdot (\omega_{21} + \underline{1}) = \underline{1},$$

and therefore π is an automorphism of $\mathfrak{G}$. π maps the original Remak decomposition onto a different Remak decomposition

$$\mathfrak{G} = \mathfrak{H}_1{}^{\pi} \times \mathfrak{H}_2 \times \cdots \times \mathfrak{H}_n \quad ; \qquad \text{Q.E.D.}$$

THEOREM 11: *If* $\mathfrak{G} = \mathfrak{H}_1 \times \mathfrak{H}_2$, *then* $\mathfrak{H}_1$ *is invariant under normal operators of* $\mathfrak{G}$ *if and only if there exists no* $\mathfrak{H}_1\mathfrak{H}_2$*-homomorphy normal in* $\mathfrak{G}$ *other than the trivial one*: $\mathfrak{H}_1 \rightarrow e$.

Proof: 1. Let ω be a non-trivial normal $\mathfrak{H}_1\mathfrak{H}_2$-homomorphism. Then ωH_1 is a normal operator of $\mathfrak{G}$ which does not map $\mathfrak{H}_1$ onto itself.

2. If $\bar{\omega}$ is a normal operator of $\mathfrak{G}$ which does not map $\mathfrak{H}_1$ onto itself, then $H_2 \bar{\omega}$ induces a non-trivial normal $\mathfrak{H}_1\mathfrak{H}_2$-homomorphy, Q.E.D.

By Theorem 8, a normal $\mathfrak{H}_1\mathfrak{H}_2$-homomorphy is characterized by an abelian factor group of $\mathfrak{H}_1$ and a subgroup of the center of $\mathfrak{H}_2$ isomorphic to it.

From the previous theorems we derive

THEOREM 12: *The Remak decomposition* $\mathfrak{G} = \mathfrak{H}_1 \times \mathfrak{H}_2 \times \cdots \times \mathfrak{H}_n$ *is uniquely determined if and only if an abelian factor group of* $\mathfrak{H}_i$ *is isomorphic to no subgroup of the center of* $\mathfrak{H}_k$, $i \neq k$, *different from e.*

THEOREM 13 (Speiser): *A group whose factor commutator group or center is of order* 1 *has exactly one Remak decomposition.*

THEOREM 14: *The Remak decomposition of a finite group*

$$\mathfrak{G} = \mathfrak{H}_1 \times \mathfrak{H}_2 \times \cdots \times \mathfrak{H}_r$$

is uniquely determined if and only if the order of the factor commutator

group of each of its factors is relatively prime to the order of the center of each of its other factors.

Proof: By Theorem 8 and Theorem 11 the condition is sufficient. If, however, the prime number p divides $\mathfrak{H}_1 : \mathfrak{H}_1'$ and $\mathfrak{z}(\mathfrak{H}_2) : 1$ then it follows from the basis theorem for abelian groups (which is proven in § 4) that $\mathfrak{H}_1$ has a normal subgroup of index p, and that $\mathfrak{z}(\mathfrak{H}_2)$ contains a subgroup of order p. Since the factor group and the subgroup are isomorphic, there is a non-trivial normal $\mathfrak{H}_1\mathfrak{H}_2$-homomorphy; by Theorem 11 and Theorem 10 the Remak decomposition of $\mathfrak{G}$ is therefore not uniquely determined.

§ 3. Abelian Groups

Let P be a ring with unity element and let $\mathfrak{A}$ be a finite P-module. Thus there are a finite number of elements $v_1, v_2, \ldots, v_n$ in $\mathfrak{A}$ such that every element v in $\mathfrak{A}$ is of the form.

$$v = a_1 v_1 + a_2 v_2 + \cdots + a_n v_n$$

with the a_i in P. Let $\mathfrak{M}_n$ be the P-vector module $(u_1, \ldots, u_n)$.

The mapping

$$a_1 u_1 + a_2 u_2 + \cdots + a_n u_n \rightarrow a_1 v_1 + a_2 v_2 + \cdots + a_n v_n$$

is an operator homomorphy of $\mathfrak{M}_n$ onto $\mathfrak{A}$, and the abelian group $\mathfrak{A}$ with the operator domain P is completely determined by the P-module $\mathfrak{R}$ consisting of all vectors which are mapped onto the zero element of $\mathfrak{A}$:

$$\mathfrak{A} \simeq \mathfrak{M}_n/\mathfrak{R}.$$

With every system of generators $R_1, R_2, \ldots, R_\omega$ of $\mathfrak{R}$ over P we associate the matrix $A_\mathfrak{R}$ whose row vectors are precisely the vectors R_i. A matrix $A_\mathfrak{R} = (a_{ik})$ is characterized by the properties

1. $$\sum_{k=1}^{n} a_{ik} v_k = 0 \qquad (i = 1, 2, \ldots),$$

2. if $$\sum b_k v_k = 0,$$

then $b_k = \sum_i a_{ik} x_i$ is solvable in P where the summation is over only a finite number of i.

Since each row of $A_\mathfrak{R}$ corresponds to a relation valid in $\mathfrak{A}$, we say that $A_\mathfrak{R}$ is a *relation matrix* belonging to $\mathfrak{A}$.

Conversely the row vectors of a matrix A with n columns generate a P-module $\mathfrak{R}$ in $\mathfrak{M}_n$ such that A is a relation matrix belonging to $\mathfrak{M}_n/\mathfrak{R}$.

When do two relation matrices belong to the same finite P-module $\mathfrak{A}$?

We say that two matrices with coefficients in P are *equivalent* if they are relation matrices of the same finite P-module $\mathfrak{A}$.

This equivalence has the three familiar properties.

A rule which uniquely assigns to each matrix an equivalent matrix is called an *elementary transformation.*

We want to find the simplest elementary transformations which by repeated application will transform any two equivalent matrices into one-another.

The zero vector can be adjoined to the generators of $\mathfrak{R}$:

N_0: The elementary transformation N_0 adjoins a row of zeros to the matrix A:

$$A = (a_{ik}) \rightarrow \begin{pmatrix} 0, & \ldots, 0 \\ a_{11}, & \ldots, a_{1n} \\ & \ldots\ldots \end{pmatrix}.$$

N_0': Delete the first row if at least two rows occur and if the first row is a series of zeros.

The generator R_i may be replaced by $R_i + aR_j$ where $i \neq j$:

$T_{i,j}^{a}$: The elementary transformation $T_{i,j}^{a}$ replaces the i-th row of (a_{ik}) by $(a_{i1} + aa_{j1},\ a_{i2} + aa_{j2}, \ldots,\ a_{in} + aa_{jn})$, where $i \neq j$.

We have $$T_{i,j}^{a}\ T_{i,j}^{b}\ A = T_{i,j}^{a+b}\ A.$$

T: By repeated application of $T_{i,j}^{a}$ an arbitrary linear combination of the other rows can be added to the i-th row.

Moreover we can obtain, by composition of the $T_{i,j}^{a}$:

$(i \neq j)$ $V_{i,j}$: Exchanges the i-th with the j-th row and changes the sign in the j-th row:

$$V_{i,j}\ A = T_{i,j}\ T_{j,i}^{-1}\ T_{i,j}\ A.$$

N: By applying N_0 and T an arbitrary linear combination of rows can be adjoined to a matrix.

$M_{i,\varepsilon}$: Moreover by repeated application of $T_{i,j}^{a}$ and N_0, N_0', the i-th row of A can be multiplied by a unit ε of P:

$$M_{i,\varepsilon}\ A = N_0'\ T_{1,i+1}^{-\varepsilon^{-1}}\ V_{1,i+1}\ T_{1,i+1}^{-\varepsilon}\ N_0\ A.$$

$M_{j,-1}\ V_{i,j}$ exchanges the i-th and j-th rows.

If we adjoin $v_0 = a_1 v_1 + a_2 v_2 + \cdots + a_n v_n$ to the generators $v_1, \ldots, v_n$ then we obtain a single new relation:

$$v_0 - a_1 v_1 - a_2 v_2 - \cdots - a_n v_n = 0.$$

S: The elementary transformation S adjoins to the matrix $A = (a_{ik})$

the row $(1, -a_1, -a_2, \ldots, -a_n)$ and the column $\begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \end{pmatrix}$:

$$A \to \begin{pmatrix} 1 & -a_1, & \ldots, & -a_n \\ 0 & a_{11}, & a_{12}, \ldots, & a_{1n} \\ \vdots & a_{21}, & \ldots & \end{pmatrix}$$ (bordering of a matrix).

S': Changes to an unbordered matrix if the first column is of the form $\begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \end{pmatrix}$.

$R_{i,j}$: Exchange of the i-th with the j-th generator of $\mathfrak{A}$ induces an exchange of the i-th with the j-th column in A.

From the elementary transformations found up to now we can form

$(k \neq j)$ $S^a_{k,j}$: Adds the j-th column multiplied by a to the k-th column:

Let S denote bordering with the vector which has 1 at the zero-th, –1 at the j-th and a at the k-th place, and has zeros elsewhere. In SA the first row is multiplied by a_{ij} and added to the $(i+1)$-st row, $(i=1, 2, \ldots)$. After this the first and $(j+1)$-st columns are interchanged, the first line is multiplied by –1 and, finally, the border removed.

THEOREM 15: *By repeated application of the elementary transformations*

$$N_0, N_0', T^a_{i,k}, S, S', R_{i,k} \quad ,$$

a matrix can be transformed into any matrix equivalent to it.

Proof: Let the matrices A, B be equivalent. Then there is a finite P-module $\mathfrak{A}$ with two systems of generators

$$S_1, S_2, \ldots, S_n$$

and

$$T_1, T_2, \ldots, T_{n'},$$

such that A is the relation matrix of the S_i and B is the relation matrix of the T_i.

After n' applications of S, A goes into a relation matrix belonging to the system of generators $T_1, T_2, \ldots, T_{n'}, S_1, S_2, \ldots, S_n$. After n applications of S and repeated application of $R_{i,k}$, B goes into a relation matrix belonging to $T_1, T_2, \ldots, T_{n'}, S_1, S_2, \ldots, S_n$.

Since the inverse of every transformation in the set of the six types of elementary transformations is also in the set, we need only carry out

the proof for $S_i = T_i$, $n = n'$. By repeated application of N, A goes into the matrix $\binom{B}{A}$ and B goes into the matrix $\binom{A}{B}$. The new matrices can be obtained from each other by row permutations and thus the theorem is proven.

Are there easily calculated invariants under elementary transformation?

DEFINITION: The ideal generated by all r-rowed subdeterminants of a matrix A is called the *r-th elementary ideal* $\mathfrak{E}_r(A)$. From the expansion theorem for determinants it follows that $\mathfrak{E}_r(A) \subseteq \mathfrak{E}_{r-1}(A)$. We set $\mathfrak{E}_0(A) = \mathfrak{P}$. Then there is a well-defined index s such that $\mathfrak{E}_s(A) = \mathfrak{P}$ and such that $\mathfrak{E}_{s+1}(A)$, if it exists, is smaller than $\mathfrak{P}$. $\mathfrak{E}_s, \mathfrak{E}_{s+1}, \ldots$ is called the *chain of elementary ideals of A.*

THEOREM 16: *The chain of elementary ideals is invariant under elementary transformation.*

By Theorem 15 it suffices to show the equality of the chain of elementary ideals in the four cases

$$\text{a) } B = N_0 A, \quad \text{b) } B = T^a_{i,k} A, \quad \text{c) } B = SA, \quad \text{d) } B = R_{i,k} A$$

In case a): except for the elements of $\mathfrak{E}_r(A)$, $\mathfrak{E}_r(B)$ contains only determinants with a zero row, and therefore $\mathfrak{E}_r(B) = \mathfrak{E}_r(A)$.

In case b), the subdeterminants of B in which the i-th row takes no part have the same value as the corresponding subdeterminants in A. The same holds true, by the properties of determinants, for the subdeterminants in which both the i-th and the k-th rows take part.

Let $D(\bar{\mathfrak{b}}_{\nu_1}, \bar{\mathfrak{b}}_{\nu_2}, \ldots, \bar{\mathfrak{b}}_{\nu_r})$ be a subdeterminant in which the row vectors $\mathfrak{b}_{\nu_1}, \mathfrak{b}_{\nu_2}, \ldots, \mathfrak{b}_{\nu_r}$ are involved, among them $\mathfrak{b}_i = \mathfrak{a}_i + a\mathfrak{a}_k$, while the index k does not occur among the ν_j. Then

$$D(\bar{\mathfrak{b}}_{\nu_1}, \bar{\mathfrak{b}}_{\nu_2}, \ldots, \bar{\mathfrak{b}}_{\nu_r}) = D(\bar{\mathfrak{a}}_{\nu_1}, \bar{\mathfrak{a}}_{\nu_2}, \ldots, \bar{\mathfrak{a}}_{\nu_r}) + a\, D(\bar{\mathfrak{a}}_{\nu_1}, \ldots, \overset{i}{\bar{\mathfrak{a}}_k}, \ldots, \bar{\mathfrak{a}}_{\nu_r}).$$

From this we conclude $\mathfrak{E}_r(B) \subseteq \mathfrak{E}_r(A)$. Since conversely $A = T^{-a}_{i,k} B$, it follows that $\mathfrak{E}_r(A) \subseteq \mathfrak{E}_r(B)$, therefore $\mathfrak{E}_r(B) = \mathfrak{E}_r(A)$.

In case c), $\mathfrak{E}_{r+1}(B) = \mathfrak{E}_r(A)$.

In case d), $\mathfrak{E}_r(B) = \mathfrak{E}_r(A)$.

A matrix is said to be a *diagonal matrix* if all the elements not on the principal diagonal are zero. Then a relation matrix A can be transformed into a diagonal matrix

$$\begin{pmatrix} d_1 & & & \\ & d_2 & & \\ & & \ddots & \\ & & & d_r \end{pmatrix}$$

by means of elementary transformations precisely when $\mathfrak{A}$ is operator isomorphic to the direct sum of residue class rings

$$\mathrm{P}/(d_1) + \mathrm{P}/(d_2) + \ldots + \mathrm{P}/(d_r).$$

The diagonal matrix A is in *elementary divisor form* if the diagonal elements form a chain of divisors such that $d_1/d_2/d_3/\ \ldots\ /d_r$ and d_1 is not a unit of P. With the help of the elementary divisor form, the chain of elementary ideals may be written:

$$\mathfrak{E}_0(A) = \mathrm{P}, \quad \mathfrak{E}_1(A) = (d_1), \quad \mathfrak{E}_2(A) = (d_1 d_2), \ldots, \quad \mathfrak{E}_r(A) = (d_1 d_2 \ldots d_r).$$

If the d_i are not zero or divisors of zero, then A is equivalent to a second elementary divisor form with the diagonal elements $d_1', d_2', \ldots, d_s'$ if and only if $r = s$ and $(d_i) = (d_i')$, i.e., if and only if the diagonal elements in the same place differ only by a unit of P.

§ 4. Basis Theorem for Abelian Groups

THEOREM 16: *A cyclic group $\mathfrak{G}$ whose order N is the product of pairwise relatively prime numbers $n_1, n_2, \ldots, n_r$, can be decomposed in one and only one way into a direct product of cyclic groups of orders $n_1, n_2, \ldots, n_r$.*

Proof: The uniqueness is clear since in a cyclic group only one subgroup exists having a given order.

We set $m_i = \frac{N}{n_i}$ and seek the i-th decomposition operator. By hypothesis the congruence $x_i m_i \equiv 1 \pmod{n_i}$ is solvable. We define the operator H_i by means of the condition: $a^{H_i} = a^{x_i m_i}$ for all a in $\mathfrak{G}$. We obtain directly the equations:

$$\sum H_i = \underline{1}, \quad H_i H_k = 0 \ (i \neq k), \quad H_i^2 = H_i.$$

Therefore $\mathfrak{G} = \mathfrak{G}^{H_1} \times \mathfrak{G}^{H_2} \times \cdots \times \mathfrak{G}^{H_r}$. Since $n_i H_i = 0$ and $\mathfrak{G}$ is cyclic, the order of $\mathfrak{G}^{H_i}$ is a divisor of n_i, and so, because of the order relation, $\mathfrak{G}^{H_i}$ has the order n_i, Q.E.D.

THEOREM 17: *An abelian group $\neq e$ with a finite number of generators is the direct product of cyclic groups having prime power order or having order zero. The sequence of basis orders is uniquely determined to within*

Proof: In order to prove the first part of the theorem, it suffices by Theorem 16 to prove decomposability into cyclic factors. Our operator ring P is the ring of integers, and our aim is to put the relation matrix A belonging to the abelian group $\mathfrak{A}$ into diagonal form by means of elementary transformations.

We apply the following reductions:

I. If A is the zero matrix, then A is already in diagonal form

If $A \neq 0$, then among those integers a_{ik} which are different from zero there is one which is smallest in absolute value. By appropriate row and column interchange we may take a_{11} to be this number.

a) If $a_{1k} \neq 0$, $k>1$, then $a_{1k} = qa_{11} + r$ where q and r belong to P and

$$0 \leqq r < |a_{11}|.$$

Multiplying the first column by q and subtracting it from the k-th column we obtain $b_{1k} = a_{1k} - qa_{11} = r$ which is smaller than a_{11} in absolute value.

b) If $a_{i1} \neq 0$, $i>1$, $a_{i1} = qa_{11} + r$, where q and r belong to P, $0 \leqq r < |a_{11}|$, then subtract q times the first row from i-th row.

After a finite number of reductions of type I.a) or I.b), we find that all the elements of the first row and first column are divisible by a_{11}.

If A has n columns, then after at most $(n-1)$ reductions by I.a) we find that the first row is of the form $(a_{11}, 0, \ldots, 0)$. The first column remains unchanged by this reduction, and we may now replace it by $\begin{pmatrix} a_{11} \\ 0 \\ 0 \\ \vdots \end{pmatrix}$. (Here reduction I.b) may have to be applied infinitely often).

The unbordered matrix which is obtained from A by deleting the first row and first column has only $n-1$ columns. We apply the reduction process described above to it; here the bordered matrix is transformed without changing the first row and column. After at most n such reductions A goes into diagonal form.

In order to prove the uniqueness we assume that $S_1, S_2, \ldots, S_n$ is a basis of $\mathfrak{A} \neq e$ such that $S_1, S_2, \ldots, S_r$ are of prime power order, and that the remaining basis elements are of order zero.

Let $S_1, S_2, \ldots, S_s$ be all the basis elements whose order is a power of the natural prime p, so that S_i is of order p^{n_i} with $0 < n_1 \leqq n_2 \cdots \leqq n_s$. All elements of $\mathfrak{A}$ whose order is a power of p form a subgroup $\mathfrak{S}_p$ with $S_1, S_2, \ldots, S_s$ as basis ($p^k \cdot \sum a_i S_i = \sum p^k a_i S_i = 0$ implies $a_i = 0$, if

$i>s$). The relation matrix of $\mathfrak{S}_p$ with respect to this system of generators has the elementary divisor form $\begin{pmatrix} p^{n_1} & & & \\ & p^{n_2} & & \\ & & \ddots & \\ & & & p^{n_s} \end{pmatrix}$.

By § 3 the numbers in the diagonal are uniquely determined to within sign.

The n_i are uniquely determined.

$S_1, S_2, \ldots, S_r$ generate the subgroup $\mathfrak{U}$ of all elements with postive order in $\mathfrak{A}$. The factor group $\mathfrak{A}/\mathfrak{U}$ has $S_{r+1}, \ldots, S_n$ as basis with the basis orders 0, 0, . . . , 0. Since the associated relation matrix, being a null matrix, is in the elementary divisor form, the number $n-r$ is uniquely determined, Q.E.D.

§ 5. The Order Ideal

The following investigations are closely related to § 3.

DEFINITION: The last member in the chain of elementary ideals of a matrix A is said to be the *order ideal* $\mathfrak{O}_A$ of A. The order ideal is generated by all the subdeterminants of greatest order of A.

The order ideal is invariant under elementary transformations.

It follows from the basis theorem that the order ideal of an ordinary abelian group with a finite number of generators is generated by the group order (where P is the ring of rational integers).

THEOREM 18 (Analogous to the Fermat Theorem of group theory): *For all operators D of the order ideal $\mathfrak{O}_A$ and all elements v in $\mathfrak{A}$,*

$$Dv=0.$$

Proof: It suffices to assume that D is an n-rowed subdeterminant of a relation matrix A with n columns, and that v is one of the corresponding generators v_i of $\mathfrak{A}$. After appropriate renumbering of the rows of A, let $D=|a_{ik}|$ $(i, k=1, \ldots, n)$.

Then $$\sum_{k=1}^{n} a_{ik}\, v_k = 0,$$

and therefore $$\sum_{k=1}^{n} a_{ik}\, A_{ih}\, v_k = 0 \qquad (i=1,2 \ldots n),$$

where A_{ih} is the algebraic complement of a_{ih} in D. After summation over these n equations, we get

$$\sum_{k=1}^{n}\left(\sum_{i=1}^{n} a_{ik}\,A_{ih}\right)v_k = 0\,.$$

As is well known, the inner sum has the value $\delta_{kh}D$, and therefore

$$Dv_k = 0, \qquad \text{Q.E.D.}$$

§ 6. Extension Theory

The extension problem posed and solved by Otto Schreier reads:

Given two abstract groups $\mathfrak{N}$ and $\mathfrak{F}$, *find all groups* $\mathfrak{G}$ *which contain* $\mathfrak{N}$ *as a normal subgroup, such that*

$$\mathfrak{G}/\mathfrak{N} \simeq \mathfrak{F}. \tag{1}$$

First we shall investigate the groups $\mathfrak{G}$ which contain $\mathfrak{N}$ as a normal subgroup with factor group isomorphic to $\mathfrak{F}$. The elements in $\mathfrak{F}$ are designated by $1, \sigma, \tau \ldots$.

There is a decomposition $\mathfrak{G} = \sum_{\sigma \in \mathfrak{F}} \mathfrak{N} S_\sigma$ of $\mathfrak{G}$ into cosets with respect to $\mathfrak{N}$ such that $\mathfrak{N}S_\sigma \cdot \mathfrak{N}S_\tau = \mathfrak{N}S_{\sigma\tau}$, and therefore

$$S_\sigma S_\tau = C_{\sigma,\tau} S_{\sigma\tau},\ C_{\sigma,\tau} \in \mathfrak{N}. \tag{2}$$

Since $\mathfrak{N}$ is a normal subgroup of $\mathfrak{G}$, for the elements $E, A, B, C, \ldots$ in $\mathfrak{N}$:

$$S_\sigma A S_\sigma^{-1} = A^{S_\sigma} \in \mathfrak{N}, \tag{3}$$

$$(AB)^{S_\sigma} = A^{S_\sigma} B^{S_\sigma}, \tag{4}$$

$$(A^{S_\tau})^{S_\sigma} = A^{S_\sigma S_\tau} = A^{C_{\sigma,\tau} S_{\sigma\tau}} = (A^{S_{\sigma\tau}})^{C_{\sigma,\tau}}, \tag{5}$$

$$S_1 S_1 = C_{1,1} S_1, \text{ hence } S_1 = C_{1,1}, \tag{6}$$

$$A^{S_1} = A^{C_{1,1}}, \tag{7}$$

$$AS_\sigma \cdot BS_\tau = AB^{S_\sigma} C_{\sigma,\tau} S_{\sigma\tau}. \tag{8}$$

From the associative law in $\mathfrak{G}$ it follows that

$$\begin{aligned}(S_\sigma S_\tau)S_\varrho = (C_{\sigma,\tau}S_{\sigma\tau})S_\varrho &= C_{\sigma,\tau}C_{\sigma\tau,\varrho}S_{\sigma\tau\varrho} \\ &= S_\sigma(S_\tau S_\varrho) = S_\sigma C_{\tau,\varrho} S_{\tau\varrho} = C_{\tau,\varrho}^{S_\sigma} C_{\sigma,\tau\varrho} S_{\sigma\tau\varrho},\end{aligned}$$

and from this follow the *associativity relations*

$$C_{\sigma,\tau}C_{\sigma\tau,\varrho} = C_{\tau,\varrho}^{S_\sigma} C_{\sigma,\tau\varrho}. \tag{9}$$

Conversely, let single-valued mappings S_σ of $\mathfrak{N}$ onto itself be given and let a system of elements $C_{\sigma,\tau}$ in $\mathfrak{N}$ be given also, so that

I. $(AB)^{S_\sigma} = A^{S_\sigma} B^{S_\sigma}$,

II. $(A^{S_\tau})^{S_\sigma} = A^{S_\sigma S_\tau} = (A^{S_{\sigma\tau}})^{C_{\sigma,\tau}} = A^{C_{\sigma,\tau} S_{\sigma\tau}}$, $\quad A^{S_1} = A^{C_{1,1}}$,

III. $C_{\sigma,\tau} C_{\sigma\tau,\varrho} = C_{\tau,\varrho}^{S_\sigma} C_{\sigma,\tau\varrho}$.

A system of elements $C_{\sigma,\tau}$ which occurs in a solution of these three equations is said to be a *factor system in* $\mathfrak{N}$ *belonging to* $\mathfrak{F}$.

A group will be constructed which contains $\mathfrak{N}$ as a normal subgroup and whose factor group is isomorphic to $\mathfrak{F}$ such that the multiplication of the representatives of $\mathfrak{G}$ over $\mathfrak{N}$ follows rule (8).

Let $\mathfrak{G}$ be the set of all symbols AS_σ with A in $\mathfrak{N}$; $AS_\sigma = BS_\tau$ if and only if $A = B$, $\sigma = \tau$. We define multiplication in $\mathfrak{G}$ by

$$AS_\sigma \cdot BS_\tau = AB^{S_\sigma} C_{\sigma,\tau} S_{\sigma\tau}.$$

In $\mathfrak{G}$ the associative law is valid:

$$\begin{aligned}
(AS_\sigma \cdot BS_\tau) \cdot CS_\varrho &= AB^{S_\sigma} C_{\sigma,\tau} S_{\sigma\tau} \cdot CS_\varrho \\
&= AB^{S_\sigma} C^{S_{\sigma\tau}} C_{\sigma\tau,\varrho} S_{\sigma\tau\varrho} \\
&= AB^{S_\sigma} C^{C_{\sigma,\tau} S_{\sigma\tau}} C_{\sigma,\tau} C_{\sigma\tau,\varrho} S_{\sigma\tau\varrho} \\
&= AB^{S_\sigma} C^{S_\sigma S_\tau} C_{\tau,\varrho}^{S_\sigma} C_{\sigma,\tau\varrho} S_{\sigma\tau\varrho} \qquad \text{(by II. and III.)} \\
&= A(BC^{S_\tau} C_{\tau,\varrho})^{S_\sigma} C_{\sigma,\tau\varrho} S_{\sigma\tau\varrho} \qquad \text{(by I.)} \\
&= AS_\sigma \cdot BC^{S_\tau} C_{\tau,\varrho} S_{\tau\varrho} \\
&= AS_\sigma \cdot (BS_\tau \cdot CS_\varrho).
\end{aligned}$$

If we set $\sigma = \tau = 1$ in III, then

$$C_{1,1} C_{1,\varrho} = C_{1,\varrho}^{S_1} C_{1,\varrho}, \quad C_{1,1} = C_{1,\varrho}^{C_{1,1}}, \quad \text{therefore}$$

$$C_{1,\varrho} = C_{1,1}. \tag{10}$$

If on the other hand we set $\tau = \varrho = 1$ in III, then

$$C_{\sigma,1} C_{\sigma,1} = C_{1,1}^{S_\sigma} C_{\sigma,1}, \qquad \text{therefore}$$

$$C_{\sigma,1} = C_{1,1}^{S_\sigma}. \tag{11}$$

$e = C_{1,1}^{-1} S_1$ is left identity of $\mathfrak{G}$, since

$$e \cdot A S_\varrho = C_{1,1}^{-1} A^{C_{1,1}} C_{1,\varrho} S_\varrho = A S_\varrho .$$

As solution of $\quad X S_\sigma \cdot B S_\tau = e,$

that is, of
$$\begin{cases} X B^{S_\sigma} C_{\sigma,\tau} = C_{1,1}^{-1} \\ \sigma\tau = 1, \end{cases}$$

we find
$$X = C_{1,1}^{-1} C_{\sigma,\tau}^{-1} B^{-S_\sigma}$$
$$\sigma = \tau^{-1}.$$

$\mathfrak{G}$ is a group.

We set $\quad \bar{A} = A C_{1,1}^{-1} S_1 .$

Then
$$\bar{A}\bar{B} = A C_{1,1}^{-1} S_1 \cdot B C_{1,1}^{-1} S_1 = A C_{1,1}^{-1} \left(B C_{1,1}^{-1}\right)^{S_1} \cdot C_{1,1} S_1$$
$$= A B C_{1,1}^{-1} S_1 = \overline{AB}.$$

Now $\quad \bar{A} = e \quad$ implies $\quad A = 1.$

Therefore $A \to \bar{A}$ is an isomorphic mapping of $\mathfrak{A}$ onto a subgroup $\bar{\mathfrak{A}}$ of $\mathfrak{G}$.

Set $\bar{S}_\sigma = 1 S_\sigma$. Then

$$\bar{A} \cdot \bar{S}_\sigma = A C_{1,1}^{-1} S_1 \cdot 1 S_\sigma = A C_{1,1}^{-1} C_{1,\sigma} S_\sigma = A S_\sigma \qquad \text{by (10)},$$
$$\bar{S}_\sigma \cdot \bar{S}_\tau = 1 S_\sigma \cdot 1 S_\tau = C_{\sigma,\tau} S_{\sigma\tau} = \bar{C}_{\sigma,\tau} \cdot \bar{S}_{\sigma\tau},$$
$$\bar{S}_\sigma \cdot \bar{A} = 1 S_\sigma A C_{1,1}^{-1} S_1 = A^{S_\sigma} C_{1,1}^{-S_\sigma} C_{\sigma,1} S_\sigma = A^{S_\sigma} S_\sigma$$
$$= \overline{A^{S_\sigma}} \cdot \bar{S}_\sigma ,$$

therefore $\quad \bar{A}^{S_\sigma} = \overline{A^{S_\sigma}}.$

$\bar{\mathfrak{A}}$ is a normal subgroup of $\mathfrak{G}$ with the $\bar{S}_\sigma$ as a system of representatives, the $\bar{C}_{\sigma,\tau}$ as factor system, and the $\bar{S}_\sigma$ as automorphisms, and the mapping $A \to \bar{A}$ is an operator isomorphism between $\mathfrak{A}$ and $\bar{\mathfrak{A}}$. Thus the problem stated above is completely solved.

Let $\mathfrak{G}$ and $\bar{\mathfrak{G}}$ be two extensions of $\mathfrak{A}$ which belong to the same factor system $C_{\sigma,\tau}$ and the same automorphism set S_σ. The elements in $\mathfrak{G}$ are uniquely of the form $A S_\sigma$, those in $\bar{\mathfrak{G}}$ uniquely of the form $A \bar{S}_\sigma$, where

$$A S_\sigma B S_\tau = A B^{S_\sigma} C_{\sigma,\tau} S_{\sigma\tau}$$
$$A \bar{S}_\sigma B \bar{S}_\tau = A B^{S_\sigma} C_{\sigma,\tau} \bar{S}_{\sigma\tau}.$$

Then the identity automorphism of $\mathfrak{N}$ can be extended, by means of the mapping $A S_\sigma \to A \bar{S}_\sigma$, to an isomorphism between $\mathfrak{G}$ and $\bar{\mathfrak{G}}$. We say more briefly: $\mathfrak{G}$ and $\bar{\mathfrak{G}}$ are $\mathfrak{N}$-isomorphic.

From these investigations we conclude:

THEOREM 19: *To each extension $\mathfrak{G}$ of a normal subgroup $\mathfrak{N}$ with given factor group $\mathfrak{F}$, there belongs a factor system and a set of automorphisms of $\mathfrak{N}$ such that conditions I, II, III are fulfilled.*

Conversely, to a given factor system and a given set of automorphisms of $\mathfrak{N}$ which fulfill I, II, III, there belongs an extension of $\mathfrak{N}$, unique to within isomorphy over $\mathfrak{N}$.

If instead of choosing S_σ as a representative of $S_\sigma \mathfrak{N}$ we choose $T_\sigma = A_\sigma S_\sigma$ with A_σ in $\mathfrak{N}$, then the automorphism S_σ of $\mathfrak{N}$ is replaced by $A_\sigma S_\sigma = T_\sigma$ and $C_{\sigma,\tau}$ is replaced by $A_\sigma A_\tau^{S_\sigma} C_{\sigma,\tau} A_{\sigma\tau}^{-1}$, since

$$T_\sigma T_\tau = A_\sigma S_\sigma A_\tau S_\tau = A_\sigma A_\tau^{S_\sigma} C_{\sigma,\tau} S_{\sigma\tau} = A_\sigma A_\tau^{S_\sigma} C_{\sigma,\tau} A_{\sigma\tau}^{-1} T_{\sigma\tau}.$$

The converse is clear.

DEFINITION: Two factor systems $(S_\sigma, C_{\sigma,\tau})$, $(T_\sigma, D_{\sigma,\tau})$ are said to be equivalent if there are elements A_σ such that

$$A^{T_\sigma} = A^{A_\sigma S_\sigma} \text{ for all } A \leq \mathfrak{N}$$

and

$$D_{\sigma,\tau} = A_\sigma A_\tau^{S_\sigma} C_{\sigma,\tau} A_{\sigma\tau}^{-1}.$$

We then write

$$(T_\sigma, D_{\sigma,\tau}) \sim (S_\sigma, C_{\sigma,\tau}).$$

For this equivalence the three rules are valid.

Two factor systems with sets of automorphisms induce extensions which are isomorphic over $\mathfrak{N}$ and for which the coset R_σ maps onto the coset $\bar{R}_\sigma$, if and only if the factor systems are equivalent.

There always exists at least one factor system, namely that belonging to the direct product $\mathfrak{F} \times \mathfrak{N}$:

$$C_{\sigma,\tau} = 1,$$
$$A^{S_\sigma} = A.$$

A factor system is equivalent to $(T_\sigma, 1)$ if and only if

$$1 = A_\sigma A_\tau^{S_\sigma} C_{\sigma,\tau} A_{\sigma\tau}^{-1}$$

is solvable.

An equivalent condition is: In some associated extension, a subgroup can be found which is a system of representatives with respect to $\mathfrak{N}$.

Then $\mathfrak{G}$ decomposes into a product of $\mathfrak{F}$ and $\mathfrak{N}$ where $\mathfrak{F} \cap \mathfrak{N} = e$. Therefore we say that a factor system equivalent to $(T_\sigma, 1)$ is a *retracting factor system.*

If the given normal subgroup $\mathfrak{N}$ of $\mathfrak{G}$ is abelian, then the automorphism $A \to A^{S_\sigma}$ is independent of the particular choice of the representative S_σ and therefore we simply set $A^{S_\sigma} = A^\sigma$.

Three necessary and sufficient conditions in terms of $(\sigma, C_{\sigma,\tau})$ are then

$$\text{I. } (A\,B)^\sigma = A^\sigma\,B^\sigma,$$

$$\text{II. } (A^\tau)^\sigma = A^{\sigma\tau},\ A^1 = A\,.$$

$$\text{III. } C_{\sigma,\tau}\,C_{\sigma\tau,\varrho} = C^\sigma_{\tau,\varrho}\,C_{\sigma,\tau\varrho}.$$

The factor systems belonging to the same group $(\sigma, \tau, \ldots)$ of automorphisms of $\mathfrak{N}$ form a group $(C_{\sigma,\tau})$. The number of non-equivalent factor systems is equal to the index

$$(C_{\sigma,\tau}) : (A_\sigma\,A^\sigma_\tau\,A^{-1}_{\sigma\tau}).$$

The number of different retracting factor systems is equal to the index

$$(A_\sigma) : (\delta_\sigma), \quad \text{where} \quad \delta_\sigma\,\delta^\sigma_\tau = \delta_{\sigma\tau}.$$

If $\mathfrak{N}$ is of order m and $\mathfrak{F}$ is of order n, then the last index is equal to

$$m^n/((\delta_\sigma) : 1).$$

§ 7. Extensions with Cyclic Factor Group

Let the factor group of $\mathfrak{G}$ over the normal subgroup $\mathfrak{N}$ be isomorphic to the cyclic group $\mathfrak{F} = (\sigma)$.

Let S be a representative of the coset associated with σ.

If $\mathfrak{F}:1=0$, then $1, S^{\pm 1}S^{\pm 2}, \ldots$ is a system of representatives of $\mathfrak{G}$ over $\mathfrak{N}$ and $C_{\sigma^i,\,\sigma^k} = 1$.

If $\mathfrak{F}:1=n>0$ then $1, S, S^2, \ldots, S^{n-1}$ s a system of representatives of $\mathfrak{G}$ over $\mathfrak{N}$. Then $S^n = N$ is an element in $\mathfrak{N}$ for which $N^S = N$ holds. Moreover $A^{S^n} = A^N$ for all A in $\mathfrak{N}$ and

$$C_{\sigma^i,\,\sigma^k} = \begin{cases} 1, & i+k<n \\ N, & i+k \geqq n \end{cases} \qquad (0 \leqq i,\ k<n).$$

Conversely if $\mathfrak{F}:1=0$, and $A \to A^S$ is any automorphism of $\mathfrak{N}$, then

we set $C_{\sigma^i,\,\sigma^k} = 1$ and see that one and only one extension group $\mathfrak{G}$ of $\mathfrak{N}$ exists such that $\mathfrak{G}/\mathfrak{N} = (S\mathfrak{N}) \simeq \mathfrak{F}$ and $SAS^{-1} = A^S$ for all A in $\mathfrak{N}$.

If $\mathfrak{F}: 1 = n > 0$ and $A \to A^\sigma$ is a single-valued mapping of $\mathfrak{N}$ onto itself with the properties **Ia.** $(AB)^\sigma = A^\sigma B^\sigma$,

IIa. $A^{\sigma^n} = A^N$, $N \in \mathfrak{N}$,

IIIa. $N^\sigma = N$, then there exists one and only one extension group $\mathfrak{G}$ of $\mathfrak{N}$ such that $\mathfrak{G}/\mathfrak{N} = (S\mathfrak{N}) \simeq \mathfrak{F}$ and $SAS^{-1} = A^\sigma$ for all A in $\mathfrak{N}$, $S^n = N$.

Proof: In order to see that $\mathfrak{G}$ exists, we set

$$C_{\sigma^i,\,\sigma^k} = \begin{cases} 1 & \\ N, & \text{if} \quad \begin{matrix} i + k < n \\ i + k \geqq n \end{matrix} \end{cases} \qquad (0 \leqq i,\ k < n).$$

Then I and II hold.

The validity of III means, since $N^\sigma = N$, that certain identities with the factors 1, N are fulfilled, no matter what the structure of $\mathfrak{N}$. Now since the infinite cyclic group (S) is a cyclic extension of index n over (S^n), and $N = S^n$ generates an infinite cyclic group, the identities are valid in all groups.

Since $\mathfrak{G}$ is uniquely determined by $\mathfrak{N}$, σ and N, we denote $\mathfrak{G}$ by $(\mathfrak{N}, \sigma, N)$.

When is $(\mathfrak{N}, \sigma, N)$ isomorphic to $(\mathfrak{N}, \sigma^*, N^*)$ over $\mathfrak{N}$?

We can assume that the two groups are identical, and then $S_{\sigma^*} = A S_\sigma^\nu$ where $0 < \nu \leqq n$ and $(\nu, n) = 1$:

$$N^* = (A S_\sigma^\nu)^n = A^{1 + \sigma^\nu + \cdots + \sigma^{\nu(n-1)}} N^\nu.$$

Conversely if $x^{\sigma^*} = x^{A\sigma^\nu}$ for all x in N, where $(\nu, n) = 1$, and if $N^* = A^{1 + \sigma^\nu + \cdots + \sigma^{\nu(n-1)}} N^\nu$, then $(\mathfrak{N}, \sigma^*, N^*)$ is a cyclic extension of index n of N, which is isomorphic to $(\mathfrak{N}, \sigma, N)$ over $\mathfrak{N}$.

Example: Let $\mathfrak{N}$ be a finite cyclic group with order m. If $\mathfrak{N} = (A)$, then $N = A^t$ and $A^\sigma = A^r$. $\mathfrak{G}$ is uniquely described by the four numbers n, m, t, r. IIa. implies $r^n \equiv 1\,(m)$, and conversely. IIIa. implies $rt \equiv t\,(m)$, and conversely. We obtain:

THEOREM 20 (Hölder): *A group $\mathfrak{G}$ of finite order $n.m$ with cyclic normal subgroup (A) and with cyclic factor group $(B\ (A))$ of finite order n has the two generators A, B with the defining relations:*

$$A^m = e, \quad B^n = A^t, \quad BAB^{-1} = A^r$$

and with the numerical conditions

$$\text{a)} \quad 0 < n, m.$$

$$\text{b)} \quad r^n \equiv 1\,(m),$$

$$\text{c)} \quad t(r-1) \equiv 0\,(m).$$

Conversely if the numerical conditions are fulfilled, then a group with the previously given properties is defined by the three relations. For fixed n and m the replacement of r, t by

$$r^* = r^\nu, \quad (\nu, n) = 1,$$

$$t^* = \nu t + (1 + r^\nu + r^{2\nu} + \cdots + r^{(n-1)\nu})$$

leads to $\mathfrak{N}$-isomorphic extensions.

§ 8. Extensions with Abelian Factor Group

Let the factor group of the group $\mathfrak{G}$ over the normal subgroup $\mathfrak{N}$ be isomorphic to the direct product

$$\mathfrak{F} = (\sigma_1) \times (\sigma_2) \times \ldots \times (\sigma_r),$$

of cyclic groups (σ_i) of orders n_i. Let $(S_i\,\mathfrak{N})$ be cosets associated with σ_i. The following relations hold in $\mathfrak{G}$:

$$S_i A S_i^{-1} = A^{S_i} \in \mathfrak{N} \qquad \text{if} \qquad A \in \mathfrak{N},$$

$$S_i^{n_i} = A_i \in \mathfrak{N},$$

$$S_i S_k S_i^{-1} S_k^{-1} = A_{i,k} \in \mathfrak{N}.$$

For the mappings $A \to A^{S_i}$ of $\mathfrak{N}$ onto itself the rules

$$(A\,B)^{S_i} = A^{S_i}\,B^{S_i},$$

$$A^{S_i^{n_i}} = A^{A_i},$$

$$A^{S_i\,S_k} = A^{A_{i,k}\,S_k\,S_i}$$

hold.

Moreover $A_{i,k}\,A_{k,i}=1$, $n_i \geqq 0$, and if $n_i=0$ then $A_i=1$.

$$
\begin{aligned}
A_k^{S_i} &= S_i A_k S_i^{-1} = S_i S_k^{n_k} S_i^{-1} = \left(S_i S_k S_i^{-1}\right)^{n_k} \\
&= \left(A_{i,k} S_k\right)^{n_k} = A_{i,k}\left(S_k A_{i,k} S_k^{-1}\right) S_k^2 A_{i,k} \ldots \\
&= A_{i,k} A_{i,k}^{S_k} \ldots A_{i,k}^{S_k^{n_k-1}} A_k \\
S_i A_{k,l} S_i^{-1} &= A_{k,l}^{S_i} \\
&= \left(S_i S_k S_i^{-1}\right) \cdot \left(S_i S_l S_i^{-1}\right) \left(S_i S_k S_i^{-1}\right)^{-1} \left(S_i S_l S_i^{-1}\right)^{-1} \\
&= A_{i,k} S_k \cdot A_{i,l} S_l \cdot \left(A_{i,k} S_k\right)^{-1} \cdot \left(A_{i,l} S_l\right)^{-1} \\
&= A_{i,k} A_{i,l}^{S_k} \cdot S_k S_l S_k^{-1} S_l^{-1} \cdot A_{i,k}^{-S_l} A_{i,l}^{-1} \\
&= A_{i,k} A_{i,l}^{S_k} A_{k,l} A_{i,k}^{-S_l} A_{i,l}^{-1}.
\end{aligned}
$$

Now conversely let a group $\mathfrak{N}$ be given which contains the elements $A_i, A_{i,k}$ $(i,k=1,2,\ldots,r;\ i \neq k)$ and let single valued mappings $A \to A^{S_i}$ of $\mathfrak{N}$ onto itself be defined with the following properties:

1. $(A\,B)^{S_i} = A^{S_i} B^{S_i}$,

2. $A^{S_i^{n_i}} = A^{A_i}$ (if $n_i > 0$), $A_i^{S_i} = A_i$,

2a. $n_i \geqq 0$, and if $n_i = 0$, then $A_i = 1$,

3. $A^{S_i S_k} = A^{A_{i,k} S_k S_i}$ $(i > k)$,

3a. $A_{i,k} A_{k,i} = 1$ $(i > k)$,

4. $A_k^{S_i} = A_{i,k}^{1+S_k+\cdots+S_k^{n_k-1}} A_k$ (if $n_k > 0$, $i \neq k$),

5. $A_{i,k}^{S_l} A_{k,l}^{-1} A_{l,i}^{S_k} A_{i,k}^{-1} A_{k,l}^{S_i} A_{l,i}^{-1} = 1$ $(i < k < l)$.

THEOREM 21: *The group $\mathfrak{G}$ with generators $\bar{A}$ $(A \in N)$, $S_1, S_2, \ldots, S_r$ and with the defining relations*

a) $\overline{A\,B} = \bar{A}\,\bar{B}$,

b) $S_i \bar{A} S_i^{-1} = \overline{A^{S_i}}$,

c) $S_i^{n_i} = \bar{A}_i$,

d) $S_i S_k S_i^{-1} S_k^{-1} = \bar{A}_{i,k}$ $(i > k)$

contains the normal subgroup $\overline{\mathfrak{N}}$ of all $\bar{A}$ such that the factor group is the direct product of the cyclic groups $(S_i\overline{\mathfrak{N}})$ of order n_i and the mapping $A \to \bar{A}$ is an isomorphism of $\mathfrak{N}$ onto $\overline{\mathfrak{N}}$.

Proof: If $r=1$ then the theorem follows from § 6. Let $r>1$ and assume that the theorem has been proven when there are only $r-1$ generators S_i.

Let $\mathfrak{G}_1$ be the group generated by $\bar{A}$ and $S_1, \ldots, S_{r-1}$ which satisfy conditions 1. to 5. and relations a) to d) where the indices i, k, l run from 1 to $r-1$.

We define $\quad \bar{A}^{S_r} = \overline{A^{S_r}}, \quad S_k^{S_r} = \bar{A}_{r,k} S_r \qquad (k = 1, 2, \ldots, r-1).$

Conditions 1., 3., 3a. and 4. with $i=r$, 5. with $l=r$ merely state that the mapping S_r just defined can be extended (uniquely) to an operator S_r of $\mathfrak{G}_1$.

The conditions $A^{A_r} = A^{S_r^{n_r}}$, $A_r^{S_r} = A_r$, state, by § 6, that the relations

b) $S_r \bar{A} S_r^{-1} = \bar{A}^{S_r}$,

c) $S_r^{n_r} = \bar{A}_r$,

d) $S_r S_i S_r^{-1} S_i^{-1} = \bar{A}_{r,i} \quad (i < r)$

define a cyclic extension $\mathfrak{G}$ of index n_r over $\mathfrak{G}_1$.

By the induction hypothesis, $A \to \bar{A}$ is an isomorphism of $\mathfrak{A}$ onto $\bar{\mathfrak{A}}$. It follows from b) that $\bar{\mathfrak{A}}$ is a normal subgroup of $\mathfrak{G}$. It follows from d) that $\mathfrak{G}/\bar{\mathfrak{A}}$ is abelian and is generated by $S_1\bar{\mathfrak{A}}, S_2\bar{\mathfrak{A}}, \ldots, S_r\bar{\mathfrak{A}}$.

Now $\quad \prod_1^r S_i^{\nu_i} \equiv 1 \,(\bar{\mathfrak{A}})$

implies $\quad S_r^{\nu_r} \equiv 1 \,(\mathfrak{G}_1),$

therefore $\quad \nu_r \equiv 0 \,(n_r),$

hence $\prod_1^{r-1} S_i^{\nu_i} \equiv 1 \,(\bar{\mathfrak{A}})$, and the induction hypothesis applied to $\mathfrak{G}_1$ gives

$$\nu_i \equiv 0 \,(n) \qquad (i = 1, 2, \ldots, r-1).$$

$\mathfrak{G}/\bar{\mathfrak{A}}$ is the direct product of the cyclic groups $(S_i\,\bar{\mathfrak{A}})$ with orders n_i $(i=1, 2, \ldots, r)$, Q.E.D. If the normal subgroup $\mathfrak{A}$ is abelian then the conditions can be stated more simply:

1. $(A\,B)^{\sigma_i} = A^{\sigma_i} B^{\sigma_i}$,
2. $A^{\sigma_i^{n_i}} = A$,
2a. $n_i \geqq 0$, and if $n_i = 0$, then $A_i = 1$,
3. $A^{\sigma_i \sigma_k} = A^{\sigma_k \sigma_i}$,
3a. $A_{i,k} A_{k,i} = 1 \quad (i < k)$,
4. $A_k^{\sigma_k - 1} = A_{i,k}^{1+\sigma_k+\sigma_k^2+\cdots+\sigma_k^{n_k-1}}$ (if $n_k > 0$, $i \neq k$),
5. $A_{i,k}^{\sigma_l - 1} A_{k,l}^{\sigma_i - 1} A_{l,i}^{\sigma_k - 1} = 1 \quad (i < k < l)$

and the relations

b) $S_i A S_i^{-1} = A^{\sigma_i}$,

c) $S_i^{n_i} = A_i$,

d) $S_i S_k S_i^{-1} S_k^{-1} = A_{i,k} \quad (i<k)$.

§ 9. Splitting Groups

Definition: A group $\overline{\mathfrak{G}}$ which contains the extension $\mathfrak{G}$ of $\mathfrak{N}$ by $\mathfrak{F}$ with the system of representatives S_σ is said to be a *splitting group* of $\mathfrak{G}$ over $\mathfrak{N}$, if $\overline{\mathfrak{G}}$ has a normal subgroup $\overline{\mathfrak{N}}$ containing $\mathfrak{N}$, with S_σ as system of representatives, such that $\overline{\mathfrak{G}}$ splits over $\overline{\mathfrak{N}}$.

THEOREM 22 (Artin): *Every group with abelian normal subgroup $\mathfrak{N}$ has a splitting group.*

Proof: We set $A_1 = C_{1,1}^{-1}$, but let (A_σ) be the infinite cyclic group generated by the new element A_σ, if $\sigma \neq 1$. Let $\overline{\mathfrak{N}}$ be the direct product of $\mathfrak{N}$ with the (A_σ), $(\sigma \neq 1)$. Then an operator S_σ of $\overline{\mathfrak{N}}$ is defined by

$$A_\tau^{S_\sigma} = A_\sigma^{-1} A_{\sigma\tau} C_{\sigma,\tau}^{-1} \qquad (\tau \neq 1)$$

and $$\overline{N}^{S_\sigma} = \Big(N \cdot \prod_\tau A_\tau^{m_\tau}\Big)^{S_\sigma} = N^{S_\sigma} \cdot \prod_\tau (A_\tau^{S_\sigma})^{m_\tau}.$$

The same formula holds for $A_1^{S_\sigma}$, since

$$A_1^{S_\sigma} = (C_{1,1}^{-1})^{S_\sigma} = C_{\sigma,1}^{-1} = A_\sigma^{-1} A_\sigma C_{\sigma,1}^{-1}.$$

The factor system $C_{\sigma,\tau}$ and the mapping S_σ satisfy conditions I and III. Now II must be verified.

$A^{S_1} = A^{C_{1,1}}$ holds for all A in $\mathfrak{N}$:

$$A_\tau^{S_1} = A_1^{-1} A_\tau C_{1,1}^{-1} = C_{1,1} A_\tau C_{1,1}^{-1} = A_\tau^{C_{1,1}},$$

and therefore $\overline{N}^{S_1} = \overline{N}^{C_{1,1}}$ for all $\overline{N}$ in $\overline{\mathfrak{N}}$.

$$\begin{aligned}
(A_\varrho^{S_\tau})^{S_\sigma} &= (A_\tau^{-1} A_{\tau\varrho} C_{\tau,\varrho}^{-1})^{S_\sigma} = (A_\tau^{S_\sigma})^{-1} A_{\tau\varrho}^{S_\sigma} (C_{\tau,\varrho}^{S_\sigma})^{-1} \\
&= (A_\sigma^{-1} A_{\sigma\tau} C_{\sigma,\tau}^{-1})^{-1} A_\sigma^{-1} A_{\sigma\tau\varrho} C_{\sigma,\tau\varrho}^{-1} (C_{\tau,\varrho}^{S_\sigma})^{-1} = C_{\sigma,\tau} A_{\sigma\tau}^{-1} A_{\sigma\tau\varrho} C_{\sigma,\tau\varrho}^{-1} (C_{\tau,\varrho}^{S_\sigma})^{-1} \\
&= (A_{\sigma\tau}^{-1} A_{\sigma\tau\varrho})^{C_{\sigma,\tau}} C_{\sigma,\tau} (C_{\sigma,\tau} C_{\sigma\tau,\varrho})^{-1} = (A_{\sigma\tau}^{-1} A_{\sigma\tau\varrho} C_{\sigma\tau,\varrho}^{-1})^{C_{\sigma,\tau}} \text{ (by III.!)} \\
&= A_\varrho^{C_{\sigma,\tau} S_{\sigma\tau}}.
\end{aligned}$$

Since II is valid in $\mathfrak{N}$ it holds also in $\overline{\mathfrak{N}}$. Therefore there exists an extension group $\overline{\mathfrak{G}}$ of $\overline{\mathfrak{N}}$ with the elements S_σ as system of representatives, the $C_{\sigma,\tau}$ as factor system, and the S_σ as automorphisms of $\overline{\mathfrak{N}}$.

This extension naturally contains the extension $\mathfrak{G}$ of $\mathfrak{N}$ with the factor group $\mathfrak{F}$ and system of representatives S_σ. $\overline{\mathfrak{G}}$ is a splitting group of $\mathfrak{G}$ since

$$e = A_\sigma A_\tau^{S_\sigma} C_{\sigma,\tau} A_{\sigma\tau}^{-1}.$$ [1]

[1] If we take $\overline{\mathfrak{G}}$ as the free product (which will be defined later) of $\mathfrak{G}$ with the infinite cyclic groups (A_σ) then it follows in exactly the same way that every group has a splitting group.

IV. SYLOW p-GROUPS AND p-GROUPS

§ 1. The Sylow Theorems

In a finite group $\mathfrak{G}$ of order N, the order of every subgroup is a divisor of N. On the other hand there need not be a subgroup with order d for every divisor d of N. For example, in the tetrahedral group, as one can see easily, there is no subgroup of order 6. We shall now prove, however, that for every power p^a of a prime dividing N there is a subgroup with the order p^a.

DEFINITION: A group is said to be a *p-group* if its order is a power of the prime p.

We determine the largest possible p-groups in the finite group $\mathfrak{G}$.

DEFINITION: A subgroup of $\mathfrak{G}$ is said to be a *Sylow p-group*, if its order is equal to the greatest power of the natural prime p dividing N.

For example, the four group is a Sylow 2-group of the tetrahedral group. A Sylow p-group of $\mathfrak{G}$ is denoted by S_p or by $\mathfrak{P}$. The normalizer of S_p in $\mathfrak{G}$ is denoted by N_p, the center of S_p by z_p.

THEOREM 1. *For every natural prime p, every finite group contains a Sylow p-group.*

Proof: If the order N of $\mathfrak{G}$ is 1, then the theorem is clear. Now let $N>1$ and assume the theorem proven for groups of order smaller than N.

If in the center $\mathfrak{z}$ of $\mathfrak{G}$ there is an element a of order $m.p$, then the factor group $\mathfrak{G}/(a^m)$ is of order $\frac{N}{p}$ and contains by the induction assumption a Sylow p-group $\mathfrak{P}/(a^m)$ of order p^{n-1}, where $\frac{N}{p^n}$ is not divisible by p.

$\mathfrak{P}$ is of order p^n and therefore is a Sylow p-group of $\mathfrak{G}$.

Now let there be no element of order divisible by p in the center $\mathfrak{z}$ of $\mathfrak{G}$. If the order of $\mathfrak{z}$ were divisible by p, then the factor group of $\mathfrak{z}$ with respect to a cyclic normal subgroup $(a) \neq 1$ is of order divisible by p. But then by the induction hypothesis $\mathfrak{z}/(a)$ would contain a Sylow p-group $\neq 1$, and therefore would contain elements $b.(a)$ of order divisible by p. Then the order of b in $\mathfrak{z}$ would be divisible by p. Therefore the order of $\mathfrak{z}$ is not divisible by p. If $p \nmid N$ then e is the Sylow p-group sought. If p/N then it follows from the class equation

$$N = (\mathfrak{z} : 1) + \sum_{h_i > 1} h_i$$

and from $p \nmid (\mathfrak{Z}:1)$, p/N, that at least one $h_i > 1$ is not divisible by p. $\mathfrak{G}$ contains a normalizer N_i of index $h_i > 1$ and therefore N_i contains, by the induction hypothesis, a Sylow p-group $\mathfrak{P}$. Since $p \nmid h_i$, $\mathfrak{P}$ is also a Sylow p-group of $\mathfrak{G}$.

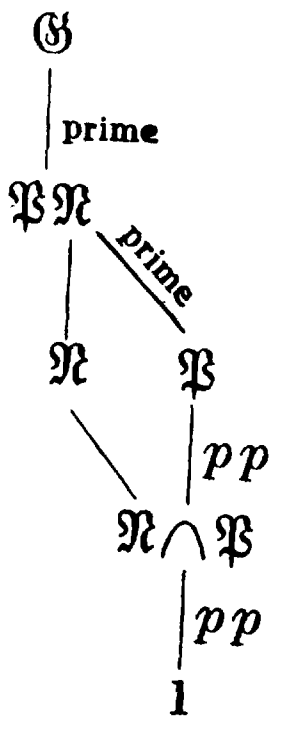
COROLLARY: For every prime divisor p of the order of a finite group there is an element of order p (Cauchy).

The order and exponent of a finite group have the same prime divisors.

THEOREM 2: *If $\mathfrak{P}$ is a Sylow p-group of $\mathfrak{G}$ and $\mathfrak{N}$ a normal subgroup of $\mathfrak{G}$, then $\mathfrak{N} \cap \mathfrak{P}$ is a Sylow p-group of $\mathfrak{N}$; $\mathfrak{P}\mathfrak{N}/\mathfrak{N}$ is a Sylow p-group of $\mathfrak{G}/\mathfrak{N}$.*

Proof[1]: A subgroup $\mathfrak{U}$ of $\mathfrak{G}$ is a Sylow p-group if and only if

1. The order of $\mathfrak{U}$ is a power of p (written: pp),
2. The index of $\mathfrak{U}$ is prime to p (written: *prime*).



Now we may construct the diagram to the left and observe first that $\mathfrak{P}\mathfrak{N}:\mathfrak{P}$ is prime to p, and $\mathfrak{P}:\mathfrak{N} \cap \mathfrak{P}$ is a p-power. From the second isomorphism theorem it follows that $\mathfrak{P}\mathfrak{N}:\mathfrak{N}$ is the p-power, hence $\mathfrak{N}:\mathfrak{N} \cap \mathfrak{P}$ is prime to p, from which the theorem follows.

If a Sylow p-group $\mathfrak{P}$ is a normal subgroup of $\mathfrak{G}$ then it is the only Sylow p-group, since for every other Sylow p-group $\mathfrak{P}_1$ it follows that $\mathfrak{P}_1\mathfrak{P}$ is of p-power order, but $\mathfrak{G}:\mathfrak{P}_1\mathfrak{P}$ is prime to p, and therefore $\mathfrak{P}_1\mathfrak{P} = \mathfrak{P} = \mathfrak{P}_1$. Consequently a Sylow p-group S_p of a finite group $\mathfrak{G}$ is the only Sylow p-group of its normalizer N_p.

THEOREM 3: *All Sylow p-groups of a finite group $\mathfrak{G}$ are conjugate under $\mathfrak{G}$. Their number when divided by p leaves a remainder 1.*

Proof: Let the Sylow p-groups of $\mathfrak{G}$ be $\mathfrak{P} = \mathfrak{P}_1, \ldots, \mathfrak{P}_r$.

Under the mapping $x \to \begin{pmatrix} a \\ x\,a\,x^{-1} \end{pmatrix}$ of $\mathfrak{G}$ onto the group of inner automorphisms, $\mathfrak{P}$ is represented as a permutation group. Since conjugate subgroups have the same order, the $\mathfrak{P}_i$ are transformed into each other by $\mathfrak{P}$, so that we obtain a representation Δ of $\mathfrak{P}$ as a permutation group of degree r. By a remark above, $\mathfrak{P}$ transforms only $\mathfrak{P}_1$ and no other $\mathfrak{P}_i$ into itself. Consequently there is only one system of transitivity of first degree. The other systems of transitivity of Δ have a degree > 1 which is a divisor of $\mathfrak{P}:1$ and which, therefore, is a p-power. Consequently $r \equiv 1\,(p)$.

$\mathfrak{P}$ transforms the $s = \mathfrak{G}:N_p$ Sylow p-groups conjugate to $\mathfrak{P}$ under $\mathfrak{G}$

[1] According to a communication from E. Witt.

among themselves, and as above it follows that $s \equiv 1\,(p)$. If there were another system of conjugate Sylow p-groups, then its members would be transformed into each other by $\mathfrak{P}$ in systems of transitivity whose degree would be divisible by p. The system would therefore contain a number s_1, divisible by p, of Sylow p-groups; on the other hand we conclude for s_1, just as we did for s, that $s_1 \equiv 1\ (p)$. Consequently all Sylow p-groups are conjugate to $\mathfrak{P}$, Q.E.D.

THEOREM 4: *Every p-group $\mathfrak{U}$ in $\mathfrak{G}$ is contained in a Sylow p-group.*

Proof: We replace $\mathfrak{P}$ by $\mathfrak{U}$ in the proof of the previous theorem. Let the transformed objects again be $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$. The degree of a system of transitivity of Δ is either 1 or a p-power. Since $r \equiv 1\,(p)$, there is certainly a system of transitivity of degree 1. Therefore there is a $\mathfrak{P}_i$ which is transformed into itself by all the elements of $\mathfrak{U}$. Since $\mathfrak{U}\mathfrak{P}_i$ is a p-group which contains $\mathfrak{P}_i$, we have $\mathfrak{U}\mathfrak{P}_i = \mathfrak{P}_i$, $\mathfrak{U} \subseteq \mathfrak{P}_i$, , Q.E.D.

THEOREM 5: *Every subgroup $\mathfrak{U}$ of $\mathfrak{G}$ which contains the normalizer N_p of a Sylow p-group S_p, is its own normalizer.*

Proof: We must show that $x\,\mathfrak{U}\,x^{-1} \subseteq \mathfrak{U}$ implies

$$x \in \mathfrak{U}.$$

In any case S_p and xS_px^{-1} are Sylow p-groups of $\mathfrak{U}$, and by Theorem 3 there is a U in $\mathfrak{U}$ such that $U\,x\,S_p\,x^{-1}U^{-1} = S_p$;

therefore $$Ux \in N_p \subseteq \mathfrak{U},$$

therefore $$x \in \mathfrak{U},$$ Q.E.D.

THEOREM 6: *If the p-group $\mathfrak{U}$ contained in the finite group $\mathfrak{G}$ is not a Sylow p-group, then the normalizer $N_{\mathfrak{U}}$ of $\mathfrak{U}$ is larger than $\mathfrak{U}$.*

Proof: If $p \nmid \mathfrak{G} : N_{\mathfrak{U}}$ then the theorem is clear; if, however $\mathfrak{G} : N_{\mathfrak{U}} = pr$, then $\mathfrak{U}$ transforms the pr subgroups conjugate to $\mathfrak{U}$ in systems of transitivity whose degrees are 1 or numbers divisible by p. Since $\mathfrak{U}$ is transformed into itself, there are at least p subgroups $\mathfrak{U}_1 = \mathfrak{U}, \mathfrak{U}_2, \ldots, \mathfrak{U}_p$, conjugate to $\mathfrak{U}$ which are transformed into themselves by $\mathfrak{U}$. Consequently $N_{\mathfrak{U}_2}$ is greater than $\mathfrak{U}_2$, and therefore $N_{\mathfrak{U}}$ is greater than $\mathfrak{U}$, Q.E.D.

COROLLARIES:

1. Every maximal subgroup of a p-group is a normal subgroup; therefore it is of index p.

2. If a p-group is simple then it is of order p.

3. The composition factors of a p-group are of order p and therefore every p-group is solvable.

§ 2. Theorems on Sylow p-Groups

Information on the intersection of different Sylow p-groups is given by

THEOREM 7: *In the normalizer of a maximal*[1] *intersection* $\mathfrak{D}$ *of two different Sylow p-groups of* $\mathfrak{G}$ *we have*:

1. *Every Sylow p-group of* $N_{\mathfrak{D}}$ *contains* $\mathfrak{D}$ *properly.*
2. *The number of Sylow p-groups of* $N_{\mathfrak{D}}$ *is greater than* 1.
3. *The intersection of two distinct Sylow p-groups of* $N_{\mathfrak{D}}$ *is equal to* $\mathfrak{D}$.
4. *Every Sylow p-group of* $N_{\mathfrak{D}}$ *is the intersection of* $N_{\mathfrak{D}}$ *with exactly one Sylow p-group of* $\mathfrak{G}$.
5. *The intersection of* $N_{\mathfrak{D}}$ *with a Sylow p-group of* $\mathfrak{G}$ *which contains* $\mathfrak{D}$ *is a Sylow p-group of* $N_{\mathfrak{D}}$.
6. *The normalizer of a Sylow p-group of* $N_{\mathfrak{D}}$ *in* $N_{\mathfrak{D}}$ *is equal to the intersection of* $N_{\mathfrak{D}}$ *with the normalizer of a Sylow p-group of* $\mathfrak{G}$ *which contains* $\mathfrak{D}$.

Proof: $\mathfrak{D}$ is in a Sylow p-group $\mathfrak{P}$ of $\mathfrak{G}$ and by hypothesis $\mathfrak{D} \neq \mathfrak{P}$. Therefore by Theorem 6: $\mathfrak{D} \neq \mathfrak{p} = N_{\mathfrak{D}} \cap \mathfrak{P}$. $\mathfrak{p}$ is a p-group in $N_{\mathfrak{D}}$, thus by Theorem 4 it lies in a Sylow p-group $\bar{\mathfrak{p}}$ of $N_{\mathfrak{D}}$. By Theorem 4, $\bar{\mathfrak{p}}$ lies in a Sylow p-group $\bar{\mathfrak{P}}$ of $\mathfrak{G}$. Since $\mathfrak{P} \cap \bar{\mathfrak{P}}$ contains $\mathfrak{p}$ and thus is larger than $\mathfrak{D}$, $\mathfrak{P} = \bar{\mathfrak{P}}$. Therefore $\mathfrak{p} = \mathfrak{P} \cap N_{\mathfrak{D}} = \bar{\mathfrak{p}}$ is a Sylow p-group of $N_{\mathfrak{D}}$, and the $\mathfrak{P}$ in $\mathfrak{p} = \mathfrak{P} \cap N_{\mathfrak{D}}$ is uniquely determined by $\mathfrak{p}$. Since every p-group in $N_{\mathfrak{D}}$ is in a Sylow p-group of $\mathfrak{G}$, the intersection of two distinct Sylow p-groups of $N_{\mathfrak{D}}$ is equal to $\mathfrak{D}$. Since $\mathfrak{D}$ is the intersection of two different Sylow p-groups of $\mathfrak{G}$, $N_{\mathfrak{D}}$ contains several Sylow p-groups. $\mathfrak{p} = \mathfrak{P} \cap N_{\mathfrak{D}}$ is a normal subgroup of $n_{\mathfrak{p}} = N_{\mathfrak{P}} \cap N_{\mathfrak{D}}$. If we have

$$x\,\mathfrak{p}\,x^{-1} = \mathfrak{p},$$

for an x in $N_{\mathfrak{D}}$, then it follows that $\mathfrak{p} \leq x\,\mathfrak{P}\,x^{-1}$, and therefore by 4., $\mathfrak{P} = x\,\mathfrak{P}\,x^{-1}$, $x \leq N_{\mathfrak{P}}$, $x \in n_{\mathfrak{p}}$, consequently $n_{\mathfrak{p}} = N_{\mathfrak{P}} \cap N_{\mathfrak{D}}$ is the normalizer of $\mathfrak{p}$ in $N_{\mathfrak{D}}$, Q.E.D. .

As an application of this theorem, we shall show that *every group* $\mathfrak{G}$ of order $p^n q$ *is solvable* (p, q *are two distinct primes*).

If a Sylow p-group $\mathfrak{P}$ is a normal subgroup, then $\mathfrak{G}/\mathfrak{P}$ is cyclic and by Theorem 6, Corollary 3, $\mathfrak{P}$ is solvable. Hence $\mathfrak{G}$ is solvable. Now suppose $\mathfrak{P}$ is not a normal subgroup of $\mathfrak{G}$; then $\mathfrak{G} : N_{\mathfrak{P}} = q$, $N_{\mathfrak{P}} = \mathfrak{P}$.

[1] If $\mathfrak{D}$ is the intersection of two Sylow p-groups and no group containing $\mathfrak{D}$ properly is contained in the intersection of *any* two Sylow p-groups, $\mathfrak{D}$ is called a *maximal* intersection of two Sylow p-groups.

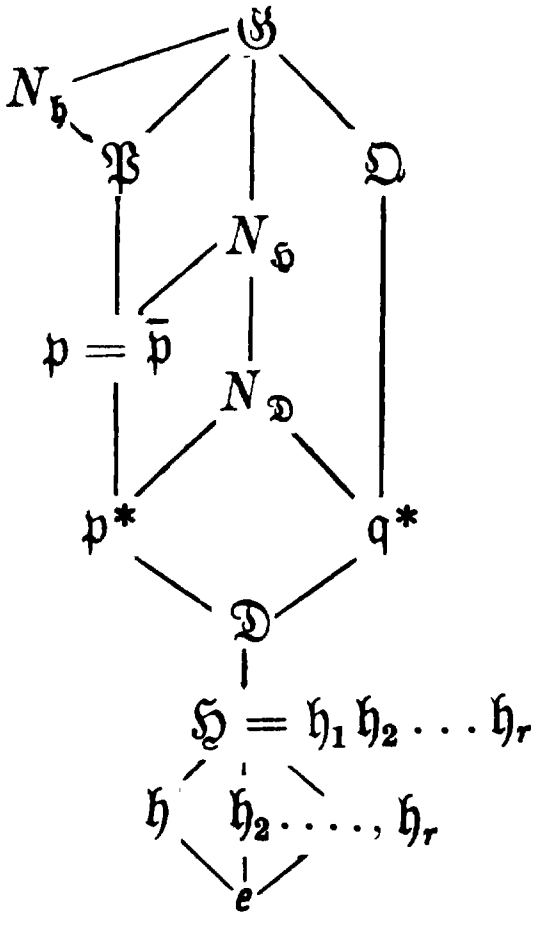
If the intersection of any two different Sylow p-groups is 1, then there are $1 + q.(p^n - 1)$ elements of p-power order, and therefore there is at most one subgroup with order q. Consequently a Sylow q-group $\mathfrak{Q}$ is a normal subgroup of $\mathfrak{G}$, and $\mathfrak{G}/\mathfrak{Q}$ is isomorphic to $\mathfrak{P}$. Since $\mathfrak{G}/\mathfrak{Q}$ and $\mathfrak{Q}$ are solvable, $\mathfrak{G}$ is also solvable. Finally let $\mathfrak{D}$ be a maximal intersection of different Sylow p-groups greater than 1. The number of Sylow p-groups of $N_{\mathfrak{D}}$ is > 1, is not divisible by p, is a divisor of $p^n q$ and therefore is equal to q. Also it follows from the previous theorem that $\mathfrak{D}$ lies in q different Sylow p-groups of $\mathfrak{G}$. Therefore $\mathfrak{D}$ is the intersection of all the Sylow p-groups of $\mathfrak{G}$. $\mathfrak{D}$ is a normal subgroup of $\mathfrak{G}$, and the factor group $\mathfrak{G}/\mathfrak{D}$ has as the maximal intersection of different Sylow p-groups the element 1. By what has already been proven, $\mathfrak{G}/\mathfrak{D}$ is solvable. Moreover the p-group $\mathfrak{D}$ is solvable. Consequently $\mathfrak{G}$ is solvable, Q.E.D.

For many applications the following theorem is useful:

THEOREM 8 (Burnside): *If the p-group $\mathfrak{h}$ in the finite group $\mathfrak{G}$ is a normal subgroup of one Sylow p-group but is not a normal subgroup of another Sylow p-group, then there is a number r, relatively prime to p, of subgroups $\mathfrak{h}_1, \mathfrak{h}_2, \ldots, \mathfrak{h}_r (r > 1)$ conjugate to $\mathfrak{h}$ which are all normal subgroups of $\mathfrak{H} = \mathfrak{h}_1 \mathfrak{h}_2 \ldots \mathfrak{h}_r$ but which are not all normal subgroups of the same Sylow p-group of $\mathfrak{G}$, so that the normalizer of $\mathfrak{H}$ transforms the $\mathfrak{h}_i$ transitively among themselves.*

Proof: Among the Sylow p-groups which contain $\mathfrak{h}$ as a non-normal subgroup, $\mathfrak{Q}$ is chosen so that the intersection $\mathfrak{D}$ of $\mathfrak{Q}$ with the normalizer $N_{\mathfrak{H}}$ of $\mathfrak{H}$ is as large as possible. Let $\mathfrak{h} = \mathfrak{h}_1, \mathfrak{h}_2, \ldots, \mathfrak{h}_s$ be the subgroups conjugate to $\mathfrak{h}$ in the normalizer $N_{\mathfrak{D}}$ of $\mathfrak{D}$. Along with $\mathfrak{h}$, all the $\mathfrak{h}_i$ are also normal subgroups of $\mathfrak{D}$. The normalizer $N_{\mathfrak{h}}$ of $\mathfrak{H} = \mathfrak{h}_1 \mathfrak{h}_2 \ldots \mathfrak{h}_s$ contains $N_{\mathfrak{D}}$. Let $\mathfrak{h}_1, \mathfrak{h}_2, \ldots, \mathfrak{h}_s, \ldots, \mathfrak{h}_r$ be all the groups conjugate to $\mathfrak{h}$ in $N_{\mathfrak{H}}$. Along with $\mathfrak{h}$, all the $\mathfrak{h}_i$ are normal subgroups of $\mathfrak{H}$. $\mathfrak{D}$ is contained in a Sylow p-group $\mathfrak{p}^*$ of $N_{\mathfrak{D}} \cap N_{\mathfrak{h}}$. Since $\mathfrak{D}$ is not a Sylow p-group of $\mathfrak{G}$, while, by hypothesis, a Sylow p-group of $N_{\mathfrak{h}}$ is also a Sylow p-group of $\mathfrak{G}$, then $\mathfrak{p}^*$ is larger than $\mathfrak{D}$. $\mathfrak{p}^*$ is in a Sylow p-group $\bar{\mathfrak{p}}$ of $N_{\mathfrak{H}} \cap N_{\mathfrak{h}}$. $\bar{\mathfrak{p}}$ is in a Sylow p group $\mathfrak{p}$ of $N_{\mathfrak{H}}$, and $\mathfrak{p}$ in a Sylow p-group $\mathfrak{P}$ of $\mathfrak{G}$. Since the intersection of $\mathfrak{P}$ with $N_{\mathfrak{h}}$ contains $\mathfrak{p}^*$, and therefore is larger than $\mathfrak{D}$, then by the construction of $\mathfrak{D}$ the Sylow p-group $\mathfrak{P}$ of $\mathfrak{G}$ is contained in $N_{\mathfrak{h}}$, and therefore a fortiori $\mathfrak{p}$ is contained in $N_{\mathfrak{h}}$.

Since $\mathfrak{p}$ contains the Sylow p-group $\bar{\mathfrak{p}}$ of $N_{\mathfrak{H}} \cap N_{\mathfrak{h}}$, we have $\mathfrak{p} = \bar{\mathfrak{p}}$. Since therefore a Sylow p-group of $N_{\mathfrak{H}} \cap N_{\mathfrak{h}}$ is already a Sylow p-group of $N_{\mathfrak{H}}$, $r = N_{\mathfrak{H}} : N_{\mathfrak{H}} \cap N_{\mathfrak{h}}$ is relatively prime to p. If all the $\mathfrak{h}_i$ were



normal subgroups of the same Sylow p-group of $\mathfrak{G}$, then the latter would be contained in $N_{\mathfrak{H}}$. But then the groups $\mathfrak{h}_i$ conjugate to each other in $N_{\mathfrak{H}}$ would be normal subgroups in all the Sylow p-groups of $N_{\mathfrak{H}}$. Then $\mathfrak{h}$ would be a normal subgroup of the Sylow p-group $\mathfrak{q}^*$ of the intersection of $N_{\mathfrak{D}}$ with $\mathfrak{Q}$. But $\mathfrak{q}^*$ is larger than $\mathfrak{D}$, and this contradicts the definition of $\mathfrak{D}$ as the intersection of $\mathfrak{Q}$ with $N_{\mathfrak{h}}$; therefore the $\mathfrak{h}_i$ are not all normal subgroups of the same Sylow p-group of $\mathfrak{G}$, Q.E.D.

The positional relationships of the subgroups of $\mathfrak{G}$ constructed in this proof can be seen from the diagram on the left.

§ 3. On p-Groups

1. *Nilpotent Groups.*

Fundamental for the theory of p-groups is the following statement:

THEOREM 9: *The center of a p-group different from e is itself different from e.*

Proof: From the class equation for a group of order $p^n > 1$:

$$p^n = \mathfrak{z} : 1 + \sum_{i>0} p^i,$$

where the summands p^i run through indices > 1 of certain normalizers. Therefore $\mathfrak{z} : 1$ is divisible by p, and consequently $\mathfrak{z} \neq e$.

COROLLARY: The $(n+1)$-th member of the ascending central series of a group $\mathfrak{G}$ of order p^n is equal to the whole group.

The members of the ascending central series are defined as the normal subgroups $\mathfrak{z}_i$ of $\mathfrak{G}$ such that $\mathfrak{z}_0 = e$, $\mathfrak{z}_{i+1}/\mathfrak{z}_i$ is the center of $\mathfrak{G}/\mathfrak{z}_i$. Now either $\mathfrak{z}_i = \mathfrak{G}$ or, as just proven, $\mathfrak{z}_{i+1}$ is larger than $\mathfrak{z}_i$, and therefore certainly $\mathfrak{z}_n = \mathfrak{G}$.

By refinement of the ascending central series of a p-group we obtain a principal series in which every factor is of order p. It follows from the Jordan - Hölder - Schreier theorem that:

Every principal series of a p-group has steps of prime order.

The index of the center of a non-abelian p-group is divisible by p^2. This follows from the useful lemma: *If a normal subgroup $\mathfrak{N}$ of a group $\mathfrak{G}$ is contained in the center and has a cyclic factor group, then $\mathfrak{G}$ is abelian.*

Since $\mathfrak{G}/\mathfrak{N}$ is generated by a coset $A\mathfrak{N}$, all the elements of $\mathfrak{G}$ are of the form A^iZ where Z is in the center.
Therefore

$$A^iZ \cdot A^kZ' = A^{i+k}ZZ' = A^kZ' \cdot A^iZ$$

and $\mathfrak{G}$ is abelian.

If we apply the result found above to a p-group in which $\mathfrak{G} = \mathfrak{z}_c \neq \mathfrak{z}_{c-1} \neq e$, then: $p^2/\mathfrak{G} : \mathfrak{z}_{c-1}$, and since $\mathfrak{G}/\mathfrak{z}_{c-1}$ is abelian, it follows that:

The factor commutator group of a non-abelian p-group has an order divisible by p^2.

A group of order p or p^2 is abelian. In a non-abelian group of order p^3, the center and the commutator group are identical and are of order p.

DEFINITION: A group $\mathfrak{G}$ is said to be *nilpotent*[1] if the ascending central series contains the whole group as a member, if therefore

$$e = \mathfrak{z}_0 \subset \mathfrak{z}_1 \subset \mathfrak{z}_2 \subset \cdots \subset \mathfrak{z}_c = \mathfrak{G}.$$

The uniquely determined number c is called, following Hall, the *class of the group*. Therefore "nilpotent of class 1" is the same as "abelian $\neq e$."

THEOREM 10: *In a nilpotent group of class c it is possible to ascend to the whole group from any subgroup by forming normalizers at most c times.*

Proof: Let $\mathfrak{G}$ be nilpotent of class c; let $\mathfrak{U}$ be be a subgroup. Certainly $\mathfrak{z}_0$ is contained in $\mathfrak{U}$. If $\mathfrak{z}_i$ is already contained in $\mathfrak{U}$, then by the definition of $\mathfrak{z}_{i+1}$, it follows that $\mathfrak{z}_{i+1}$ is contained in the normalizer of $\mathfrak{U}$. By at most c repetitions of this procedure we obtain the result.

COROLLARY: *Every maximal subgroup of a nilpotent group is a normal subgroup and therefore is of prime index.*

Therefore in a p-group $\mathfrak{G}$ the intersection of all the normal subgroups of index p is equal to the Φ-subgroup defined earlier. The factor group $\mathfrak{G}/\Phi$ is an abelian group of exponent p. By its order p^d the important invariant $d = d(\mathfrak{G})$ is defined. The significance of d is made clear by the following BURNSIDE BASIS THEOREM: *From every system of generators of $\mathfrak{G}$ exactly d can be selected so that these alone generate $\mathfrak{G}$.* By the general basis theorem this theorem need only be proven for $\mathfrak{G}/\Phi$.

[1] This name is used because for finite continuous groups the associated Lie ring of infinitesimal transformations is nilpotent precisely when the ascending central series terminates with the full group.

2. *Elementary Abelian Groups.*

An abelian group $\mathfrak{A}$ with prime exponent p is called an *elementary abelian group.* If $\mathfrak{A}$ is of order p^d then it is possible to generate $\mathfrak{A}$ by d elements: Let S_1 be an element $\neq e$ in $\mathfrak{A}$; let S_2 be an element in $\mathfrak{A}$ not in (S_1) ; let S_3 be an element of $\mathfrak{A}$ not in $\{S_1, S_2\}$; let $S_{d'}$ be an element in $\mathfrak{A}$ and not in $\{S_1, S_2, \ldots, S_{d'-1}\}$ and $\{S_1, S_2, \ldots, S_{d'}\} = \mathfrak{A}$. Then (S_i) is of prime order p so that we must have

$$(S_i) \cap \{S_1, S_2, \ldots, S_{i-1}\} = e$$

It follows from this that

$$\{S_1, S_2, \ldots, S_i\} = \{S_1, S_2, \ldots, S_{i-1}\} \times (S_i)$$

$$\mathfrak{A} = (S_1) \times (S_2) \times \cdots \times (S_d'),$$

and since $\mathfrak{A} : 1 = p^d$, , we see that $d = d'$. Therefore a finite elementary abelian group is the direct product of a finite number of cyclic groups of prime order. Conversely a direct product of a finite number of cyclic groups $(S_1), (S_2), \ldots, (S_d)$ of order p is an elementary abelian group. The elements $S_1, S_2, \ldots, S_d$ in the direct product representation are said to be a basis of $\mathfrak{A}$. The above method of construction shows that every generating system of $\mathfrak{A}$ contains a basis. Therefore d is the minimal number of generators. Consequently every system of d generators is a basis of $\mathfrak{A}$. The number of basis systems of $\mathfrak{A}$ can be calculated easily:

In the above construction there are p^d-1 possibilities for S_1; after choosing S_1, there are p^d-p possibilities for S_2 and so forth, so that we obtain the number $(p^d - 1)(p^d - p) \cdot \ldots \cdot (p^d - p^{d-1})$ as the number of basis systems of $\mathfrak{A}$. If $S_1, S_2, \ldots, S_d$ is a fixed basis and $T_1, T_2, \ldots, T_d$ is an arbitrary basis then the mapping

$$S_1^{\alpha_1} S_2^{\alpha_2}, \ldots, S_d^{\alpha_d} \rightarrow T_1^{\alpha_1} T_2^{\alpha_2}, \ldots, T_d^{\alpha_d}$$

defines an automorphism of $\mathfrak{A}$ and conversely. Therefore it follows that:

The number of automorphisms of an elementary abelian group of order p^d is equal to $(p^d - 1)(p^d - p) \cdot \ldots \cdot (p^d - p^{d-1})$. If we set

$$k_d = (p^d - 1) \quad (p^{d-1} - 1) \cdot \ldots \cdot (p - 1),$$

then the number is equal to $p^{\frac{1}{2}d(d-1)} k_d$. From the general basis theorem in II, § 4, it follows that:

The number of automorphisms of a p-group of order p^n $(n > 0)$ and d generators is a divisor of

$$p^{d(n-d)} \cdot (p^d - p)(p^d - p) \cdot \ldots \cdot (p^d - p^{d-1}).$$

Remark: The highest power of p which divides this number is $p^{\frac{1}{2}d(2n-1-d)}$, and since $0 < d \leqq n$, this number is a divisor of $p^{\frac{1}{2}n(n-1)}$, as can easily be seen. Therefore the number of automorphisms of an arbitrary group of order p^n is a divisor of the number of automorphisms of the elementary abelian group of order p^n.

For later theorems it is important to obtain several formulae about the number $\varphi_{d,\alpha}$ of subgroups of order p^α in the elementary abelian group of order p^d. Let $0 < \alpha \leqq d$. Every subgroup of order p^α is elementary.

If $S_1, S_2, \ldots, S_\alpha$ are the first α elements of a basis of the whole group, then these α elements are a basis of a subgroup of order p^α Conversely, as we have seen

previously, every basis of a subgroup of order p^α can be extended to a basis of the whole group. Since the elements $S_1, S_2, \ldots, S_\alpha$ can be chosen in

$$(p^d - 1)(p^d - p)\cdot\ldots\cdot(p^d - p^{\alpha-1})$$

different ways, and every subgroup of order p^α has $(p^\alpha - 1)\cdot\ldots\cdot(p^\alpha - p^{\alpha-1})$ different basis systems, then

$$(1) \qquad \varphi_{d,\alpha} = \frac{(p^d-1)\cdot\ldots\cdot(p^d-p^{\alpha-1})}{(p^\alpha-1)\cdot\ldots\cdot(p^\alpha-p^{\alpha-1})} = \frac{k_d}{k_\alpha k_{d-\alpha}} = \varphi_{d,d-\alpha},$$

where $k_0 = 1$. From this the reader can derive the recursion formula

$$(2) \qquad \varphi_{d+1,\alpha} = \varphi_{d,\alpha} + p^{d+1-\alpha}\varphi_{d,\alpha-1}$$

for $0 < \alpha \leqq d$, where $\varphi_{d,0} = 1 = \frac{k_d}{k_0 k_d}$. If we set $\varphi_{d,\alpha} = 0$ for rational integers α which are larger than d or smaller than 0, then the formula is valid generally. From this formula we derive the congruence

$$(3) \qquad \varphi_{d+i,\alpha} \equiv \varphi_{d,\alpha}\,(p^{d+1-\alpha}) \qquad (i \geqq 1)$$

and the polynomial identity

$$(4) \qquad \prod_{\nu=1}^{d}(x - p^{\nu-1}) = \sum_{0}^{d}(-1)^\alpha p^{\frac{1}{2}\alpha(\alpha-1)}\varphi_{d,\alpha}\,x^{d-\alpha}$$

by induction. If we set $x = 1$, then

$$(5) \qquad 0 = 1 - \varphi_{d,1} + p\,\varphi_{d,2} + \cdots + (-1)^d p^{\frac{1}{2}d(d-1)}.$$

An abelian group of order p^μ can be decomposed, by the basis theorem, into the direct product of cyclic groups of orders $p^{n_1}, p^{n_2}, \ldots, p^{n_r}$. Here the exponents $n_1, n_2, \ldots, n_r$ are determined uniquely to within order. Therefore we say: *The group is of type* $(p^{n_1}, p^{n_2}, \ldots, p^{n_r})$. If we order the n_i by size so that p^j occurs a_j times as the order of a basis element, then we say: *The group is of type*

$$a_1 \cdot 1 + a_2 \cdot 2 + \cdots + a_n \cdot n.$$

Here the non-negative integers a_i are bound only by the relation $\sum_1^n a_i \cdot i = n$.

3. *Finite Nilpotent Groups.*

The direct product of a finite number of nilpotent groups is nilpotent, as is easily seen. For example, the direct product of a finite number of p-groups is nilpotent. The following converse is important:

THEOREM 11: *Every finite nilpotent group is the direct product of its Sylow groups.*

Proof: The normalizer of a Sylow group is its own normalizer by Theorem 5, and therefore, by Theorem 10, it is equal to the whole group; consequently every Sylow group is a normal subgroup.

Let $p_1, p_2, \ldots, p_r$ be the various prime divisors of the group order, and assume we have already shown that

$$S_{p_1} S_{p_2} \cdot \ldots \cdot S_{p_i} = S_{p_1} \times S_{p_2} \times \cdots \times S_{p_i}, \quad i < r.$$

Then the normal subgroups $S_{p_1} \cdot S_{p_2} \cdot \ldots \cdot S_{p_i}$ and $S_{p_{i+1}}$ have relatively prime orders so that their intersection is e; and therefore

$$S_{p_1} \cdot S_{p_2} \cdot \ldots \cdot S_{p_{i+1}} = S_{p_1} \times S_{p_2} \times \cdots \times S_{p_{i+1}}.$$

But from the equation $S_{p_1} \cdot S_{p_2} \cdot \ldots \cdot S_{p_r} = S_{p_1} \times S_{p_2} \times \cdots \times S_{p_r}$ it follows, by comparing the orders, that the whole group is the direct product of its Sylow groups.

THEOREM 12: *The Φ-subgroup of a nilpotent group contains the commutator group.*

Proof: As we saw earlier, the Φ-subgroup is equal to the intersection of the whole group with its maximal subgroups. By the Corollary to Theorem 10, every maximal subgroup of a nilpotent group is a normal subgroup of prime index, and therefore every maximal subgroup of a nilpotent group contains the commutator group. Consequently the Φ-subgroup of a nilpotent group contains the commutator group.

Remark: We have further that $\Phi(\mathfrak{G})/\mathfrak{G}' = \Phi(\mathfrak{G}/\mathfrak{G}')$, which can be derived from the definition of the Φ-subgroup as the intersection of the whole group with its maximal subgroups.

For finite groups we have the converse:

THEOREM 13 (Wieland): *If the Φ-subgroup of a finite group contains the commutator group, then the group is nilpotent.*

Proof: As in the proof of Theorem 11 it suffices to prove that every Sylow group is a normal subgroup. If the normalizer of a Sylow group were not the whole group, then it would be contained in a maximal subgroup which on the one hand would contain the Φ-subgroup and therefore the commutator group; and on the other hand, by Theorem 5, must be its own normalizer. Since this is not possible, every Sylow group must be a normal subgroup of the whole group.

THEOREM 14 (Hall): *If the normal subgroup $\mathfrak{N}$ is not contained in $\mathfrak{z}_i$, but is contained in $\mathfrak{z}_{i+1}$, then the following is a normal subgroup chain without repetitions:* $\mathfrak{N} > \mathfrak{N} \cap \mathfrak{z}_i > \mathfrak{N} \cap \mathfrak{z}_{i-1} > \cdots > e$.

Proof: We have $(\mathfrak{G}, \mathfrak{N}) \leq \mathfrak{N} \cap (\mathfrak{G}, \mathfrak{z}_{i+1}) \leq \mathfrak{N} \cap \mathfrak{z}_i$. Since $\mathfrak{N}$ is not contained in $\mathfrak{z}_i$, $(\mathfrak{G}, \mathfrak{N})$ is not contained in $\mathfrak{z}_{i-1}$, and therefore $\mathfrak{N} \cap \mathfrak{z}_i$ is not contained in $\mathfrak{N} \cap \mathfrak{z}_{i-1}$. We apply the same argument to $\mathfrak{N} \cap \mathfrak{z}_i$, etc., Q.E.D.

4. *Maximal abelian normal subgroups.*

It is natural to consider the maximal abelian normal subgroups as well as the maximal abelian factor group. In general abelian normal subgroups which are contained in no other abelian normal subgroup are neither uniquely determined nor isomorphic to each other, as is easily seen in the example of the dihedral group of eight elements. The center seems to be more appropriate as a counterpart of the factor commutator group, as we already have seen in the theorems on direct products.

In any case, there is, in every group whose elements $e=a_1, a_2, \ldots$, are well ordered, a maximal abelian normal subgroup. We can construct an abelian normal subgroup $\mathfrak{A}_\omega$ for any index ω in the following way: $\mathfrak{A}_1 = e$ let $\mathfrak{B}_\omega$ be the union of all $\mathfrak{A}_\nu$ with $\nu < \omega$; let $\mathfrak{A}_\omega$ be equal to the normal subgroup generated by $\mathfrak{B}_\omega$ and a_ω if this normal subgroup is abelian. Otherwise let $\mathfrak{A}_\omega = \mathfrak{B}_\omega$. The union of all the $\mathfrak{A}_\omega$ is a maximal abelian normal subgroup.

A maximal abelian normal subgroup $\mathfrak{A}$ of a nilpotent group is its own centralizer.

Proof: The centralizer $Z_{\mathfrak{A}}$ is a normal subgroup of $\mathfrak{G}$. If $Z_{\mathfrak{A}}$ contained $\mathfrak{A}$ properly, then by Theorem 14, a center element $X\mathfrak{A}$ in $Z_{\mathfrak{A}}/\mathfrak{A}$ would be contained in $\mathfrak{G}/\mathfrak{A}$ [1] so that the subgroup generated by X and $\mathfrak{A}$ would be larger than $\mathfrak{A}$. But since this subgroup containing $\mathfrak{A}$ would also be an abelian normal subgroup, we must have $Z_{\mathfrak{A}} = \mathfrak{A}$.

If $\mathfrak{G}$ and $\mathfrak{A}$ are of orders p^n and p^m, respectively, then the index p^{n-m} is a divisor of the number of automorphisms of $\mathfrak{A}$, whereupon, by Part 2, it follows that

$$p^{n-m} / p^{\frac{1}{2}m(m-1)},$$

$$2n \leqq m(m+1). \tag{6}$$

5. *The automorphism group of Z_N.*

We wish to determine the automorphism group of the cyclic group Z_N for $N>1$. For this purpose we consider Z_N as the residue class module (quotient module) $\mathfrak{o}(N)$ of the additive group of integers with respect to the submodule of integers divisible by N. The operators of Z_N are given by the multiplications $\underline{t} = \begin{pmatrix} x \\ tx \end{pmatrix}$ by the rational integers t; $\underline{t_1}$ and $\underline{t_2}$ are equal if and only if t_1 and t_2 are congruent mod N. $\underline{t}$ is an automorphism if and only if t is relatively prime to N. The number $\varphi(N)$ of automorphisms of Z_N is equal to the number of residue classes (cosets) mod N which contain numbers relatively prime to N (*prime residue classes*).

The automorphism group of Z_N (cyclic group of order N) is isomorphic to the group of prime residue classes mod N. If N is the product of relatively prime numbers m_1, m_2, then Z_N is the direct product of two characteristic cyclic groups of orders m_1, m_2. For the automorphism group we have the corresponding situation; in particular

$$\varphi(N) = \varphi(m_1)\varphi(m_2).$$

[1] Here we must anticipate the result of § 5 which is trivial for p-groups; namely, that every factor group of a nilpotent group is itself nilpotent.

If N is the n-th power of a prime p then a residue class is prime if and only if it consists of numbers relatively prime to p; the number of these residue classes is $p^n - p^{n-1}$. If $N = p_1^{n_1} p_2^{n_2} \cdot \ldots \cdot p_r^{n_r}$ is the prime power decomposition, then

$$(7) \qquad \varphi(N) = \prod_1^r \varphi(p_i^{n_i}) = \prod_1^r (p_i^{n_i} - p_i^{n_i - 1}) = N \cdot \prod_1^r \left(1 - \frac{1}{p_i}\right).$$

The residue class ring $\mathfrak{o}(p)$ is a field and therefore, by II, § 7, the automorphism group of Z_p is cyclic of order $p-1$. A rational number g whose order mod p is $p-1$ is said to be a *primitive congruence root* mod p. g has an order which is divisible by $p-1$ mod p^n; say therefore, it has the order $(p-1) \cdot p^\nu$. The order of $g_1 = g^{p^\nu}$ is then equal to p-1, mod p^m. If $a = 1 + kp^m$, then it follows from the binomial theorem that $a^p \equiv 1 + kp^{m+1} + \frac{p(p-1)}{2} k^2 p^{2m} (p^{m+2})$. Therefore $a \equiv 1 (p^m)$ implies that $a^p \equiv 1 (p^{m+1})$. However if $m > 1$ or if p is odd then $a \not\equiv 1 (p^{m+1})$ implies that $a^p \not\equiv 1 (p^{m+2})$. If p is odd, then $1 + p$ is of order p^{n-1} mod p^n, $(1+p) \cdot g_1$ is of order $(p-1) \cdot p^{n-1}$. If $p = 2$, then $1 + 2^2$ is of order 2^{n-2} mod 2^n $(n > 2)$. Since -1 is congruent to no power of 5 mod 4, there are, mod 2^n, the 2^{n-1} different prime residue classes $\pm 5^\nu$ $(0 \leqq \nu < 2^{n-2})$. As a result we obtain:

If $n < 3$ or p is odd, then the automorphism group of Z_{p^n} is cyclic of order $(p-1)p^{n-1}$. The automorphism group of Z_{2^n}, for $n > 2$, is abelian of type $(2^{n-2}, 2)$ with the associated basis automorphisms $\underline{5}$ and $\underline{-1}$.

6. *p-Groups with only one Subgroup of Order p.*

A non-cyclic abelian group of exponent p^n contains at least two different subgroups of order p.

Proof: Let A be an element of order p^n and let B not be a power of A. Then the order p^ν of B mod (A) is greater than 1, but at most p^n. We have

$$B^{p^\nu} = A^r, \quad B^{p^n} = A^{r \cdot p^{n-\nu}} = e, \quad r = s \cdot p^\nu, \quad (B \cdot A^{-s})^{p^\nu} = e.$$

Therefore $(BA^{-s})^{p^{\nu-1}}$ and $A^{p^{n-1}}$ generate two different subgroups of order p.

We wish to find non-abelian groups of order p^n which contain only one subgroup of order p.

An example is the *quaternion group*. By the theorem of Hölder it is defined by the relations $A^4 = 1$, $BAB^{-1} = A^{-1}$, $B^2 = A^2$ as a group of order 8 with generators A and B. Its eight elements are called quaternions; they are

$$1, A, \quad A^2, \quad A^3$$
$$B, AB, A^2B, A^3B.$$

If instead we write

$$1, \mathrm{i}, -1, -\mathrm{i}$$
$$\mathrm{j}, \mathrm{k}, -\mathrm{j}, -\mathrm{k}$$

and set

$$-(-1)=1,\ -(-\mathfrak{i})=\mathfrak{i},\ -(-\mathfrak{j})=\mathfrak{j},\ -(-\mathfrak{k})=\mathfrak{k},$$

then we have the following calculational rules:

$$1\cdot x=x\cdot 1=x,\ -1\cdot x=x\cdot -1=-x,\ (-1)^2=1,$$
$$\mathfrak{i}^2=\mathfrak{j}^2=\mathfrak{k}^2=-1,\ \mathfrak{i}\mathfrak{j}=-\mathfrak{j}\mathfrak{i}=\mathfrak{k},\ \mathfrak{j}\mathfrak{k}=-\mathfrak{k}\mathfrak{j}=\mathfrak{i},$$
$$\mathfrak{k}\mathfrak{i}=-\mathfrak{i}\mathfrak{k}=\mathfrak{j}.$$

From this we conclude that there is only one subgroup of order 2 and exactly three subgroups of order 4. The center is equal to the commutator group which is equal to (—1).

The *generalized quaternion group* is defined by the relations

$$A^{2^{n-1}}=1,\ BAB^{-1}=A^{-1},\ B^2=A^{2^{n-2}} \qquad (n>2) \tag{8}$$

as a group generated by A, B, and of order 2^n, by the Hölder Theorem. Since

$$(BA^\nu)^2=BA^\nu B^{-1}\cdot B^2\cdot A^\nu=A^{-\nu}B^2A^\nu=B^2,$$

this group contains only one subgroup of order 2. The elements $A^{2^{n-3}}$ and B generate a quaternion group.

The relations above can be written more elegantly in the form

$$A^{2^{n-2}}=B^2=(AB)^2\ . \tag{9}$$

The new relations follow from those above.

From the new relations, however, it follows that

$$BAB^{-1}=A^{-1}(AB)^2B^{-2}=A^{-1}$$
$$BA^{2^{n-2}}B^{-1}=A^{-2^{n-2}}=BB^2B^{-1}=B^2=A^{2^{n-2}}$$
$$A^{2^{n-1}}=1,$$

and therefore the old relations follow.

If A' is of order 2^{n-1}, B' of order 4, and if A' and B' generate the whole group, then

$$A'^{2^{n-2}}=B'^2=(A'B')^2=A^{2^{n-2}}.$$

Therefore all the calculational rules which are valid for power products of A and B also remain valid for the corresponding power products of A' and B'.

Since A' and B' generate the whole group, (A') is a normal subgroup of index 2, and every element can be written uniquely in the form

$$A'^\nu B'^\mu\ (0\leqq\nu<2^{n-1},\ 0\leqq\mu<2).$$

Therefore the mapping $A^\nu B^\mu\to A'^\nu B'^\mu$ is an automorphism of the group. The number of all the automorphisms is equal to the number of pairs A', B'. It follows by simple enumeration that:

The quaternion group has exactly 24 *automorphisms. The generalized quaternion group of order* 2^n *has exactly* 2^{2n-2} *automorphisms for* $n > 3$.

In the automorphism group A of the quaternion group, the inner automorphisms form an abelian normal subgroup J of order 4. An automorphism which commutes with all the inner automorphisms is itself an inner automorphism. Since it changes each generator by a factor in the center, there are at most $2 \cdot 2$ such automorphisms.

A group A having order 24, and containing a normal subgroup J of order 4 which is its own centralizer, must be isomorphic to $\mathfrak{S}_4$.

This is because a central element of A must be in J, and an element of order 3 must transform the three elements $\neq e$ in J in a cyclic manner. Then, since according to the results of Sylow there are elements of order 3, the center is e, and there is no normal subgroup of order 3. From these results also, the index in A of the normalizer N_3 of a Sylow 3-group is 4. A transitive representation of A in 4 ciphers is associated with N_3. The representation is faithful since the intersection of all 3–normalizers contains only center elements with orders 1 or 2 and therefore is e. Since A consists of 24 elements, A is isomorphic to $\mathfrak{S}_4$.

The automorphism group of the quaternion group is isomorphic to the symmetric permutation group of four ciphers.

The quaternion group is the only p-group which contains two different cyclic subgroups of index p but only one subgroup of order p.

Proof:[1] Let $\mathfrak{G}$ be of order p^n and let it contain two different cyclic subgroups $\mathfrak{U}_1$ and $\mathfrak{U}_2$ of index p. $\mathfrak{U}_1$ and $\mathfrak{U}_2$ are different normal subgroups of index p, and therefore their intersection $\mathfrak{D}$ is of index p^2. Moreover $\mathfrak{D}$ is in the center and contains the commutator group. It follows for any two elements x, y that x^p and y^p are in $\mathfrak{D}$, and that

$$(y, x)^p = (y^p, x) = e, \quad (xy)^p = (y, x)^{\frac{1}{2}p(p-1)} x^p y^p.$$

If p is odd, then $(xy)^p = x^p y^p$, and therefore the operation of raising to power p is a homomorphy. Since the group of p-th powers is contained in $\mathfrak{D}$, by the first isomorphism theorem the elements whose p-th power is e form a subgroup whose order is at least p^2. There are at least two different subgroups of order p in this subgroup.

If $p = 2$, then $(xy)^4 = (y, x)^6 x^4 y^4 = x^4 y^4$. Now we conclude just as above that either $\mathfrak{D} = 1$ and $\mathfrak{U}_1$, $\mathfrak{U}_2$ are two different subgroups of order 2, or there are two subgroups $u_1 \neq u_2$ of order 4 by the first isomorphism theorem. We may assume that u_1 is in $\mathfrak{U}_1$. If u_1 is different from $\mathfrak{U}_1$, then u_1 is in $\mathfrak{D}$ and $u_1 \cdot u_2$ is an abelian group of order 8. Since it contains two different subgroups of index 2, it is not cyclic, and therefore it also contains two different subgroups of order 2. If, in conclusion, $u_1 = \mathfrak{U}_1$, then the whole group is of order 8. Let $\mathfrak{U}_1 = (A)$ and $\mathfrak{U}_2 = (B)$. If there is only one subgroup of order 2 then $B^2 = (AB)^2 = A^2$, and therefore the group is the quaternion group.

THEOREM 15: *A p-group which contains only one subgroup of order p is either cyclic or a generalized quaternion group.*

Proof: Let $\mathfrak{G}$ be of order p^n and let it contain only one subgroup of order p. First

[1] In accordance with a communication from Herr Maass, Hamburg.

let p be odd. If $n=0, 1$, then the theorem is clearly true. We now apply induction to n.

Every subgroup of index p is cyclic by the induction hypothesis, and therefore by what was proven previously there is only one subgroup of index p in $\mathfrak{G}$, and therefore $\mathfrak{G}$ itself is cyclic.[1]

Now let $p=2$ and let $\mathfrak{A}$ be a maximal abelian normal subgroup. $\mathfrak{A}$ is cyclic and its own centralizer. Therefore $\mathfrak{G}/\mathfrak{A}$ is isomorphic to a group of automorphisms of $\mathfrak{A}$. We shall show that only one automorphism of order 2 can occur, namely, the operation of a raising the elements of $\mathfrak{A}$ to the power -1. Since this automorphism is not the square of any other automorphism of $\mathfrak{A}$, it follows that $\mathfrak{G}:\mathfrak{A}$ is either 1 or 2. If we set $\mathfrak{A}=(A)$ and assume that $B \not\equiv e(\mathfrak{A})$, $B^2 \equiv e(\mathfrak{A})$, then as a preliminary BAB^{-1} must be shown to be equal to A^{-1}. In fact, we want to show further that the group generated by A and B is a generalized quaternion group with relations (8) and (9). Then the theorem will be proven.

Since B cannot commute with all the elements of A, $(B^2) \neq A$, and there is a subgroup $\mathfrak{A}_1$ of $\mathfrak{A}$ which contains (B^2) as a subgroup of index 2. The group $\mathfrak{A}_1(B)$ contains the two different cyclic subgroups $\mathfrak{A}_1$ and (B) of index 2; and therefore it is, as was previously shown, the quaternion group. If A is of order 2^m then: $B^2 = A^{2^{m-1}}$. We also conclude $(AB)^2 = A^{2^{m-1}}$. Therefore A and B generate the generalized quaternion group of order 2^{m+1}.

THEOREM 16: *A group of order p^n is cyclic if it contains only one subgroup of order p^m (where $1 < m < n$).*

Proof: There is a subgroup $\mathfrak{U}$ of order p^m. $\mathfrak{U}$ is contained in a subgroup $\mathfrak{U}_1$ of order p^{m+1} and is the only subgroup of index p in $\mathfrak{U}_1$. Therefore $\mathfrak{U}_1$ is cyclic and consequently $\mathfrak{U}$ is cyclic. Since every subgroup of order p or p^2 is contained in a subgroup of order p^m, and since the only subgroup of order p^m is cyclic, there is only one subgroup of order p and one of order p^2. Since the generalized quaternion group contains some subgroups of order 4, we conclude from the previous theorem that the whole group is cyclic.

If in a p-group, every subgroup of order p^2 is cyclic, then there is only one subgroup of order p, and conversely.

If there were two different subgroups of order p then we can assume that one of them is contained in the center. But then the product of the two subgroups is a non-cyclic group of order p^2. Conversely, in a non-cyclic group of order p^2 there are certainly two different subgroups of order p. Now one can easily prove:

THEOREM 17: *A group of order p^n in which every subgroup of order p^m is cyclic, where $1 < m < n$, is cyclic except in the case $p=2$, $m=2$ in which case the group can also be a generalized quaternion group.*

7. *p-Groups with a Cyclic Normal Subgroup of Index p.*

We shall determine all the p-groups which contain a cyclic normal subgroup of index p. This problem will now be solved for non-abelian p-groups, which contain some subgroups of order p. If $\mathfrak{G}$ is of order p^n, then in $\mathfrak{G}$ there is an element A

[1] This last by the basis theorem.

of order p^{n-1} and an element B of order p which is not a power of A. A and B generate $\mathfrak{G}$, and the subgroup (A) of index p is a normal subgroup. Therefore

$$A^{p^{n-1}} = B^p = 1, \qquad BAB^{-1} = A^r,$$
$$r \not\equiv 1\,(p^{n-1}), \qquad r^p \equiv 1\,(p^{n-1}).$$

If for odd p the element B is replaced by an appropriate power, then we can take $r = 1 + p^{n-2}$.

If $p = 2$, $n = 3$, then we must have $r \equiv -1\,(4)$. If $p=2$, $n>3$, then there are three possibilities for r,

$$r \equiv -1,\ 1 + 2^{n-2},\ -1 + 2^{n-2}\,(2^{n-1}).$$

The number r is not altered mod 2^{n-1} if B is replaced by BA^{4k}.

If $r \equiv 1 + 2^{n-2}$, then the commutator subgroup is of order 2; in the other two cases it is of order 2^{n-1}.

If $r \equiv -1$, then $(BA^\nu)^2 = (BA^\nu B^{-1})B^2A^\nu = A^{-\nu}B^2A^\nu = 1$, and therefore there is only one cyclic subgroup of index 2. Thus r is uniquely determined by the group. As a result we obtain:

The groups $\mathfrak{G}$ of order p^n which contain an element A of order p^{n-1}, are of the following types:

a) *$\mathfrak{G}$ abelian:*

$n \geqq 1$ I $\quad Z_{p^n}: B^{p^n} = 1$

$n \geqq 2$ II $\quad A^{p^{n-1}} = 1, \quad B^p = 1, \quad AB = BA;$

b) *$\mathfrak{G}$ non-abelian, p odd:*

$n \geqq 3$ III $\quad A^{p^{n-1}} = 1, \quad B^p = 1, \quad BAB^{-1} = A^{1+p^{n-2}};$

c) *$\mathfrak{G}$ non-abelian, $p = 2$:*

$n \geqq 3$ III *generalized quaternion group:*

$$A^{2^{n-1}} = 1, \quad B^2 = A^{2^{n-2}}, \quad BAB^{-1} = A^{-1}$$

$n \geqq 3$ IV *dihedral group D_{2^n}:*

$$A^{2^{n-1}} = 1, \quad B^2 = 1, \quad BAB^{-1} = A^{-1}$$

$n \geqq 4$ V $\quad A^{2^{n-1}} = 1, \quad B^2 = 1, \quad BAB^{-1} = A^{1+2^{n-2}},$

$n \geqq 4$ VI $\quad A^{2^{n-1}} = 1, \quad B^2 = 1, \quad BAB^{-1} = A^{-1+2^{n-2}}.$

Groups of different type are not isomorphic. From Hölder's theorem it follows that all types exist. For $n = 3$, V will coincide with IV, and VI with II.

Now it is simple to give all groups of order p^3. We must now investigate among such all those in which the p-th power of every element is e. A group in which all squares are equal to e is abelian since

$$x = x^{-1}, \text{ thus } xy = (xy)^{-1} = y^{-1}x^{-1} = yx.$$

If the group is non-abelian and p is odd, then it is generated by two elements

A and B such that the relations

$$A^p = B^p = (A, B)^p = 1, A(A, B) = (A, B)A, \quad B(A, B) = (A, B)B$$

hold. By III, Theorem 21, these relations define a non-abelian group with generators A, B and order p^3, in which, for any two elements x, y, we have:

$$(xy)^p = (x, y)^{-\frac{1}{2}p(p-1)} x^p y^p = x^p y^p.$$

Thus the p-th power of every element is equal to e. As a result we obtain:

There are, for every prime number p, five types of groups of order p^3, namely the three abelian types:

I. $Z_{p^3} : B^{p^3} = 1,$

II. $A^{p^2} = 1, \ B^p = 1, \ AB = BA,$

VII. $\cdot A^p = B^p = C^p = 1, \ AB = BA, \ AC = CA, \ BC = CB \quad ,$

and two non-abelian types, which are, for $p=2$: III, the quaternion group and IV, the dihedral group, and for odd p the types

III. $A^{p^2} = 1, \ B^p = 1, \ BAB^{-1} = A^{1+p},$

IV. $A^p = B^p = (A, B)^p = 1, \ A(A, B) = (A, B)A, \ B(A. B) = (A, B)B.$

Exercises

1. If a p-group contains a cyclic normal subgroup of index p, then every subgroup different from e has the same property.

2. For odd p, the following properties hold for abelian groups of type (p, p^{n-1}) and for non-abelian groups of order p^n having a cyclic subgroup of index p, where m is a number greater than zero and less than n:

a) The number of subgroups of order p^m is $1 + p$ in both cases.

b) The number of cyclic subgroups of order p^m is, in both cases, $1+p$ or p according to whether $m=1$ or $m>1$.

c) The number of elements whose p^m-th power$=e$ is p^{m+1} in both cases.

d) In both groups, every subgroup whose order is divisible by p^2 is a normal subgroup. Therefore for $m>1$ there are equally many normal subgroups of order p^m.

e) The number of automorphisms is $p^n(p\text{-}1)$.

3. The two types of non-abelian groups of order p^3 can be defined by the relations

III. $A^p = B^p = (A, B),$

IV. $A^p = B^p = (A, A, B) = (B, B, A) = 1$

for all p by an appropriate choice of generators A, B.

4. If a 2-group contains a cyclic subgroup of index 2 and is neither abelian of type (2, 2) nor the quaternion group, then the number of its automorphisms is a power of 2.

5. In a finite group, the index of the normalizer over the centralizer of a Sylow p-group with d generators is a divisor of k_d. If the order of the group is divisible neither by the third power of its smallest prime factor p, nor by 12, then every Sylow p-group is in the center of its normalizer.

6. In an abelian p-group $\mathfrak{G}$ with the exponent p^m, the characteristic chains

$$\mathfrak{G} > \mathfrak{G}^p > \mathfrak{G}^{p^2} > \cdots > \mathfrak{G}^{p^m} = e$$

and

$$\mathfrak{G} = \mathfrak{G}_{p^m} > \mathfrak{G}_{p^{m-1}} > \cdots > \mathfrak{G}_p > e$$

give rise to a characteristic series through the refinement process which was given in the proof of the Jordan-Hölder-Schreier Theorem. There is only this one characteristic series. (Here $\mathfrak{G}^{p^\nu}$ denotes the group of the p^ν-th powers and $\mathfrak{G}_{p^\nu}$ denotes the group of all elements whose p^ν-th power is e.)

7. Theorem 2 in § 1 admits the following corollaries: If $\mathfrak{P}$ is a Sylow p-group in $\mathfrak{G}$, $N_\mathfrak{P}$ its normalizer, $\mathfrak{N}$ a normal subgroup of $\mathfrak{G}$, then

a) $N_\mathfrak{P}\mathfrak{N}/\mathfrak{N}$ is the normalizer of the Sylow p-group $\mathfrak{P}\mathfrak{N}/\mathfrak{N}$ of $\mathfrak{G}/\mathfrak{N}$,

b) $N_\mathfrak{P}$ is contained in the normalizer $N_\mathfrak{p}$ of the Sylow p-group $\mathfrak{p} = \mathfrak{P} \cap \mathfrak{N}$ of $\mathfrak{N}$,

c) $N_\mathfrak{p}\mathfrak{N} = \mathfrak{G}$, therefore by the Second Isomorphism Theorem

$$N_\mathfrak{p}/N_\mathfrak{p} \cap \mathfrak{N} \simeq \mathfrak{G}/\mathfrak{N}.$$

(Hint for a): If $x\mathfrak{P}\mathfrak{N}x^{-1} = \mathfrak{P}\mathfrak{N}$, then by Theorem 3: $x\mathfrak{P}x^{-1} = v\mathfrak{P}v^{-1}$ is solvable for v in $\mathfrak{N}$; therefore $v^{-1}x \in N_\mathfrak{P}$; (for c): for every x in $\mathfrak{G}$, $x\mathfrak{p}x^{-1} = v\mathfrak{p}v^{-1}$ is solvable for v in $\mathfrak{N}$.)

With the help of c) it should be shown that the Φ-subgroup of a finite group is nilpotent.

§ 4. On the Enumeration Theorems of the Theory of p-Groups

In the study of finite groups the question arises naturally as to the number of elements or subgroups with some given property. The results obtained in connection with this question do not lie very deep.

The following systematic derivation of the enumeration theorems in p-groups is due to P. Hall.

THEOREM 18 (Counting Principle): Let $\mathfrak{G}$ be a finite p-group. $\mathfrak{M}_\alpha$ denotes any subgroup of index p^α, which contains $\Phi(\mathfrak{G})$. Let $(\mathfrak{K})$ be a set of complexes such that each complex $\mathfrak{K}$ in $(\mathfrak{K})$ is contained in at least one subgroup of index p. Let $n(\mathfrak{M}_\alpha)$ be the number of complexes of $(\mathfrak{K})$ which are contained in $\mathfrak{M}_\alpha$. Then

$$n(\mathfrak{M}_0) - \sum_{(\mathfrak{M}_1)} n(\mathfrak{M}_1) + p \sum_{(\mathfrak{M}_2)} n(\mathfrak{M}_2) - p^3 \sum_{(\mathfrak{M}_3)} n(\mathfrak{M}_3) + \cdots$$
$$+ (-1)^\alpha p^{\frac{1}{2}\alpha(\alpha-1)} \sum_{(\mathfrak{M}_\alpha)} n(\mathfrak{M}_\alpha) + \cdots + (-1)^d p^{\frac{1}{2}d(d-1)} n(\mathfrak{M}_d) = 0,$$

where the summation, $\sum_{(\mathfrak{M}_\alpha)}$, is extended over the $\varphi_{d,\alpha}$ subgroups $\mathfrak{M}_\alpha$ of $\mathfrak{G}$.

Proof: We shall show that the number of times that an element $\mathfrak{K}$

in $(\mathfrak{K})$ is "counted" with the appropriate sign on the left of the equation above is equal to zero.

The intersection of all $\mathfrak{M}_\alpha$ which contain $\mathfrak{K}$, contains $\Phi(\mathfrak{G})$, and therefore is an $\mathfrak{M}_\varrho$. By hypothesis $\mathfrak{K}$ is contained in an $\mathfrak{M}_1$ and therefore $\varrho > 0$. The number of all $\mathfrak{M}_\alpha$'s which contain $\mathfrak{K}$ is equal to the number of all $\mathfrak{M}_\alpha$'s which contain $\mathfrak{M}_\varrho$, i.e., $\varphi_{\varrho,\alpha}$. Therefore the number of times that $\mathfrak{K}$ is "counted" is

$$1 - \varphi_{\varrho,1} + p\,\varphi_{\varrho,2} - p^3\,\varphi_{\varrho,3} + \cdots + (-1)^\alpha\, p^{\frac{1}{2}\alpha(\alpha-1)}\,\varphi_{\varrho,\alpha} + \cdots + (-1)^\varrho\, p^{\frac{1}{2}\varrho(\varrho-1)}.$$

But this number is zero, by § 3, Formula 5, Q.E.D.

THEOREM 19: *The number of subgroups of fixed order p^m $(0 \leq m \leq n)$ of a p-group $\mathfrak{G}$ of order p^n leaves 1 as a remainder when divided by p.*

Proof: If $n = 0$, then the theorem is clear. Now let $n > 0$ and assume that the theorem is proven for p-groups whose order is less than p^n. If $m = n$ then the theorem is trivial. Let $m < n$. For Theorem 19, let $(\mathfrak{K})$ denote the set of all subgroups of $\mathfrak{G}$ of order p^m. Then:

$$n(\mathfrak{M}_0) \equiv \sum_{\mathfrak{M}_1} n(\mathfrak{M}_1)\,(p),$$

and by the induction hypothesis

$$n(\mathfrak{M}_1) \equiv 1\,(p);$$

moreover the number of all $\mathfrak{M}_1$ is $\varphi_{d,\,d-1}$, and therefore by § 3 congruent to 1 mod p, so that

$$n(\mathfrak{M}_0) \equiv 1\,(p)$$

follows, Q.E.D.

THEOREM 20 (Kulakoff): *In a non-cyclic p-group of odd order p^n, the number of subgroups of order p^m $(0 < m < n)$ is congruent to $1 + p$ modulo p^2.*

In the non-cyclic group of order p^2 there are $p + 1$ subgroups of order p. We apply induction on n and assume $n > 2$.

The number of all $\mathfrak{M}_1$ is $\varphi_{d,\,d-1}$, and therefore, since $d > 1$, is congruent to $1+p$ mod p^2. Let $m < n$-1, $(\mathfrak{K})$ be the set of all subgroups of order p^m. By the Counting Principle it follows that

$$n(\mathfrak{M}_0) \equiv \sum_{\mathfrak{M}_1} n(\mathfrak{M}_1) - p \sum n(\mathfrak{M}_2).$$

By Theorem 19

$$n(\mathfrak{M}_2) \equiv 1 \,(p)$$

and by § 3, 2., the number of all $\mathfrak{M}_2$ (namely $\varphi_{d,\,d-2}$) is congruent to 1 mod p. Consequently

$$n(\mathfrak{M}_0) \equiv \sum_{\mathfrak{M}_1} n(\mathfrak{M}_1) - p\,(p^2).$$

For the non-cyclic $\mathfrak{M}_1$, $n(\mathfrak{M}_1) \equiv 1 + p\,(p^2)$ by the induction hypothesis. As was shown, the number of all $\mathfrak{M}_1$ is congruent to $1 + p\ (p^2)$. If there is no cyclic subgroup of index p in $\mathfrak{G}$, then

$$\sum_{\mathfrak{M}_1} n(\mathfrak{M}_1) \equiv (1+p)^2 - p \,(\mathrm{mod}\, p) \equiv 1 + p \,(\mathrm{mod}\, p^2).$$

If $\mathfrak{G}$ contains a cyclic subgroup of index p, then the theorem follows from the solution of Exercise 2a at the end of § 3.

THEOREM 21 (Miller): *In a non-cyclic group of odd order p^n, the number of cyclic subgroups of order p^m $(1 < m < n)$ is divisible by p.*

Proof: If $\mathfrak{G}$ contains a cyclic subgroup of index p, then the theorem follows from the solution of Exercise 2b at the end of § 3. To continue, let every subgroup of index p in $\mathfrak{G}$ be non-cyclic, $m < n$-1 and assume the proof has been carried out already for smaller n. Let $(\mathfrak{K})$ be the set of cyclic subgroups of order p^m. We find the congruence:

$$n(\mathfrak{M}_0) \equiv \sum_{\mathfrak{M}_1} n(\mathfrak{M}_1)\,(p).$$

By the induction hypothesis each of the numbers $n(\mathfrak{M}_1)$ is divisible by p, and therefore the desired number $n(\mathfrak{M}_0)$ is also.

THEOREM 22 (Hall): *The number of subgroups of index p^α in $\mathfrak{G}$ $(0 \leqq \alpha \leqq d)$ is congruent to $\varphi_{d,\,\alpha} (\mathrm{mod} p^{d-\alpha+1})$. The number of those subgroups which do not contain $\Phi(\mathfrak{G})$ is consequently divisible by $p^{d-\alpha+1}$.*

Proof: If $d = n$, then the number in question is already known to be $\varphi_{d,\,\alpha}$. Let $n > 1$ and let the theorem be proved for smaller n. If $\alpha = 0$, then the theorem is clearly true. Let $\alpha > 0$, then $n(\mathfrak{M}_\beta)$ is equal to the number of all subgroups of index $p^{\alpha-\beta}$ in $\mathfrak{M}_\beta$. Therefore $n(\mathfrak{M}_\beta) = 0$ if $\beta > \alpha$; but otherwise by the induction hypothesis

$$n(\mathfrak{M}_\beta) \equiv \varphi_{d(\mathfrak{M}_\beta),\,\alpha-\beta}\,(p^{d(\mathfrak{M}_\beta)-(\alpha-\beta)+1}).$$

Since $d(\mathfrak{M}_\beta) \geqq d - \beta$ and therefore by § 3

$$\varphi_{d(\mathfrak{M}_\beta),\,\alpha-\beta} \equiv \varphi_{d-\beta,\,\alpha-\beta}\,(p^{(d-\beta)-(\alpha-\beta)+1}),$$

we have

$$n(\mathfrak{M}_\beta) \equiv \varphi_{d-\beta,\,\alpha-\beta}\,(p^{d-\alpha+1}).$$

The Counting Principle now gives the congruence

$$n(\mathfrak{M}_0) \equiv \varphi_{d,1}\varphi_{d-1,\alpha-1} - p\,\varphi_{d,2}\varphi_{d-2,\alpha-2} + \cdots + (-1)^{\alpha-1} p^{\frac{1}{2}\alpha(\alpha-1)} \varphi_{d,\alpha}\varphi_{d-\alpha,0}(p^{d-\alpha+1}).$$

But by the Counting Principle, the right side of the congruence is exactly the number of subgroups of index p^α in an elementary abelian group of order p^d, so that

$$n(\mathfrak{M}_0) \equiv \varphi_{d,\alpha}(p^{d-\alpha+1}) \quad , \qquad \text{Q.E.D.}$$

Exercise (Kulakoff): In a non-cyclic p-group of odd order p^n, the number of solutions of $x^{p^m} = e\,(0 < m < n)$ is divisible by p^{m+1}.

Exercise: The number of normal subgroups of order p^m in a group of order $p^n\,(0 < m < n)$ is congruent to 1 (mod p).

If p is odd, $1 < m$, and $\mathfrak{G}$ is non-cyclic then, more precisely, the number is congruent to $1 + p \pmod{p^2}$.

§ 5. On the Descending Central Series

P. Hall has generalized the concept of a terminating ascending central series by defining:

A chain of normal subgroups of $\mathfrak{G}$

$$\mathfrak{G} = \mathfrak{N}_1 \geqq \mathfrak{N}_2 \geqq \mathfrak{N}_3 \geqq \cdots \geqq \mathfrak{N}_{r+1} = e \tag{1}$$

is called a *central chain* if $\mathfrak{N}_i/\mathfrak{N}_{i+1}$ is contained in the center of $\mathfrak{G}/\mathfrak{N}_{i+1}$ $(i = 1, 2, \ldots, r)$.

If the ascending central series (See II § 4, 3.) terminates, then it is a central chain. The following definition is still more useful: A chain of subgroups

$$\mathfrak{G} = \mathfrak{N}_1 \geqq \mathfrak{N}_2 \geqq \cdots \geqq \mathfrak{N}_{r+1} = e$$

is said to be a central chain if the mutual commutator group $(\mathfrak{G}, \mathfrak{N}_i)$ is contained in $\mathfrak{N}_{i+1}$ $(i = 1, \ldots, r)$. Since for every x_i in $\mathfrak{N}_i$, x in $\mathfrak{G}$: $x x_i x^{-1} x_i^{-1} \equiv e(\mathfrak{N}_{i+1})$, and thus certainly $x x_i x^{-1} \in \mathfrak{N}_i$, it follows that $\mathfrak{N}_i$ is a normal subgroup of $\mathfrak{G}$ and that $\mathfrak{N}_i/\mathfrak{N}_{i+1}$ is contained in the center of $\mathfrak{G}/\mathfrak{N}_{i+1}$. The converse is clear. $\mathfrak{N}_{r+1}$ is contained in $\mathfrak{z}_0$; if it has already been shown that $\mathfrak{N}_{r+1-i}$ is in $\mathfrak{z}_i$ where $i < r$, then

$$(\mathfrak{G}, \mathfrak{N}_{r-i}) \leqq \mathfrak{N}_{r+1-i} \leqq \mathfrak{z}_i,$$

and therefore $\mathfrak{N}_{r-i} \leqq \mathfrak{z}_{i+1}$. Hence in

$$\mathfrak{N}_{r+1-i} \leqq \mathfrak{z}_i \qquad (i = 0, 1, 2, \ldots, r). \tag{2}$$

Consequently $\mathfrak{z}_r = \mathfrak{G}$.

If a group has a central chain, then it is nilpotent and the length of every central chain is at least equal to the class of the group.

Now it is natural to define the *descending central series* for an arbitrary group $\mathfrak{G}$ as $\mathfrak{Z}_1 \geqq \mathfrak{Z}_2 \geqq \mathfrak{Z}_3, \ldots,$ where $\mathfrak{Z}_1(\mathfrak{G}) = \mathfrak{Z}_1 = \mathfrak{G}$,

$$\mathfrak{Z}_2(\mathfrak{G}) = \mathfrak{Z}_2 = (\mathfrak{G}, \mathfrak{G}) = \mathfrak{G}', \ldots, \mathfrak{Z}_{n+1}(\mathfrak{G}) = \mathfrak{Z}_{n+1} = (\mathfrak{G}, \mathfrak{Z}_n) \quad \ldots$$

If $\mathfrak{G}$ has a central chain (1) then it follows by induction that: $\mathfrak{Z}_1 \leqq \mathfrak{N}_1$, $\mathfrak{Z}_2 \leqq \mathfrak{N}_2, \ldots, \mathfrak{Z}_{r+1} \leqq \mathfrak{N}_{r+1}$, and therefore $\mathfrak{Z}_{r+1} = e$. If, conversely, the descending central series is equal to e from the $(r+1)$-th place on, then $\mathfrak{G} = \mathfrak{Z}_1 \geqq \mathfrak{Z}_2 \geqq \cdots \geqq \mathfrak{Z}_{r+1} = e$ is a central chain. If c is the class of $\mathfrak{G}$, then $r \geqq c$, $\mathfrak{Z}_i \leqq \mathfrak{z}_{c+1-i}$, and therefore $\mathfrak{Z}_c \neq e$, $\mathfrak{Z}_{c+1} = e$.

In a nilpotent group, the class c can be found from the relation:

$$\mathfrak{G} = \mathfrak{Z}_1 > \mathfrak{Z}_2 > \cdots > \mathfrak{Z}_{c+1} = e \tag{3}$$

By Chapter II, § 6, $\mathfrak{Z}_i$ is a commutator form of $\mathfrak{G}$ of weight[1] i and of degree 1 and is generated by the higher commutators $(G_1, G_2, \ldots, G_i)$ where $G_j \in \mathfrak{G}$. Therefore $\mathfrak{Z}_i$ is a fully invariant subgroup of $\mathfrak{G}$.

For every subgroup $\mathfrak{U}$ of $\mathfrak{G}$ it follows that

$$\mathfrak{Z}_i(\mathfrak{U}) \leqq \mathfrak{Z}_i(\mathfrak{G}).$$

If $\mathfrak{N}$ is a normal subgroup of $\mathfrak{G}$, then

$$\mathfrak{Z}_i(\mathfrak{G}/\mathfrak{N}) = \mathfrak{Z}_i(\mathfrak{G})\mathfrak{N}/\mathfrak{N}.$$

It follows from this that:

Every subgroup and every factor group of a nilpotent group is itself nilpotent, and the class of the subgroup or factor group is at most equal to the class of the whole group.

We wish to state something about the positional relationships, and the mutual commutator groups, of members of the descending central series and of an arbitrary central chain.

If $\mathfrak{N}_1 \geqq \mathfrak{N}_2 \geqq \mathfrak{N}_3 \ldots$ is a sequence of subgroups of an arbitrary group $\mathfrak{G}$, so that $(\mathfrak{G}, \mathfrak{N}_j) \leqq \mathfrak{N}_{j+1}$ $(j = 1, 2, \ldots)$, it follows immediately that $\mathfrak{N}_i$ is a normal subgroup of $\mathfrak{G}$. If moreover $\mathfrak{Z}_i \leqq \mathfrak{N}_j$, then it follows by induction that $\mathfrak{Z}_{i+k} \leqq \mathfrak{N}_{j+k}$ $(k = 0, 1, 2, \ldots)$. In nilpotent groups of class c we can conclude from this that:

(4) $\mathfrak{Z}_i$ is not contained in $\mathfrak{z}_{c-i}$ (since otherwise we would have $\mathfrak{Z}_c = e$).

[1] $\mathfrak{Z}_i$ is also called the i-th *Reidemeister commutator group.*

Now we claim that in the general case

$$(\mathfrak{Z}_i, \mathfrak{N}_j) \leqq \mathfrak{N}_{i+j}. \tag{5}$$

We carry out the proof by induction on i. By hypothesis

$$(\mathfrak{Z}_1, \mathfrak{N}_j) = (\mathfrak{G}, \mathfrak{N}_j) \leqq \mathfrak{N}_{j+1}.$$

Let $i > 1$ and assume we have already proven that $(\mathfrak{Z}_{i-1}, \mathfrak{N}_k) \leqq \mathfrak{N}_{i+k-1}$ for all k.

Then by II. Theorem 14:

$$\begin{aligned}(\mathfrak{Z}_i, \mathfrak{N}_j) = (\mathfrak{N}_j, \mathfrak{Z}_i) &= (\mathfrak{N}_j, (\mathfrak{G}, \mathfrak{Z}_{i-1})) \\ &= (\mathfrak{N}_j, \mathfrak{G}, \mathfrak{Z}_{i-1}) \leqq (\mathfrak{G}, \mathfrak{Z}_{i-1}, \mathfrak{N}_j) \cdot (\mathfrak{Z}_{i-1}, \mathfrak{N}_j, \mathfrak{G})\end{aligned}$$

and by the induction hypothesis:

$$(\mathfrak{G}, \mathfrak{Z}_{i-1}, \mathfrak{N}_j) = (\mathfrak{G}, (\mathfrak{Z}_{i-1}, \mathfrak{N}_j)) \leqq (\mathfrak{G}, \mathfrak{N}_{i+j-1}) \leqq \mathfrak{N}_{i+j}$$

$$(\mathfrak{Z}_{i-1}, \mathfrak{N}_j, \mathfrak{G}) = (\mathfrak{Z}_{i-1}, (\mathfrak{G}, \mathfrak{N}_j)) \leqq (\mathfrak{Z}_{i-1}, \mathfrak{N}_{j+1}) \leqq \mathfrak{N}_{i+j}.$$

Therefore $(\mathfrak{Z}_i, \mathfrak{N}_j) \leqq \mathfrak{N}_{i+j}$.

If we set

$$\mathfrak{N}_1 = \mathfrak{Z}_1, \ \mathfrak{N}_2 = \mathfrak{Z}_2, \ldots, \mathfrak{N}_j = \mathfrak{Z}_j, \ldots$$

then

$$(\mathfrak{Z}_i, \mathfrak{Z}_j) \leqq \mathfrak{Z}_{i+j}. \tag{6}$$

We can now show by induction on the weight that:

An arbitrary commutator form $f(\mathfrak{G})$ of weight w is contained in $\mathfrak{Z}_w$.

This is true if $w = 1$. Now let $w > 1$, and assume that the statement is already known to be true for commutator forms with weight less than w. We have $f(\mathfrak{G}) = (f_1(\mathfrak{G}), f_2(\mathfrak{G}))$ where the f_i are commutator forms of weight w_i such that $w = w_1 + w_2$. By the induction hypothesis it follows that $f_1(\mathfrak{G}) \leqq \mathfrak{Z}_{w_1}$, $f_2(\mathfrak{G}) \leqq \mathfrak{Z}_{w_2}$, thus

$$f(\mathfrak{G}) \leqq (\mathfrak{Z}_{w_1}, \mathfrak{Z}_{w_2}) \leqq \mathfrak{Z}_{w_1+w_2} = \mathfrak{Z}_w.$$

In particular it follows that

$$\mathfrak{Z}_i(\mathfrak{Z}_k(\mathfrak{G})) \leqq \mathfrak{Z}_{ik}(\mathfrak{G}). \tag{7}$$

$$D^k\mathfrak{G} \leqq \mathfrak{Z}_{2k}(\mathfrak{G}). \tag{8}$$

A nilpotent group of class c is always k-step metabelian, where k satisfies the inequality

$$2^{k-1} \leqq c \tag{9}$$

Moreover if we set $\mathfrak{z}_{-1} = \mathfrak{z}_{-2} = \cdots = e$, then in general

$$(\mathfrak{Z}_i, \mathfrak{z}_j) \leqq \mathfrak{z}_{j-i}. \tag{10}$$

In particular, $\mathfrak{Z}_i$ commutes with $\mathfrak{z}_i$ elementwise.

THEOREM 23 (Hall): *If the non-abelian normal subgroup $\mathfrak{N}$ of the p-group $\mathfrak{G}$ is contained in $\mathfrak{Z}_i$, then its center is of order at least p^i, $\mathfrak{N}$ itself is at least of order p^{i+2}, its factor commutator group is at least of order p^{i+1}.*

Proof: Since $\mathfrak{z}_i$ commutes with $\mathfrak{Z}_i$ elementwise, $\mathfrak{N}$ is not contained in $\mathfrak{z}_i$. $\mathfrak{N} \cap \mathfrak{z}_i$ is in the center of $\mathfrak{N}$ and, by Theorem 14, is at least of order p^i, so that *a fortiori* the center of $\mathfrak{N}$ is of order divisible by p^i. Since $p^2 / \mathfrak{N} : \mathfrak{z}(\mathfrak{N})$, the order of $\mathfrak{N}$ is divisible by p^{i+2}. Since $\mathfrak{N}$ is not abelian, we can find in the normal subgroup $\mathfrak{N}'$ of $\mathfrak{G}$ a normal subgroup $\mathfrak{N}_1$ of $\mathfrak{G}$ with $\mathfrak{N}_1$ of index p under $\mathfrak{N}'$. $\mathfrak{N}/\mathfrak{N}_1$ is a non-abelian normal subgroup of $\mathfrak{G}/\mathfrak{N}_1$ and so we conclude as above that $\mathfrak{N} : \mathfrak{N}_1$ is divisible by p^{i+2}. Consequently $\mathfrak{N}/\mathfrak{N}'$ has an order divisible by p^{i+1}, Q.E.D.

Now if in a p-group of order p^n, $D^i \mathfrak{G} > D^{i+1} \mathfrak{G} > e$, then $D^i \mathfrak{G} \leqq \mathfrak{Z}_{2^i}$ and therefore as was just shown, $D^i \mathfrak{G} : D^{i+1} \mathfrak{G} \geqq p^{2^i+1}$. If $\mathfrak{G}$ is now $(k+1)$-step metabelian, then

$$n \geqq 1 + \sum_0^{k-1} (2^i + 1) = 2^k + k.$$

The order of a $(k+1)$-step metabelian p-group is divisible by p^{2^k+k}.

Remark: Under the hypothesis of Theorem 23 it can be shown by the same methods that the factor groups of the ascending and descending central series of the normal subgroup $\mathfrak{N}$ have an order divisible by p^i, with the possible exception of the last factors different from 1. The proof is left to the reader.

Exercises

1. In a finite group $\mathfrak{G}$ the intersection of all the normal subgroups whose factor group is an abelian p-group is called the *p-commutator group* of $\mathfrak{G}$ and is denoted by $\mathfrak{G}'(p)$.

Prove: The *p-factor commutator group* $\mathfrak{G}/\mathfrak{G}'(p)$ is an abelian p-group. Moreover, the commutator group of $\mathfrak{G}$ is the intersection of the p-commutator groups, and the factor commutator group is isomorphic to the direct product of the p-factor commutator groups. Moreover, $\mathfrak{G}/\mathfrak{G}'(p) \simeq S_p / S_p \cap \mathfrak{G}'$.

2. For an arbitrary group $\mathfrak{G}$, the class may be defined by the following property: Let the class be equal to c, if $\mathfrak{Z}_{c+1}$ is a proper subgroup $\mathfrak{Z}_c$ and $\mathfrak{Z}_{c+1} = \mathfrak{Z}_{c+2} = \cdots$ Let the class be equal to zero, if the group coincides with its commutator group.[1] Let the class be infinite if $\mathfrak{Z}_{i+1}$ is a proper subgroup of $\mathfrak{Z}_i$ for all i.

For nilpotent groups the two definitions of class coincide.

Prove: If the class c is finite then $\mathfrak{Z}_{c+1}$ is the intersection of all normal subgroups with nilpotent factor group, and the factor group $\mathfrak{G}/\mathfrak{Z}_{c+1}$ is also nilpotent. Hence we shall call the factor group $\mathfrak{G}/\mathfrak{Z}_{c+1}$ the *maximal nilpotent factor group*. Its class is c. The class of every factor group is at most c.

If the class is infinite, then there are factor groups of any given class.

3. In finite groups of class c we can obtain $\mathfrak{Z}_{c+1}$ in the following way:

For every prime number p we form the intersection $\mathfrak{D}_p(\mathfrak{G})$ of all normal subgroups of p-power index.

Prove: $\mathfrak{D}_p$ itself is of p-power index. Hence we shall call the factor group $\mathfrak{G}/\mathfrak{D}_p$ the *maximal p-factor group* of $\mathfrak{G}$.

Prove: $\mathfrak{Z}_{c+1}$ is the intersection of all $\mathfrak{D}_p$, and the maximal nilpotent factor group is isomorphic to the direct product of the maximal p-factor groups over all prime divisors of the group order.

4. If p^a is divisible by the exponent of the maximal p-factor group of the finite group $\mathfrak{G}$ (see Exercise 3), then the subgroup generated by all p^a-th powers is equal to $\mathfrak{D}_p$. Therefore $\mathfrak{D}_p$ is a fully invariant subgroup of $\mathfrak{G}$. Moreover, prove that

$$\mathfrak{D}_p(\mathfrak{D}_p(\mathfrak{G})) = \mathfrak{D}_p(\mathfrak{G}).$$

5. a) An abelian group with a finite number of generators is finite if and only if the factor group over its Φ-subgroup is finite.

b) A nilpotent group with a finite number of generators is finite if and only if the factor group over its Φ-subgroup is finite. [Use a) and apply induction to the length of the descending central series!]

6. In a nilpotent group all the elements of finite order form a fully invariant subgroup. (Use Exercise 5.)

7. a) (Hilton.) In a nilpotent group any two elements with relatively prime orders commute.

(*Hint*: Show that the commutator of the two elements is in members of the descending central series with arbitrarily great subscript.)

b) Two elements with p-power order generate a p-group.

c) Prove the following generalization of Theorem 11: A nilpotent group in which every element is of finite order is the direct product of nilpotent groups in which every element is of prime power order.

§ 6. Hamiltonian Groups

In an abelian group every subgroup is a normal subgroup. What other groups also have this property?

DEFINITION: A non-abelian group in which every subgroup is a

[1] These groups are also said to be *perfect groups*.

normal subgroup is said to be a *Hamiltonian group*. For example, the quaternion group is a Hamiltonian group.

THEOREM: *A Hamiltonian group is the direct product of a quaternion group with an abelian group in which every element is of odd order and an abelian group of exponent* 2, *and conversely.*

Proof: In a Hamiltonian group $\mathfrak{H}$ there are two elements A, B which do not commute with each other. Since (A) and (B) are normal subgroups of $\mathfrak{H}$, the commutator $C = (A, B) = ABA^{-1}B^{-1}$ of A and B is contained in the intersection of (A) and (B), and therefore in the center of the subgroup $\mathfrak{Q} = \{A, B\}$ generated by A and B.

The commutator group $\mathfrak{Q}'$ of $\mathfrak{Q}$ is generated by C and is a proper subgroup of (A) and likewise of (B). Since $(C) \neq e$, $C = A^r = B^s$ where $r, s \neq 0$. By Chapter II § 6, $(A, B)^s = (A, B^s)$, and therefore $C^s = e$. Consequently A and B have finite orders m and n respectively. We choose A and B so that m and n are minimal. Then it follows for a prime divisor p of m that

$$(A^p, B) = e \text{ and therefore } C^p = (A, B)^p = (A^p, B) = e.$$

Similarly it follows for a prime divisor p of n that $C^p = e$. The orders of A, B are consequently powers of the same natural prime p; they are divisible by p^2 since (C) is a proper subgroup of both (A) and (B), while A^p, B^p are contained in the center of $\mathfrak{Q}$.

If, say $A^{p^a} = C^\nu$, $B^{p^b} = C^\mu$, where ν, μ are not divisible by p, then we replace A by A^μ, B by B^ν, and we may assume that

$$A^{p^a} = B^{p^b} = (A, B) = C \neq e.$$

where $a \geqq b > 0$.

By chapter II § 6, in $\mathfrak{Q}$ we have the relation

$$(xy)^p = (x, y)^{-\frac{1}{2}p(p-1)} x^p y^p.$$

Now A, $A^{-p^{a-b}}B$ also generate $\mathfrak{Q}$, and therefore $B_1 = A^{-p^{a-b}}B$ must be of order at least equal to that of B. From this we conclude:

$$B_1^p = C^{p^{a-b+1} \cdot \frac{p-1}{2}} A^{-p^{a-b+1}} B^p,$$

$$B_1^{p^b} = C^{p^a \cdot \frac{p-1}{2}},$$

$$p = 2, \qquad a = b = 1.$$

Therefore $\mathfrak{Q}$ is a quaternion group with the relations $A^2 = B^2 = ABA^{-1}B^{-1} = C, C^2 = e$.[1]

[1] Instead of this process one can apply Theorem 15 of § 3 to the group $\mathfrak{Q}$!

We wish to show that $\mathfrak{H}$ is generated by $\mathfrak{Q}$ and the group $\mathfrak{V}$ of all elements of $\mathfrak{H}$ which commute with every element of $\mathfrak{Q}$.

If the element X does not commute with A, then $XAX^{-1} = A^{-1}$ and therefore BX commutes with A. If, now , BX does not commute with B, then ABX commutes with B. Consequently $\mathfrak{H} = \mathfrak{Q}\mathfrak{V}$.

Every element X in $\mathfrak{V}$ is of finite order, since BX does not commute with A, and therefore BX is of finite order. But B is of order 4 and commutes with X, therefore X is of finite order. Now, if $X^4 = e, X \in \mathfrak{V}$, then $(A, BX) \neq e$, $(A, BX) = A^2 = B^2$. Since $(BX)^4 = e$, we have $(A, BX) = (BX)^2 = B^2X^2$ and therefore $X^2 = e$.

In $\mathfrak{V}$ there is no element of order 4 and thus certainly no quaternion group. But since every subgroup in $\mathfrak{V}$ is a normal subgroup, $\mathfrak{V}$ is abelian. $\mathfrak{V}$ is the direct product of the subgroup $\mathfrak{U}$ of all elements of odd order, and the subgroup $\mathfrak{G}_1$ of all elements whose square is e. C is contained in $\mathfrak{G}_1$. Among all the subgroups of $\mathfrak{G}_1$ which do not contain C there is a largest, $\mathfrak{G}$. For every element X in $\mathfrak{G}_1$ not contained in $\mathfrak{G}$, C must be contained in $\{\mathfrak{G}, X\}$. Since $X^2 = e$, we have $\{\mathfrak{G}, X\} : \mathfrak{G} = 2$ and likewise $\{\mathfrak{G}, C\} : \mathfrak{G} = 2$, and therefore $\{\mathfrak{G}, X\} = \{\mathfrak{G}, C\}$; it follows that $\{\mathfrak{G}, C\} = \mathfrak{G}_1$ and moreover $\mathfrak{G} \cap (C) = e$; therefore

$$\mathfrak{V} = \mathfrak{U} \times \mathfrak{G} \times (C).$$

Since $\mathfrak{Q} \cap \mathfrak{V} = (C)$, we have $\mathfrak{Q} \cap (\mathfrak{U} \times \mathfrak{G}) = e$, and moreover $\mathfrak{Q} \cdot (\mathfrak{U} \times \mathfrak{G}) = \mathfrak{H}$; therefore $\mathfrak{H} = \mathfrak{Q} \times \mathfrak{U} \times \mathfrak{G}$.

Conversely a group with this structure is Hamiltonian. For $\mathfrak{Q}$ is not abelian. We have yet to show that every cyclic subgroup (QUG) is a normal subgroup. Since $\mathfrak{Q}$ is the only non-abelian factor of the decomposition we only need show that the transform of QUG by A or B is in (QUG).

Now $A(QUG)A^{-1} = Q^iUG$ where i is either 1 or 3. The order of U is an odd number d. Therefore the congruences $r \equiv i\,(4)$, $r \equiv 1\,(d)$ can be solved, and $G^r = G$, $AQUGA^{-1} = (QUG)^r$, Q.E.D.

§ 7. Applications of Extension Theory

Let $\mathfrak{G}$ be an extension of the normal subgroup $\mathfrak{N}$ with the factor group $\mathfrak{F}$.

We say a factor system $(C_{\sigma,\tau})$ is an *abelian factor system* if all the $C_{\sigma,\tau}$ commute with each other.

THEOREM 24: *The* $(\mathfrak{F}:1)$*-th power of an abelian factor system is a retracting*[1] *factor system.*

[1] See end of § 6, Chapter III.

Proof: Let $(\mathfrak{F}:1) = n > 0$. We set $a_\sigma = \prod_\varrho C_{\sigma,\varrho}$ and form the product over ϱ of all the equations $C_{\sigma,\tau} C_{\sigma\tau,\varrho} = C^{\sigma}_{\tau,\varrho} C_{\sigma,\tau\varrho}$.

Then it follows that $C^n_{\sigma,\tau} = a^\sigma_\tau a_\sigma a^{-1}_{\sigma\tau}$, Q.E.D.

THEOREM 25 (Schur): *If the order n of the finite factor group $\mathfrak{F}$ is relatively prime to the order m of the finite normal subgroup $\mathfrak{N}$, then the extension $\mathfrak{G}$ splits over $\mathfrak{N}$.*

Proof: We need only show that $\mathfrak{G}$ contains a subgroup of order n.

If $m = 1$, this is clear. Let $m > 1$ and assume the statement proven when the order of the normal subgroup is less than m. For a prime divisor p of m, every Sylow p-group S_p of $\mathfrak{G}$ is contained in $\mathfrak{N}$. Since there are as many Sylow p-groups in $\mathfrak{N}$ as in $\mathfrak{G}$, $N_p : \mathfrak{N} \cap N_p = n$. Now $N_p \cap \mathfrak{N}/S_p$ is a normal subgroup of N_p/S_p with index n. By the induction hypothesis there is a subgroup $\mathfrak{H}/S_p$ of order n in N_p/S_p. S_p/z_p is a normal subgroup of $\mathfrak{H}/z_p$ of index n, where z_p is the center of S_p and is different from e. By the induction hypothesis there is a subgroup $\mathfrak{U}/z_p$ of order n in $\mathfrak{H}/z_p$. Let $C_{\sigma,\tau}$ be a factor system of $\mathfrak{U}$ over z_p. Since the order z of z_p is relatively prime to n, we can solve the congruence $nn_1 \equiv 1\,(z)$ and for the factor system $C_{\sigma,\tau}$ of $\mathfrak{U}$ over z_p we find that it is the n_1-th power of the factor system $C^m_{\sigma,\tau}$ which is retracting by Theorem 24. Therefore $C_{\sigma,\tau}$ itself splits over z_p, i.e. $\mathfrak{U}$ contains a subgroup of order n, Q.E.D.

In what follows, let $\mathfrak{F}$ be a finite group of order n.

THEOREM 26: *If $a_\sigma a^\sigma_\tau = a_{\sigma\tau}$ and the a_σ commute with one another, then the equation $a^n_\sigma = \delta^{1-\sigma}$ is solvable, i.e. the mapping $S_\sigma \to a^n_\sigma S_\sigma$ can be accomplished by transformation with an element δ in $\mathfrak{N}$.*

Proof: Form the product over all equations with fixed σ:

$$a^n_\sigma \prod_\tau a^\sigma_\tau = \prod_\tau a_{\sigma\tau} = \prod_\tau a_\tau.$$

We set $\delta = \prod_\tau a_\tau$ and have $a^n_\sigma \delta^\sigma = \delta$, Q.E.D.

It has been conjectured that the following theorem is true in general.

THEOREM 27: *If the order n of the finite factor group $\mathfrak{F}$ is relatively prime to the order m of the finite normal subgroup $\mathfrak{N}$, then two representative groups of $\mathfrak{G}$ over $\mathfrak{N}$ are conjugate in $\mathfrak{G}$. We shall prove the theorem when any of the following additional conditions holds:*

1. *$\mathfrak{N}$ is abelian.*
2. *$\mathfrak{N}$ is solvable.*
3. *$\mathfrak{F}$ is solvable.*

One of the groups $\mathfrak{N}$, $\mathfrak{F}$ is of odd order, and since it is conjectured that groups of odd order are solvable, it is also expected that the above theorem is true. E. Witt reduced the theorem to the case when $\mathfrak{N}$ is simple and the centralizer of $\mathfrak{N}$ in $\mathfrak{G}$ is e. It is believed that the group of outer automorphisms of a finite simple group is solvable, so that we can conjecture the truth of Theorem 27 on this basis also.

Proof of 1: If $\mathfrak{U} = \{S_\sigma\}$ is a representative group and $\mathfrak{V} = \{a_\sigma S_\sigma\}$, a second one, then we have the equations

$$a_\sigma a_\tau^\sigma = a_{\sigma\tau}.$$

By Theorem 26, $a_\sigma^n = \delta^{1-\sigma} (\sigma \in \mathfrak{F})$ is solvable. Since by hypothesis the congruence $n \cdot n_1 \equiv 1 (\mathfrak{N} : 1)$ is solvable, $a_\sigma = a_\sigma^{n \cdot n_1} = (\delta^{n_1})^{1-\sigma}$, Q.E.D.

Proof of 2: If $\mathfrak{N}$ is abelian, then the theorem is true by 1; let $\mathfrak{N}$ be k-step metabelian and assume the theorem has already been proven for $D^{k-1}(\mathfrak{N}) = e$. . Further, let $\mathfrak{U}$ and $\mathfrak{V}$ be two representative groups of $\mathfrak{G}$ over $\mathfrak{N}$. We apply 1 to $\mathfrak{G}/\mathfrak{N}'$ and find that $\mathfrak{V}\mathfrak{N}' = (\mathfrak{U}\mathfrak{N}')^x$ with $x \in \mathfrak{N}$ is solvable i.e., $\mathfrak{V}^{x^{-1}}\mathfrak{N}' = \mathfrak{U}\mathfrak{N}'$. Since $D^{k-1}(\mathfrak{N}') = e$, then by applying the induction hypothesis to $\mathfrak{U}\mathfrak{N}'$, it follows that $\mathfrak{V}^{x^{-1}} = \mathfrak{U}^y$ is also solvable for $y \in \mathfrak{N}$ and therefore $\mathfrak{V} = \mathfrak{U}^{xy}$, with $xy \in \mathfrak{N}$, Q.E.D.

Proof of 3: Let a principal series of $\mathfrak{G}/\mathfrak{N}$ be of length l, and let $\mathfrak{U}$, $\mathfrak{V}$ be two representative groups of $\mathfrak{G}$ over $\mathfrak{N}$. Let $\mathfrak{u}$ be a minimal normal subgroup of $\mathfrak{U}$; since $\mathfrak{U}$ is solvable, $\mathfrak{u}$ is a p-group. $\mathfrak{u}$ is isomorphic to $\mathfrak{v} = \mathfrak{V} \cap \mathfrak{u}\mathfrak{N}$ where $\mathfrak{v}$ is a normal subgroup of $\mathfrak{V}$.

If $l = 1$, then $\mathfrak{u} = \mathfrak{U}$, $\mathfrak{v} = \mathfrak{V}$. Then $\mathfrak{U}$ and $\mathfrak{V}$ are Sylow p-groups of $\mathfrak{G}$, therefore conjugate in $\mathfrak{G}$. Let $l > 1$, and assume that the theorem has been proven for smaller l. By the induction hypothesis there is an x in $\mathfrak{u}\mathfrak{N} = \mathfrak{v}\mathfrak{N}$, such that $\mathfrak{v} = \mathfrak{u}^x$. We set $\mathfrak{V}_1 = \mathfrak{V}^{x^{-1}}$ and find that $\mathfrak{U}, \mathfrak{V}_1 \leq N_\mathfrak{u}$. Since the principal series of $\mathfrak{U}/\mathfrak{u}$ is of length l-1, it follows by the induction hypothesis applied to $N_\mathfrak{u}/\mathfrak{u}$ that there is a $y \in N_\mathfrak{u}$, such that $\mathfrak{V}_1 = \mathfrak{U}^y$, and therefore $\mathfrak{V} = \mathfrak{U}^{xy}$, Q.E.D.

Exercises

In a finite solvable group, certain generalized Sylow theorems are valid (Hall):

1. For every decomposition $N = n.m$ of the group order into a product of relatively prime factors, there is a subgroup of order m and index n.

2. Let n and m be chosen as in Exercise 1. All subgroups whose order is a divisor of m lie in a subgroup of order m.

3. Let m be as in Exercise 1. All subgroups of order m are conjugate. The normalizer of a subgroup of order m is its own normalizer.

(Proofs of 1 – 3 by induction on the length of the principal series and by use of Theorems 25, 27.)

V. TRANSFERS INTO A SUBGROUP

§ 1. Monomial Representations and Transfers into a Subgroup

We wish to represent the elements of a group $\mathfrak{G}$ as permutations on a set whose objects admit multiplication by the elements of a second group $\mathfrak{H}$.

DEFINITION: A set $\mathfrak{M}$ of elements $u, v, \ldots$. is called an $(\mathfrak{H}, \mathfrak{G})$-system if for every pair u, G (or H, u) the product uG (or Hu) is defined uniquely as an element of $\mathfrak{M}$, and if moreover for all u in $\mathfrak{M}$:

$$u(GG') = (uG)G', \tag{1}$$

$$(HH')u = H(H'u),$$

$$ue_{\mathfrak{G}} = e_{\mathfrak{H}}u = u, \tag{2}$$

$$H(uG) = (Hu)G. \tag{3}$$

By (1), the correspondence $G \to \pi_G = \begin{pmatrix} u \\ uG^{-1} \end{pmatrix}$ gives a representation of $\mathfrak{G}$ in single-valued mappings of $\mathfrak{M}$ onto itself. Since $\pi_e = \begin{pmatrix} u \\ ue \end{pmatrix} = \underline{1}$, the π_G form a group $\Delta_{\mathfrak{G}}$ of permutations of $\mathfrak{M}$. We shall assume in addition that $\Delta_{\mathfrak{G}}$ is transitive.

Example: Let $\mathfrak{U}$ be a subgroup of $\mathfrak{G}$, $\mathfrak{u}$ a normal subgroup of $\mathfrak{U}$. Then the right cosets of $\mathfrak{G}$ over $\mathfrak{u}$ form a $(\mathfrak{U}, \mathfrak{G})$-system for which $\Delta_{\mathfrak{G}}$ is transitive.

We shall show that all $(\mathfrak{H}, \mathfrak{G})$-systems with transitive $\Delta_{\mathfrak{G}}$ are of the type described in the preceding example.

First of all, it follows from (1) and (2) that the correspondence

$$H \to \bar{H} = \begin{pmatrix} u \\ Hu \end{pmatrix}$$

is a representation of $\mathfrak{H}$ in permutations of the elements of $\mathfrak{M}$. All these permutations $\bar{H}$ form a group $\bar{\mathfrak{H}}$, and

$$\overline{HH'} = \bar{H}\bar{H}'. \tag{4}$$

We now define $\bar{H}$ as an operator on $\mathfrak{M}$ by the equation:

$$\bar{H}u = Hu \tag{5}$$

This definition is unambiguous and now $\mathfrak{M}$ is also an $(\bar{\mathfrak{H}}, \mathfrak{G})$-system. Because of (4) and (5) the questions about $(\bar{\mathfrak{H}}, \mathfrak{G})$-systems are equivalent to the questions about $(\mathfrak{H}, \mathfrak{G})$-systems; and so we shall assume that $\mathfrak{H}$ is equal to $\bar{\mathfrak{H}}$, i.e.,

(6) $Hu = u$ for all u implies $H = e_{\mathfrak{H}}$. If $Hu_0 = u_0$, then

$$H(u_0 G) = (Hu_0)G = u_0 G$$

for all G; therefore because of the transitivity of $\Delta_{\mathfrak{G}}$:

$$Hu = u$$

for all u, and so $H = e_{\mathfrak{H}}$.

(7) Every H is indeed determined completely by the way it operates on only one element of $\mathfrak{M}$.

Let u_0 be a fixed element of $\mathfrak{M}$. All the elements of $\mathfrak{G}$ which leave u_0 fixed form a subgroup $\mathfrak{u}$. We now investigate the complex $\mathfrak{U}$ consisting of all the elements U of $\mathfrak{G}$ for which the equation $u_0 U = U^* u_0$ is solvable with some $U^* \in \mathfrak{H}$.

Because of the transitivity of $\Delta_{\mathfrak{G}}$ and because of (7), it follows that the mapping

$$U \to U^*$$

is a single-valued mapping of $\mathfrak{U}$ onto all of $\mathfrak{H}$. If U and V are contained in $\mathfrak{U}$, then

$$u_0(UV) = (u_0 U)V = U^* u_0 V = U^* V^* u_0,$$

and hence $$UV \in \mathfrak{U},\ (UV)^* = U^* V^*.$$

The mapping of U onto U^* maps $\mathfrak{U}$ homomorphically onto $\mathfrak{H}$. Precisely the elements of $\mathfrak{u}$ are mapped onto $e_{\mathfrak{H}}$. Since $\mathfrak{u}$ and $\mathfrak{H}$ are groups, $\mathfrak{U}$ is a group also. $\mathfrak{u}$ is a normal subgroup of $\mathfrak{U}$, and we may, and in fact shall, consider $\mathfrak{H}$ simply as the group of cosets of $\mathfrak{U}$ over $\mathfrak{u}$.

The mapping

(8) $$\overline{u_0 G} = \mathfrak{u} G$$

is single-valued, for from

$$u_0 G = u_0 G'$$

it follows that $$u_0 G G'^{-1} = u_0,\ G G'^{-1} \leq \mathfrak{u},$$

$$\mathfrak{u} G = \mathfrak{u} G',$$

and conversely.

Moreover

$$\overline{(u_0 G)G'} = \overline{u_0(GG')} = \mathfrak{u}GG' = (\mathfrak{u}G)G' = \overline{u_0 G}\cdot G',$$

$$\overline{U^* u_0 G} = \overline{u_0 UG} = \mathfrak{u}UG = U\,\mathfrak{u}G = U\overline{u_0 G} = U^*\overline{u_0 G}.$$

Therefore, according to (8), the given $(\mathfrak{H}, \mathfrak{G})$-system $\mathfrak{M}$ with transitive $\Delta_{\mathfrak{G}}$ can be identified with the set of right cosets of $\mathfrak{G}$ over a subgroup $\mathfrak{u}$, where $\mathfrak{u}$ is a normal subgroup of a subgroup $\mathfrak{U}$ and the factor group $\mathfrak{U}/\mathfrak{u}$ is isomorphic to $\mathfrak{H}$.

Let $G \to \overline{G}$ be a representative function belonging to the decomposition $\mathfrak{G} = \sum_1^{\omega} \mathfrak{U}G_i$. If we put $u_i = \mathfrak{u}G_i$, then every coset from $\mathfrak{M}$ has the unique form

$$u = U^* u_i.$$

Accordingly

$$u_i G = U^*_{i,G}\, u_{iG}. \tag{9}$$

Here the permutation $\begin{pmatrix} i \\ iG \end{pmatrix}$ is determined by the equation

$$\mathfrak{U}G_i G = \mathfrak{U}G_{iG}. \tag{10}$$

Moreover

$$U^*_{i,G} = G_i G\overline{G_i G}^{-1} = G_i G G_{iG}^{-1}, \tag{11}$$

for $$U^*_{i,G}u_{iG} = U^*_{i,G}\,\mathfrak{u}\overline{G_i G} = \mathfrak{u}\,U^*_{i,G}\overline{G_i G} = \mathfrak{u}\cdot G_i G = u_i G.$$

It is obvious that through (9) a matrix M_G having ω rows and ω columns can be associated with each element G of $\mathfrak{G}$:

$$M_G = (\delta_{iG,k}\, U^*_{i,G}). \tag{12}$$

That is, M_G is a matrix with the element $U^*_{i,G}$ in the i-th row and iG-th column and with zeroes elsewhere. M_G is a permutation of the u_i with factors from $\mathfrak{U}^*\,(= \mathfrak{H})$. From (1) and (3) it now follows that

$$M_G \cdot M_{G'} = M_{GG'}, \tag{13}$$

where the product of two matrices is computed in the usual manner. We call the representation (12) of $\mathfrak{G}$ in square matrices of degree ω with coefficients zero, or from the group $\mathfrak{U}^*$, the *monomial representation with ω members.*

In going over to another system of representatives of right cosets of

$\mathfrak{G}$ over $\mathfrak{U}$ we change to a new "basis" $v_1, v_2, \ldots, v_\omega$ of $\mathfrak{M}$ which is connected to the old one by equations of the form

$$v_i = U_i^* u_{\tau i} \quad , \tag{14}$$

where $\begin{pmatrix} i \\ \tau i \end{pmatrix}$ is a permutation of the numbers $1, 2 \ldots \omega$. If we put down as transformation matrix

$$T = (\delta_{\tau i, k} U_i^*),$$

where U_i^* stands at the intersection of the i-th row with the τi-th column and there are zeros everywhere else, then the representation with ω members belonging to the v_i and with matrices M_G^* is given by

$$M_G^* = T M_G T^{-1}. \tag{15}$$

If we put $\mathfrak{u} = e$, then we obtain the most general monomial representation of $\mathfrak{G}$ over $\mathfrak{U}$:

$$G \to M_G^{\mathfrak{U}} = (\delta_{iG, k} U_{i, G}), \tag{16}$$

from which the representations with arbitrary normal subgroup of $\mathfrak{U}$ can be obtained by replacing the elements by their cosets.

If $\mathfrak{V}$ is a subgroup of $\mathfrak{U}$, let $\mathfrak{U} = \sum_1^\nu \mathfrak{V} U_k$ be a right coset decomposition of $\mathfrak{U}$ over $\mathfrak{V}$. Then $\mathfrak{G} = \sum_{i,k} \mathfrak{V} U_k G_i$ is a right coset decomposition of $\mathfrak{G}$ over $\mathfrak{V}$, and from equations (10) and (12) it follows that:

(17) $M_G^{\mathfrak{V}}$ arises from the matrix $M_G^{\mathfrak{U}}$ upon the replacement of each element U from $\mathfrak{U}$ by the matrix $m_{\mathfrak{U}}^{\mathfrak{V}}$ belonging to the representation of $\mathfrak{U}$ over $\mathfrak{V}$ and by replacing each 0 by a ν-rowed matrix of zeroes.

If we replace the normal subgroup $\mathfrak{u}$ by the commutator group $\mathfrak{U}'$ of $\mathfrak{U}$, then there corresponds a representation of $\mathfrak{G}$ in matrices whose coefficients are from an abelian group. Through the construction of determinants we arrive at a new representation. We define:

The *transfer of the element* X from the group $\mathfrak{G}$ into the subgroup $\mathfrak{U}$ is the coset $V_{\mathfrak{G} \to \mathfrak{U}}(X)$ of $\mathfrak{U}$ over its commutator group $\mathfrak{U}$. If $\mathfrak{U}$ is of finite index n and has the system of left representatives $G_1, G_2, \ldots, G_n$ with the representation function $G \to \overline{G}$ then we define

$$V_{\mathfrak{G} \to \mathfrak{U}}(X) = \mathfrak{U}' \cdot \prod_1^n G_i X \overline{G_i X}^{-1}. \tag{18}$$

THEOREM 1: *The transfer is independent of the choice of the system of representatives.*

Proof: $V(X)$ is (to within sign) the determinant of the representa-

tion matrix $M_X^{\mathfrak{U}}$, having coefficients from $\mathfrak{U}/\mathfrak{U}'$ or else 0. By transforming to a new system of left representatives we simply transform M_X by a fixed matrix T. This does not alter the value of the determinant.

THEOREM 2: *The transfer of* $\mathfrak{G}$ *to* $\mathfrak{U}$ *is a homomorphy of* $\mathfrak{G}$ *into* $\mathfrak{U}/\mathfrak{U}'$.

Proof: This follows from (13) upon construction of determinants.

The transfer $V_{\mathfrak{G}\to\mathfrak{U}}$ induces an isomorphy between an abelian factor group of $\mathfrak{G}$ and $\mathfrak{U}/\mathfrak{U}'$. Hence $V_{\mathfrak{G}\to\mathfrak{U}}(\mathfrak{G}') = \mathfrak{U}'$. The subgroup of $\mathfrak{U}/\mathfrak{U}'$ consisting of all the cosets $V_{\mathfrak{G}\to\mathfrak{U}}(\mathfrak{G})$ is called the *transferred group of* $\mathfrak{G}$ *to* $\mathfrak{U}$.

THEOREM 3: *For a subgroup* $\mathfrak{V}$ *of* $\mathfrak{U}$ *with finite index it follows that*:

$$V_{\mathfrak{G}\to\mathfrak{V}}(X) = V_{\mathfrak{U}\to\mathfrak{V}}(V_{\mathfrak{G}\to\mathfrak{U}}(X)).$$

Proof: This follows from (17) upon construction of determinants two times.

Remark: If $\mathfrak{G}$ is a group with given automorphism domain, then the transferred group is an admissible group, for when $\mathfrak{T}$ is a system of left representatives of $\mathfrak{G}$ over $\mathfrak{U}$, then so is $\mathfrak{T}^\sigma$ (σ an automorphism of $\mathfrak{G}$) provided $\mathfrak{U}$ is admissible. In particular the transferred group of a transfer into a normal subgroup is itself normal.

In order to compute the transfer of a given element X, it is useful to choose a particular system of representatives. The permutation $\begin{pmatrix} \mathfrak{U}G \\ \mathfrak{U}GX \end{pmatrix}$ of the right cosets of $\mathfrak{G}$ over $\mathfrak{U}$ decomposes into r cycles. From the i-th cycle we choose a representative $\mathfrak{U}T_i$, and the cycle may be written $(\mathfrak{U}T_i, \mathfrak{U}T_iX, \ldots, \mathfrak{U}T_iX^{f_i-1})$. Then for the system of representatives $T_i, T_iX, \ldots, T_iX^{f_i-1}$ $(i = 1, 2, \ldots, r)$:

$$V_{\mathfrak{G}\to\mathfrak{U}}(X) = \mathfrak{U}' \prod_1^r T_i X^{f_i} T_i^{-1}, \tag{19}$$

where f_i is the length of the i-th cycle, and hence is a divisor of the order of X. Moreover

$$\sum_1^r f_i = \mathfrak{G} : \mathfrak{U}. \tag{20}$$

Exercise: Prove the three theorems on transfers by direct calculation, on the basis of (18) and the rules about representative functions.

§ 2. The Theorems of Burnside and Grün

LEMMA: If two complexes $\mathfrak{K}$, $\mathfrak{L}$ in a Sylow p-group $\mathfrak{P}$ of the finite group $\mathfrak{G}$ are normal[1] in $\mathfrak{P}$ and conjugate under $\mathfrak{G}$, then they are also conjugate under the normalizer $N_{\mathfrak{P}}$ of $\mathfrak{P}$.

Proof: The hypothesis says $\mathfrak{P}$ is in the normalizer $N_{\mathfrak{K}}$ of $\mathfrak{K}$ and in the normalizer $N_{\mathfrak{L}}$ of $\mathfrak{L}$, and that

$$\mathfrak{L} = T\mathfrak{K}T^{-1} = \mathfrak{K}^T$$

is solvable with T in $\mathfrak{G}$.

From $\mathfrak{P} \leq \mathfrak{K}$ and from $N_{\mathfrak{L}} = N_{\mathfrak{K}}^T$ it follows that: $\mathfrak{P}^T \leq N_{\mathfrak{L}}$. Since $\mathfrak{P}$ and $\mathfrak{P}^T$ are Sylow p-groups of $\mathfrak{G}$ in $N_{\mathfrak{L}}$, they are also Sylow p-groups of $N_{\mathfrak{L}}$, consequently $\mathfrak{P} = \mathfrak{P}^{ST}$ with S in $N_{\mathfrak{L}}$ is solvable by the third Sylow theorem.

Consequently ST is in $N_{\mathfrak{P}}$ and $\mathfrak{K}^{ST} = \mathfrak{L}^S = \mathfrak{L}$, Q.E.D.

THEOREM 4 (Burnside): *If the Sylow p-group $\mathfrak{P}$ of a finite group $\mathfrak{G}$ is in the center of its normalizer, then $\mathfrak{G}$ contains a normal subgroup with $\mathfrak{P}$ as system of representatives.*

Proof: The hypothesis implies that $\mathfrak{P}$ is abelian, so that its commutator subgroup is e. We transfer $\mathfrak{G}$ into $\mathfrak{P}$ and obtain a normal subgroup $\mathfrak{N}$ of all elements which are transferred to e, and a transfer group $V(\mathfrak{G}) \leq \mathfrak{P}$. If we show that $V(\mathfrak{P}) = \mathfrak{P}$, then $V(\mathfrak{G}) = \mathfrak{P}$, hence $\mathfrak{N}\mathfrak{P} = \mathfrak{G}$, and $\mathfrak{P} \cap \mathfrak{N} = e$, and the theorem is proven.

For an element X in $\mathfrak{P}$, by § 1, (19)

$$V(X) = \prod_1^r T_i X^{f_i} T_i^{-1}$$

for certain T_i where $\sum_1^r f_i = \mathfrak{G} : \mathfrak{P}$, and every factor of the product is contained in $\mathfrak{P}$. But the elements X^{f_i}, $T_i X^{f_i} T_i^{-1}$, conjugate under $\mathfrak{G}$, are normal in the abelian Sylow p-group $\mathfrak{P}$; therefore by the lemma they are conjugate under $N_{\mathfrak{P}}$. Therefore by hypothesis they are equal to one another, so that

$$V(X) = \prod_1^r X^{f_i} = X^{\mathfrak{G}:\mathfrak{P}} .$$

Since $\mathfrak{G}:\mathfrak{P}$ is relatively prime to the order of the Sylow group $\mathfrak{P}$, we have $V(\mathfrak{P}) = \mathfrak{P}$, which proves the theorem.

It follows immediately from the Burnside theorem that the order of a finite simple group of composite order is divisible by the cube of its smallest prime factor, or by 12. (See IV, § 3, Exercise 5).

[1] $\mathfrak{K}$ is called normal in $\mathfrak{P}$, if $x\mathfrak{K}x^{-1} = \mathfrak{K}$ for all x in $\mathfrak{P}$.

With the transfer of a finite group $\mathfrak{G}$ into a Sylow p-group $\mathfrak{P}$ we associate the normal subgroup $\mathfrak{G}_1$ which consists of all the elements of $\mathfrak{G}$ which are transferred to the commutator subgroup $\mathfrak{P}'$ of $\mathfrak{P}$. $\mathfrak{G}/\mathfrak{G}_1$ is isomorphic to the transfer of $\mathfrak{G}$ in $\mathfrak{P}$, and therefore is an abelian p-group. By Chapter IV it follows from this that $\mathfrak{G} = \mathfrak{P}\mathfrak{G}_1$ and therefore by the second isomorphy theorem, $\mathfrak{G}/\mathfrak{G}_1 \simeq \mathfrak{P}/\mathfrak{P} \cap \mathfrak{G}_1$.

Can the p-group $\mathfrak{P}_1 = \mathfrak{P} \cap \mathfrak{G}_1$ also be characterized from within? $\mathfrak{P}_1$ is defined from above as the group of those elements of $\mathfrak{P}$ whose transfers in $\mathfrak{P}$ are in $\mathfrak{P}'$. The elements of $\mathfrak{P} \cap \mathfrak{G}'$ are among these elements. In particular, in $\mathfrak{P}_1$ we have the intersection of $\mathfrak{P}$ with the commutator group $N_{\mathfrak{P}}$ of the normalizer $N_{\mathfrak{P}}$ of $\mathfrak{P}$, and the groups $\mathfrak{P} \cap \mathfrak{P}'^{T}$, where $T \in \mathfrak{G}$. Our question is now answered by the FIRST THEOREM OF GRÜN (THEOREM 5): *On transferring a finite group $\mathfrak{G}$ into a Sylow p-group $\mathfrak{P}$, the transferred group is isomorphic to the factor group of $\mathfrak{P}$ over the normal subgroup*

$$(\mathfrak{P} \cap N'_{\mathfrak{P}}) \cdot \prod_{T \in \mathfrak{G}} \mathfrak{P} \cap \mathfrak{P}'^{T}.$$

Proof: We set $V_{\mathfrak{G} \to \mathfrak{P}}(X) = VX$, and $\mathfrak{P}_2 = (\mathfrak{P} \cap N'_{\mathfrak{P}}) \cdot \prod_{T \in \mathfrak{G}} \mathfrak{P} \cap \mathfrak{P}'^{T}$, and then since $\mathfrak{P}_2 \subseteq \mathfrak{P}_1$ and $V\mathfrak{G}/\mathfrak{P}' \simeq \mathfrak{P}/\mathfrak{P}_1$ we must prove that $\mathfrak{P}_2 = \mathfrak{P}_1$.

Assume that $\mathfrak{P}_2 \neq \mathfrak{P}_1$ and then let X be an element of minimal order which is in $\mathfrak{P}_1$ but not in $\mathfrak{P}_2$. We shall be led to a contradiction by showing that $VX \notin \mathfrak{P}'$, and in fact that $VX \notin \mathfrak{P}_2$.

We anticipate the essential argument by remarking that $X^{p^t T} \in \mathfrak{P}$, $t > 0$ implies $X^{p^t T} \in \mathfrak{P}_2$, since $VX^{p^t T} = VT \cdot VX^{p^t} \cdot VT^{-1} = VX^{p^t} = \mathfrak{P}'$; and therefore $X^{p^t T}$ is in $\mathfrak{P}_1$; and since it is of lower order than X, it is in $\mathfrak{P}_2$.

Under the representation $Y \to \begin{pmatrix} \mathfrak{P}G \\ \mathfrak{P}G\,Y^{-1} \end{pmatrix}$ of $\mathfrak{G}$ in permutations of the right cosets of $\mathfrak{G}$ over $\mathfrak{P}$, we also obtain a representation of $\mathfrak{P}$, and the right cosets of $\mathfrak{G}$ over $\mathfrak{P}$ decompose under $\mathfrak{P}$ into systems $\mathfrak{T}_i$ of transitivity having p^{t_i} right cosets. Under multiplication on the right by X, the cosets from $\mathfrak{T}_i = \mathfrak{T}$ are permuted in certain p^m-member cycles. We look for a coset $\mathfrak{P}T$ from $\mathfrak{T}$ which belongs to a cycle of minimal length p^{μ}; then all p^t cosets from $\mathfrak{T}$ are of the form $\mathfrak{P}TP$ with P in $\mathfrak{P}$.

1. $T \notin N_{\mathfrak{P}}$, i.e., $p^t > 1$. Then the cosets of a p^m-member cycle are: $\mathfrak{P}TP, \mathfrak{P}TPX, \ldots, \mathfrak{P}TPX^{p^m-1}$, where m, naturally, depends on P, and $\mathfrak{P}TPX^{p^m} = \mathfrak{P}TP$. If one chooses TPX^i as coset representative, then

the product of associated transfer factors satisfies

$$TPX(TPX)^{-1} \cdot TPX^2(TPX^2)^{-1} \ldots TPX^{p^m}(TP)^{-1} = X^{p^m TP} \in \mathfrak{P},$$

and it follows from our determination of T that $\mu \leqq m$, $X^{p^m T} \in \mathfrak{P}$; therefore $X^{p^m TP} \cdot X^{-p^m T} = \left((X^{p^m})^{P-1}\right)^T = \left(P, X^{p^m}\right)^T \in \mathfrak{P}'^T$ and by the construction of $\mathfrak{P}_2$:

$$X^{p^m TP} \equiv X^{p^m T}(\mathfrak{P}_2).$$

The product of all transfer factors which belong to the right cosets in $\mathfrak{P}T\mathfrak{P}$, is congruent to $X^{p^t T}(\mathfrak{P}_2)$, and therefore, by the remark at the beginning of the proof, is contained in $\mathfrak{P}_2$.

2. $T \in N_{\mathfrak{P}}$. Then $\mathfrak{P}TX = \mathfrak{P}X^T \cdot T = \mathfrak{P}T = \mathfrak{P}T\mathfrak{P}$. The corresponding transfer factor is X^T. Since $X^T \equiv X(N'_{\mathfrak{P}})$, it follows that:

$$X^T \equiv X(\mathfrak{P}_2)$$

by the construction of $\mathfrak{P}_2$.

1. and 2. together imply the congruence

$$VX \equiv X^{N_{\mathfrak{P}} : \mathfrak{P}}(\mathfrak{P}_2),$$

and since $N_{\mathfrak{P}} : \mathfrak{P}$ is relatively prime to p, we obtain the contradiction $VX \notin \mathfrak{P}_2$, Q.E.D.

COROLLARY to the First Theorem of Grün:

The normal subgroup $\mathfrak{G}_1$ consisting of all the elements of $\mathfrak{G}$ transferred to $\mathfrak{P}'$ is the p-commutator group $\mathfrak{G}'(p)$ of $\mathfrak{G}$, i.e., the group transferred into a Sylow p-group is isomorphic to the p-factor commutator group.[1]

Proof: Since $\mathfrak{G}/\mathfrak{G}_1$ is an abelian p-group, $\mathfrak{G}'(p)$ is in $\mathfrak{G}_1$. Moreover, by what was shown in the previous proof, $\mathfrak{P}_1 = \mathfrak{P} \cap \mathfrak{G}_1 \leqq \mathfrak{P} \cap \mathfrak{G}'$. On the other hand, $\mathfrak{G}'$ is in $\mathfrak{G}_1$; therefore $\mathfrak{P} \cap \mathfrak{G}'$ is in $\mathfrak{P}_1$; therefore $\mathfrak{P}_1 = \mathfrak{P} \cap \mathfrak{G}'$. By Chapter IV, $\mathfrak{G}/\mathfrak{G}'(p) \simeq \mathfrak{P}/\mathfrak{P} \cap \mathfrak{G}'$. From this we conclude

$$\mathfrak{G}/\mathfrak{G}'(p) \simeq \mathfrak{P}/\mathfrak{P}_1 \simeq \mathfrak{G}/\mathfrak{G}_1, \quad \mathfrak{G} : \mathfrak{G}'(p) = \mathfrak{G} : \mathfrak{G}_1, \quad \mathfrak{G}_1 = \mathfrak{G}'(p).$$

DEFINITION: A finite group is said to be *p-normal* if the center of one of its Sylow p-groups is the center of every Sylow p-group in which it is contained.

For example, a finite group with abelian Sylow p-groups is is p-normal.

SECOND THEOREM OF GRÜN (THEOREM 6): *If the finite group* $\mathfrak{G}$ *is*

[1] See the definitions in IV, § 5, Exercise 1.

p-normal, then the factor commutator group of $\mathfrak{G}$ *is isomorphic to the p-factor commutator group of the normalizer of a p-center.*

Proof: Let $\mathfrak{z}$ be the center of the Sylow p-group $\mathfrak{P}$; let $\mathfrak{P}_1$ be the intersection of $\mathfrak{G}'$ with $\mathfrak{P}$; let $\mathfrak{P}_2$ be the intersection of $\mathfrak{P}$ with the commutator group $N_\mathfrak{z}'$ of the normalizer $N_\mathfrak{z}$ of $\mathfrak{z}$. By Chapter IV we know that $\mathfrak{G}/\mathfrak{G}'(p) \simeq \mathfrak{P}/\mathfrak{P}_1$, $N_\mathfrak{z}/N_\mathfrak{z}'(p) \simeq \mathfrak{P}/\mathfrak{P}_2$. Since $\mathfrak{P}_2$ is contained in $\mathfrak{P}_1$, we have to prove that $\mathfrak{P}_2$ is equal to $\mathfrak{P}_1$. By the first Grün theorem

$\mathfrak{P}_1 = (\mathfrak{P} \cap N_\mathfrak{P}') \cdot \prod_{T \in \mathfrak{G}} \mathfrak{P} \cap \mathfrak{P}'^T$, and therefore we must show:

(a) $\mathfrak{P} \cap N_\mathfrak{P}' \leq \mathfrak{P}_2$, (b) $\mathfrak{P} \cap \mathfrak{P}'^T \leq \mathfrak{P}_2$ for all T in $\mathfrak{G}$.

(a) follows from $N_\mathfrak{P} \leq N_\mathfrak{z}$, $N_\mathfrak{P}' \leq N_\mathfrak{z}'$.

For the proof of (b) we put $\mathfrak{D} = \mathfrak{P} \cap \mathfrak{P}'^T$ and find that $\mathfrak{z} \leq N_\mathfrak{D}$, $\mathfrak{z}^T \leq N_\mathfrak{D}$, since $\mathfrak{z}^T$ is the center of $\mathfrak{P}^T$. $\mathfrak{z}$ is in a Sylow p-group $\mathfrak{q}$ of $N_\mathfrak{D}$, $\mathfrak{z}^T$ is in a Sylow p-group $\mathfrak{p}$ of $N_\mathfrak{D}$ and by the second Sylow theorem there is an S in $N_\mathfrak{D}$ such that $\mathfrak{p}^S = \mathfrak{q}$; therefore $\mathfrak{z}^{ST}$ is contained in $\mathfrak{q}$, $\mathfrak{q}$ is contained in a Sylow p-group $\mathfrak{Q}$ of $\mathfrak{G}$, and since by hypothesis $\mathfrak{G}$ is p-normal, both $\mathfrak{z}$ and $\mathfrak{z}^{ST}$ are equal to the center of $\mathfrak{Q}$, and therefore equal to each other. ST is contained in $N_\mathfrak{z}$, and $\mathfrak{D} = \mathfrak{D}^S = \mathfrak{P}^S \cap \mathfrak{P}'^{ST}$, $\mathfrak{D} \leq \mathfrak{P}'^{ST} \leq N_\mathfrak{z}'$, so finally $\mathfrak{D} \leq \mathfrak{P} \cap N_\mathfrak{z}' = \mathfrak{P}_2$, Q.E.D.

COROLLARY TO THE SECOND THEOREM OF GRÜN: The transfer of a p-normal group into the Sylow p-group $\mathfrak{P}$ is equal to the transfer $V_{N_\mathfrak{z} \to \mathfrak{P}}(N_\mathfrak{z})$ of the normalizer $N_\mathfrak{z}$ of the center $\mathfrak{z}$ of $\mathfrak{P}$ into the Sylow p-group $\mathfrak{P}$ of $N_\mathfrak{z}$.

This is true since by Theorem 3 on transfers, $V_{\mathfrak{G} \to \mathfrak{P}}(\mathfrak{G})$ is contained in $V_{N_\mathfrak{z} \to \mathfrak{P}}(N_\mathfrak{z})$, and by what has just been proven, these are isomorphic.

In order to obtain results about the case where every Sylow p-group is abelian, we prove the

LEMMA: If the index of the finite group $\mathfrak{G}$ over the abelian normal subgroup $\mathfrak{A}$ is relatively prime to the order of $\mathfrak{A}$, then

$$\mathfrak{A} = (\mathfrak{A} \cap \mathfrak{G}') \times (\mathfrak{A} \cap \mathfrak{z}(\mathfrak{G})) \quad \text{and} \quad V_{\mathfrak{G} \to \mathfrak{A}}(\mathfrak{G}) = \mathfrak{A} \cap \mathfrak{z}(\mathfrak{G}).$$

Proof: Let $\mathfrak{G}_1$ be the normal subgroup of all elements which are transferred onto e by $V_{\mathfrak{G} \to \mathfrak{A}} = V$. Then $\mathfrak{G}:\mathfrak{G}_1$ is a divisor of $\mathfrak{A}:1$; therefore, applying the hypothesis, $\mathfrak{G}_1:1$ is divisible by $\mathfrak{G}:\mathfrak{A}$; consequently $\mathfrak{G} = \mathfrak{G}_1\mathfrak{A}$, i.e., $V\mathfrak{G} = V\mathfrak{A}$.

For an element X in $\mathfrak{A}$,

$$VX = \prod_{T(\mathfrak{A})} X^T = X^{\mathfrak{G}:\mathfrak{A}} \cdot \prod_{T(\mathfrak{A})} X^{T-1} \equiv X^{\mathfrak{G}:\mathfrak{A}}(\mathfrak{A} \cap \mathfrak{G}').$$

We show first that $\mathfrak{A} = (\mathfrak{A} \cap \mathfrak{G}') \times V\mathfrak{A}$. In fact, $\mathfrak{A} \cap \mathfrak{G}' \cap V\mathfrak{A} = e$,

since from $X \in \mathfrak{A}$, $VX \in \mathfrak{A} \cap \mathfrak{G}'$, it follows that $X^{\mathfrak{G}:\mathfrak{A}} \equiv e(\mathfrak{A} \cap \mathfrak{G}')$, and by hypothesis we conclude that $X \equiv e(\mathfrak{A} \cap \mathfrak{G}')$; but then $VX = e$. Moreover $(\mathfrak{A} \cap \mathfrak{G}') \cdot V\mathfrak{A} = \mathfrak{A}$, since $(\mathfrak{A} \cap \mathfrak{G}') \cdot V\mathfrak{A}$ contains all the $(\mathfrak{G}:\mathfrak{A})$-th powers of elements in $\mathfrak{A}$, and by hypothesis these form all of $\mathfrak{A}$.

Now we shall show that $V\mathfrak{A} = \mathfrak{A} \cap \mathfrak{z}(\mathfrak{G})$, from which, together with what has already been proved, our assertion follows.

By our remark on transfer into a normal subgroup, $V\mathfrak{G}$ is a normal subgroup of $\mathfrak{G}$. For all T in $\mathfrak{G}$, X in $V\mathfrak{G}$, it follows that $X^T \equiv X \equiv e(V\mathfrak{G})$; moreover $X^T \equiv X(\mathfrak{A} \cap \mathfrak{G}')$; now since $V\mathfrak{G} = V\mathfrak{A}$ and $V\mathfrak{A} \cap \mathfrak{A} \cap \mathfrak{G}' = e$, it follows that $X^T = X$, $V\mathfrak{G} \leq \mathfrak{z}(\mathfrak{G}) \cap \mathfrak{A}$. For an element X in $\mathfrak{z}(\mathfrak{G}) \cap \mathfrak{A}$, the transfer is $X^{\mathfrak{G}:\mathfrak{A}}$, and by hypothesis, the transfer into $\mathfrak{z}(\mathfrak{G}) \cap \mathfrak{A}$ induces an automorphism; consequently $\mathfrak{z}(\mathfrak{G}) \cap \mathfrak{A} = V\mathfrak{G} = V\mathfrak{A}$, Q.E.D.

THEOREM 7: *If a Sylow p-group $\mathfrak{P}$ of the finite group $\mathfrak{G}$ is abelian, then the transfer of $\mathfrak{G}$ into $\mathfrak{P}$ maps the p-factor commutator group of $\mathfrak{G}$ isomorphically onto the intersection of the Sylow p-group with the center of its normalizer.*

Proof: Since $\mathfrak{z}(\mathfrak{P}) = \mathfrak{P}$, $\mathfrak{G}$ is p-normal; therefore by the corollary to the second Grün theorem, $V_{\mathfrak{G}\to\mathfrak{P}}(\mathfrak{G}) = V_{N_{\mathfrak{P}}\to\mathfrak{P}}(N_{\mathfrak{P}})$ and by our lemma $V_{N_{\mathfrak{P}}\to\mathfrak{P}}(N_{\mathfrak{P}}) = \mathfrak{z}(N_{\mathfrak{P}}) \cap \mathfrak{P}$.

FROBENIUS' THEOREM (THEOREM 8): *If the order N of a finite group $\mathfrak{G}$ is relatively prime to*

$$k_n = (p^n - 1)(p^{n-1} - 1) \ldots\ldots (p - 1),$$

where p^n is the order of a Sylow p-group, then the maximal p-factor group[1] *of $\mathfrak{G}$ is isomorphic to every Sylow p-group of $\mathfrak{G}$.*

Proof: If $n = 0$, the theorem is clearly true. Let $n > 0$ and assume the theorem proven for groups whose Sylow p-groups are of order less than p^n.

If $\mathfrak{G}$ is not p-normal, then, by Chapter IV, Theorem 8, there are in $\mathfrak{G}$ a p-group $\mathfrak{D} \neq e$ and an element X such that transforming $\mathfrak{D}$ with X induces an automorphism of order $q > 1$ relatively prime to p. By Chapter IV, q is a divisor of $k_{d(\mathfrak{D})}$, even a divisor of k_n since $d(\mathfrak{D}) \leqq n$. Since on the other hand q is a divisor of N, q, by hypothesis, must be equal to 1; therefore $\mathfrak{G}$ is p-normal.

If $\mathfrak{P}$ is abelian, then $\mathfrak{P}$ is in the center of its normalizer since transforming $\mathfrak{P}$ with an element in $N_{\mathfrak{P}}$ induces an automorphism whose order

[1] Definition see IV, § 5, Exercise 3.

is a divisor of both $k_{d(\mathfrak{P})}$ and N, and therefore is equal to one. Now the assertion follows from Burnside's theorem.

If the center $\mathfrak{z}$ of the Sylow p-group $\mathfrak{P}$ is different from $\mathfrak{P}$, then $\mathfrak{z} \neq e$, and therefore the induction hypothesis is applicable to $N_{\mathfrak{z}}/\mathfrak{z}$. This shows that $N_{\mathfrak{z}}$ has a p-factor group different from e; that the same is true for $\mathfrak{G}$ follows from the second Grün theorem. The maximal p-factor group $\mathfrak{G}/\mathfrak{D}_p$ is now different from e. If p still divides $\mathfrak{D}_p : 1$, then the induction hypothesis would lead to the contradiction $\mathfrak{D}_p(\mathfrak{D}_p(\mathfrak{G})) \neq \mathfrak{D}_p(\mathfrak{G})$. Therefore p is relatively prime to $\mathfrak{D}_p : 1$, and this means that every Sylow p-group of $\mathfrak{G}$ forms a system of representatives of $\mathfrak{G}$ over $\mathfrak{D}_p$, Q.E.D.

COROLLARIES: 1. The order of a finite simple group of even composite order is divisible by 12, 16 or 56.

2. From the proof of the theorem it follows that the number k_n of the theorem may be replaced by k_D, which is at most as large as k_n, where p^D is the order of the maximal abelian factor group of exponent p among all those which are factor groups of p-groups in $\mathfrak{G}$.

3. If a Sylow p-group of $\mathfrak{G}$ contains a cyclic subgroup of index p, and N is relatively prime to p^2-1, then the p-factor group of $\mathfrak{G}$ is isomorphic to a Sylow p-group. For, by Chapter IV, § 3, Exercise 1, $D \leq 2$.

Exercise: A simple finite group whose order is odd and smaller than 1000 is of prime order.

§ 3. Groups whose Sylow Groups are all Cyclic

THEOREM 9: *In the series of higher commutator groups* $\mathfrak{G}' \geq \mathfrak{G}'' \geq \ldots$ *of a given group* $\mathfrak{G}$, *two successive factor groups are cyclic only if the latter one is equal to* e.

Proof: It can be assumed that $\mathfrak{G}'/\mathfrak{G}''$ is cyclic, $\mathfrak{G}''$ is generated by A, and $\mathfrak{G}''' = e$. It will be shown that $\mathfrak{G}'' = e$.

The normalizer of $\mathfrak{G}''$ is $\mathfrak{G}$. The factor group of $\mathfrak{G}$ over the centralizer N_A of $\mathfrak{G}''$ is isomorphic to a group of automorphisms of (A), and therefore is abelian. $\mathfrak{G}'$ is in N_A, and since the factor group of $\mathfrak{G}'$ over the normal subgroup $\mathfrak{G}''$ in the center of $\mathfrak{G}'$ is cyclic, $\mathfrak{G}'$ is abelian, and therefore $\mathfrak{G}'' = e$, Q.E.D.

We make the following definition: A group is said to be *metacyclic* if its commutator group and its factor commutator group are cyclic.

As a consequence of Theorem 9, it no longer makes sense to talk of 3-step metacyclic groups. A cyclic group is metacyclic.

THEOREM 10: *If every Sylow group of a finite group* $\mathfrak{G}$ *is cyclic, then* $\mathfrak{G}$ *is solvable.*

Proof: If $\mathfrak{G}$ is a p-group then the theorem is clearly true. Let the number r of different prime factors of $\mathfrak{G}:1$ be greater than 1, and assume that the theorem has been proven for all groups whose order is divisible by at most $r-1$ different primes. Let p be the smallest prime factor of $\mathfrak{G}:1$. Since a Sylow p-group is cyclic, the index of its normalizer over its centralizer is a divisor of $p-1$; therefore by the construction of p, there is a Sylow p-group in the center of its normalizer. By Burnside's theorem, $\mathfrak{G}$ contains a normal subgroup $\mathfrak{N}$ with the Sylow p-group as a system of representatives; and we can apply the induction hypothesis to $\mathfrak{N}$. This shows that $\mathfrak{N}$ is solvable, and therefore $\mathfrak{G}$ is solvable, Q.E.D.

THEOREM 11: *A finite group of order* N *containing only cyclic Sylow groups is metacyclic and has two generators* A, B *with the defining relations:*

a) $A^m = e,\ B^n = e,\ BAB^{-1} = A^r$, *and the conditions*

b) $0 < m,\ mn = N,$

c) $((r-1)\cdot n, m) = 1,$

d) $r^n \equiv 1\,(m)$, *and conversely.*

Proof: The conditions imposed on $\mathfrak{G}$ also hold for every subgroup and every factor group of a subgroup. If $\mathfrak{G}$ is abelian, then $\mathfrak{G}$ is cyclic. It follows from Theorem 9 that $\mathfrak{G}$ is metacyclic in any case. Let A be a generating element of the commutator group $\mathfrak{G}'$, of order m. Let $B\mathfrak{G}'$ be a generating coset of the factor commutator group, of order n. Then $BAB^{-1} = A^r$, $B^nAB^{-n} = A^{r^n} = A$, and therefore $r^n \equiv 1\ (m)$. Every commutator is a power of $BAB^{-1}A^{-1} = A^{r-1}$, and therefore $(r\text{-}1, m) = 1$. Since B^n is a power of A which commutes with B, we have $B^n = e$. If a prime p were to divide n and m, then $\left\{B^{\frac{n}{p}}, A^{\frac{m}{p}}\right\}$ would be a non-cyclic subgroup of order p^2 and this contradicts the hypothesis; and therefore $(n, m) = 1$.

Conversely, let $\mathfrak{G}$ be a group with generators A and B which satisfy the defining relations a) and conditions b), c), d). By Hölder's theorem in Chapter III, $\mathfrak{G}$ is of order nm. Since $(r\text{-}1, m) = 1$, $\mathfrak{G}' = (A)$. Since $(n, m) = 1$ and the order N of $\mathfrak{G}$ is nm, then for every Sylow group, there is one conjugate to it in (A) or in (B). Therefore every Sylow group of $\mathfrak{G}$ is cyclic, Q.E.D.

§ 4. The Principal Ideal Theorem

First we shall present some considerations about operator domains of abelian groups in pursuance of Chapter III. §§ 3 and 5.

Let $\mathfrak{F}$ be a group of automorphisms $U \to U^\sigma$ of the abelian group $\mathfrak{U}$ with a finite number of generators. All operators $\sum_\sigma c_\sigma \sigma$, with rational integral coefficients c_σ, only a finite number of which are different from zero, form an operator ring Ω with a unit element. Let $\mathfrak{F}_0$ be a normal subgroup of $\mathfrak{F}$ and let $\sigma \to \bar{\sigma}$ be a representation function of $\mathfrak{F}$ over $\mathfrak{F}_0$. Now what does calculation mod $\mathfrak{F}_0$ (i.e., the replacement of σ by $\bar{\sigma}$) mean in Ω? Certain elements in $\mathfrak{U}$ are identified; thus

$$U^\sigma \equiv U^{\sigma'}, \text{ if } \sigma \equiv \sigma' (\mathfrak{F}_0).$$

Instead of calculating in $\mathfrak{U}$, we must now calculate in the factor group of $\mathfrak{U}$ over a subgroup $\mathfrak{U}_0$, where $\mathfrak{U}_0$ must contain at least all $U^{\sigma-\sigma'}$ for $\sigma \equiv \sigma' (\mathfrak{F}_0)$. But all $U^{\sigma-\sigma'}$ with $\sigma \equiv \sigma' (\mathfrak{F}_0)$ generate a subgroup $\mathfrak{U}_0$ *of* $\mathfrak{U}$ *which is admissible with respect to* Ω. *The automorphisms* σ induce automorphisms $\bar{\sigma}$ of $\mathfrak{U}/\mathfrak{U}_0$, and the operator ring Ω goes over into an operator ring $\bar{\Omega}$ of $\mathfrak{U}/\mathfrak{U}_0$.

The order ideal of $\mathfrak{U}/\mathfrak{U}_0$ *over* $\bar{\Omega}$ *is obtained from the order ideal of* $\mathfrak{U}$ *over* Ω *by replacing* σ *by* $\bar{\sigma}$ *everywhere.*

In order to construct the group transferred into the normal subgroup $\mathfrak{U}$, it suffices to calculate in the factor group over $\mathfrak{U}'$, since $\mathfrak{U}'$ is a normal subgroup of $\mathfrak{G}$; thus we assume that $\mathfrak{U}' = e$.

Let $\mathfrak{G}/\mathfrak{U}$ be isomorphic to the abstract group $\mathfrak{F} = \{1, \sigma, \tau, \ldots\}$ and let $(S_\sigma, C_{\sigma,\tau})$ be a factor system of $\mathfrak{G}$ over $\mathfrak{U}$:

$$S_\sigma S_\tau = C_{\sigma,\tau} S_{\sigma\tau}.$$

Every element S in $\mathfrak{G}$ is uniquely of the form $S = U S_\tau$ with $U \in \mathfrak{U}$; therefore, using the earlier notation, we form

$$V_{\mathfrak{G}\to\mathfrak{U}}(U) = \prod_\sigma S_\sigma U \overline{S_\sigma U}^{-1} = \prod_\sigma S_\sigma U S_\sigma^{-1} = U^{\sum\sigma},$$

$$V_{\mathfrak{G}\to\mathfrak{U}}(S_\tau) = \prod_\sigma S_\sigma S_\tau \overline{S_\sigma S_\tau}^{-1} = \prod_\sigma S_\sigma S_\tau S_{\sigma\tau}^{-1} = \prod_\sigma C_{\sigma,\tau},$$

so that

$$V_{\mathfrak{G}\to\mathfrak{U}}(S) = U^{\sum\sigma} \cdot \prod_\sigma C_{\sigma,\tau}.$$

Let $\mathfrak{G}$ be the splitting group (constructed as in Chap. III, § 9) of $\mathfrak{G}$ over the abelian normal subgroup $\mathfrak{U}$; the new normal subgroup $\bar{\mathfrak{U}}$ is

the direct product of $\mathfrak{U}$ with the infinite cyclic groups (A_σ), $\sigma \neq 1$, and

$$A_\tau^\sigma = A_\sigma^{-1} A_{\sigma\tau} C_{\sigma,\tau}^{-1}. \tag{1}$$

For $\bar{\mathfrak{G}}$ over $\bar{\mathfrak{U}}$ there is a splitting factor system $(T_\sigma, 1)$, where $T_\sigma = A_\sigma S_\sigma$. Therefore

$$V_{\mathfrak{G}\to\mathfrak{U}}(S) = V_{\bar{\mathfrak{G}}\to\bar{\mathfrak{U}}}(S) = \bar{U}_\sigma^{\sum\sigma} \cdot \prod 1 = \bar{U}_\sigma^{\sum\sigma}$$

$$V_{\mathfrak{G}\to\mathfrak{U}}(\mathfrak{G}) \leq \bar{\mathfrak{U}}^{\sum\sigma}. \tag{2}$$

THEOREM 12 (PRINCIPAL IDEAL THEOREM)[1]: *The transfer of a group with a finite factor commutator group into its commutator group is equal to the second commutator group provided the second factor commutator group has a finite number of generators.*

As before we can assume in the proof that $\mathfrak{G}'' = e$. Then it remains to show that $V_{\mathfrak{G}\to\mathfrak{G}'}(\mathfrak{G}) = e$.

The following example shows that the assumption about $\mathfrak{G}'$ is necessary:

Let $\mathfrak{U}$ be the group of all numbers $e^{2\pi i r}$ with rational r, and let $\mathfrak{G} = \{\mathfrak{U}, \mathfrak{j}\}$ be the extension over $\mathfrak{U}$ of index 2 defined by

$$\mathfrak{j}^2 = e^{\pi i} = -1$$

$$\mathfrak{j} e^{2\pi i r} \mathfrak{j}^{-1} = e^{-2\pi i r}.$$

Then $\mathfrak{G}' = \mathfrak{U}$ and $\mathfrak{G}'' = e$ but

$$V_{\mathfrak{G}\to\mathfrak{G}'}(\mathfrak{j}) = -1 \neq e.$$

Instead of the principal ideal theorem, we prove the following slight generalization:

Under the same assumptions, the $(\mathfrak{U}:\mathfrak{G}')$-th power of the transfer of every element G in $\mathfrak{G}$ into an abelian group $\mathfrak{U}$ lying between $\mathfrak{G}$ and $\mathfrak{G}'$ is equal to e: i.e., $(V_{\mathfrak{G}\to\mathfrak{U}}(\mathfrak{G}))^{\mathfrak{U}:\mathfrak{G}'} = e$.

We set $\mathfrak{G}:\mathfrak{U} = n$, $\mathfrak{U}:\mathfrak{G}' = d$; n and d are different from zero; $\mathfrak{U}$ is an abelian normal subgroup of $\mathfrak{G}$. Let $\mathfrak{F}$, $\bar{\mathfrak{G}}$ and $\bar{\mathfrak{U}}$ have the same meaning as previously. By (2) it then suffices to prove

$$\bar{\mathfrak{U}}^{d\sum\sigma} = e$$

The automorphisms corresponding to σ generate an operator ring Ω of $\bar{\mathfrak{U}}$, which consists of all $\Theta = \sum_\sigma c_\sigma \sigma$ with integral rational c_σ. $\bar{\mathfrak{U}}$ has an order ideal over Ω, since $\mathfrak{G}'$ has a finite number of generators,

[1] The Principal Ideal Theorem of class field theory states that every ideal of an algebraic number field is a principal ideal in the absolute class field. The principal ideal theorem can be stated group-theoretically as Theorem 12.

$\mathfrak{U}$ is finite over $\mathfrak{G}'$, and $\bar{\mathfrak{U}}$ has a finite number of generators A_σ over $\mathfrak{U}$, so that $\bar{\mathfrak{U}}$ has a finite number of generators, hence a finite number of generators over Ω.

If we now show that $d \cdot \sum_\sigma \sigma$ generates the order ideal of $\bar{\mathfrak{U}}$ over Ω, then the theorem is proven. Now let $\Theta = \sum_\sigma c_\sigma \sigma$ be in the Ω-order ideal of $\bar{\mathfrak{U}}$. Then taking note of (1) we have:

$$e = A_\tau^{\Theta} = A_\tau^{\sum c_\sigma \sigma} = \prod_\sigma (A_\tau^\sigma)^{c_\sigma} \equiv \prod_\sigma A_\sigma^{-c_\sigma} A_{\sigma\tau}^{c_\sigma} (\mathfrak{U})$$

$$\equiv \prod_\sigma A_\sigma^{-c_\sigma + c_{\sigma\tau^{-1}}} (\mathfrak{U}).$$

Since the A_σ form a basis for $\bar{\mathfrak{U}}/\mathfrak{U}$, we must have $c_\sigma = c_{\sigma\tau^{-1}}$ for all $\sigma \neq 1$, hence $c_\sigma = c_1$ for all σ, whence $\Theta = c_1 \cdot \sum_\sigma \sigma$. Consequently, the order ideal of $\bar{\mathfrak{U}}$ over Ω is a principal ideal which is generated by $c \cdot \sum_\sigma \sigma$ with an integral rational $c \geqq 0$.

If we replace σ by 1, then, as was pointed out at the beginning of the paragraph, we are calculating in the group $\bar{\mathfrak{U}}/\bar{\mathfrak{G}}'$; for since $\bar{\mathfrak{G}}$ is generated by the $\bar{U}$ and the T_σ, $\bar{\mathfrak{G}}'$ is generated by all the elements $\bar{U} T_\sigma \bar{U}^{-1} T_\sigma^{-1} = \bar{U}^{1-\sigma}$, i.e. $\bar{\mathfrak{U}}^{1-\sigma} = \bar{\mathfrak{G}}'$. Here Ω goes over into the ring Ω_0 of rational integers. The Ω_0 order ideal of $\bar{\mathfrak{U}}/\bar{\mathfrak{G}}'$ is obtained from the Ω-order ideal of $\bar{\mathfrak{U}}$ by the same substitution; on the other hand, by Chap. III, § 5, it is generated by the group order $\bar{\mathfrak{U}} : \bar{\mathfrak{G}}'$. Therefore

$$\bar{\mathfrak{U}} : \bar{\mathfrak{G}}' = c \cdot (1 + 1 + \cdots + 1) = cn.$$

In order to show that $c = d$, we prove the isomorphism

$$\bar{\mathfrak{U}}/\bar{\mathfrak{G}}' \simeq \mathfrak{G}/\mathfrak{G}',$$

from which it follows that

$$cn = \bar{\mathfrak{U}} : \bar{\mathfrak{G}}' = \mathfrak{G} : \mathfrak{G}' = dn,$$

$$c = d.$$

Since $\mathfrak{G}'$ is a normal subgroup of each of the four groups, we may set $\mathfrak{G}' = e$ for the proof of the isomorphy. Since 1) $\bar{\mathfrak{G}}' = \bar{\mathfrak{U}}^{1-\sigma}$, 2) $\bar{\mathfrak{U}}$ is generated by $\mathfrak{U}$ and the A_τ, and moreover 3) $\mathfrak{U}^{1-\sigma} = e$, it now follows by (1) that

$$\bar{\mathfrak{G}}' = \{A_\tau^{1-\sigma}\} = \{A_\tau C_{\sigma,\tau} A_{\sigma\tau}^{-1} A_\sigma\}.$$

Therefore we can choose the elements $A_\sigma U$ as representatives of $\overline{\mathfrak{U}}/\overline{\mathfrak{G}}'$. By (1)

$$A_\sigma A_\tau = A_{\sigma\tau} C_{\sigma,\tau}^{-1} A_\tau^{1-\sigma} \equiv A_{\sigma\tau} C_{\sigma,\tau}^{-1} \ (\overline{\mathfrak{G}}').$$

The abelian group $\mathfrak{G}$ consists of the elements $S_\sigma^{-1} U$ with the calculational rule

$$S_\sigma^{-1} S_\tau^{-1} = S_{\sigma\tau}^{-1} C_{\sigma,\tau}^{-1}.$$

The correspondence $A_\sigma U \to S_\sigma^{-1} U$ therefore gives an isomorphism between $\overline{\mathfrak{U}}/\overline{\mathfrak{G}}'$ and $\mathfrak{G}$, Q.E.D.

COROLLARY OF THE PRINCIPAL IDEAL THEOREM: In a 2-step metabelian group with a finite number of generators and cyclic factor commutator group of order n, every element whose coset generates the factor commutator group is of order n.

Proof: If S is the element described in the above statement, then $\mathfrak{G}/\mathfrak{G}' = (S\mathfrak{G}')$ and therefore the powers $1, S, \ldots, S^{n-1}$ are a system of representatives of $\mathfrak{G}$ over $\mathfrak{G}'$. Consequently

$$V_{\mathfrak{G}\to\mathfrak{G}'}(S) = \prod_{\nu=0}^{n-1} S^\nu S \overline{S^{\nu+1}-1} = S^n,$$

while on the other hand $V_{\mathfrak{G}\to\mathfrak{G}'}(S) = e$.

FREQUENTLY USED SYMBOLS

$\mathfrak{G}$ — GROUP (p. 1)

$\mathfrak{U}$ — SUBGROUP (p. 10)

$\mathfrak{G} : \mathfrak{U}$ — INDEX of $\mathfrak{G}$ with respect to $\mathfrak{U}$ = number of left (right) cosets (p. 10)

$\mathfrak{K}$ — COMPLEX = subset of a group (p. 19)

$\mathfrak{K}^x$ — Complex transformed by x = set of all xKx^{-1} (p. 25)

$N_{\mathfrak{K}}$ — NORMALIZER of $\mathfrak{K}$ = group of all x which transform $\mathfrak{K}$ into itself (p. 26)

$Z_{\mathfrak{K}}$ — CENTRALIZER of $\mathfrak{K}$ = group of all x which are permutable with every element of $\mathfrak{K}$ (p. 46)

$\mathfrak{N}$ — NORMAL SUBGROUP = subgroup which is transformed into itself by all elements (p. 23)

$\mathfrak{G}/\mathfrak{N}$ — FACTOR GROUP of $\mathfrak{G}$ over $\mathfrak{N}$ = group of cosets of $\mathfrak{G}$ by $\mathfrak{N}$ (p. 34)

$\mathfrak{z}$ — CENTER OF $\mathfrak{G}$ = group of all elements commuting with every element of $\mathfrak{G}$ (p. 27)

$J_{\mathfrak{G}}$ — Group of all INNER AUTOMORPHISMS (transformations) of $\mathfrak{G}$ (p. 44)

$A_{\mathfrak{G}}$ — Group of all AUTOMORPHISMS of $\mathfrak{G}$ (p. 44)

A/J — Group of OUTER AUTOMORPHISMS of $\mathfrak{G}$ (p. 44)

Φ — A subgroup of $\mathfrak{G}$ = intersection of $\mathfrak{G}$ with its maximal subgroups (p. 47)

$(a, b) = a\,b\,a^{-1}b^{-1}$ — COMMUTATOR of a with b (p. 58)

$(a, b, c) = (a, (b, c))$ (p. 61)

$(\mathfrak{U}, \mathfrak{V})$ — mutual COMMUTATOR GROUP = group of all (U, V) (p. 61)

$\mathfrak{G}' = D\,\mathfrak{G} = (\mathfrak{G}, \mathfrak{G})$ — COMMUTATOR GROUP of $\mathfrak{G}$ (p. 58)

$\mathfrak{G}/\mathfrak{G}'$ — FACTOR COMMUTATOR GROUP (p. 58)

$D^i\,\mathfrak{G} = D\,(D^{i-1}\mathfrak{G})$ — i-TH DERIVATIVE of $\mathfrak{G}$ (p. 59)

k — degree of METABELIAN group $\mathfrak{G}$, so that $D^{k-1}\mathfrak{G} \neq D^k\mathfrak{G} = e$ (p. 59)

$\mathfrak{G} = \mathfrak{Z}_1 \supseteq \mathfrak{Z}_2 \supseteq \mathfrak{Z}_3 \ldots$ — DESCENDING CENTRAL SERIES (p. 125) so that

$\mathfrak{Z}_i = (\mathfrak{G}, \mathfrak{Z}_{i-1})$ is the i-th Reidemeister commutator group

$e = \mathfrak{z}_0 \subseteq \mathfrak{z}_1 \subseteq \mathfrak{z}_2 \ldots$ ascending central series (p. 46), so that

$\mathfrak{z}_i$ is the i-th center of $\mathfrak{G}$, hence $\mathfrak{z}_i/\mathfrak{z}_{i-1}$ is the center of $\mathfrak{G}/\mathfrak{z}_{i-1}$

c — Class of the nilpotent group $\mathfrak{G}$, hence $\mathfrak{z}_{c-1} \neq \mathfrak{z}_c = \mathfrak{G}$ and $\mathfrak{Z}_c \neq \mathfrak{Z}_{c+1} = e$

S_p — is a SYLOW p-GROUP of $\mathfrak{G}$ (p. 105)

N_p — Normalizer of S_p (p. 105)

z_p — Center of S_p (p. 105)

$d(\mathfrak{G})$ — The minimal number of independent generators of $\mathfrak{G}$ (p. 111)

$k_d = (p^d - 1)\,(p^{d-1} - 1) \ldots (p - 1)$ (p. 112)

$\mathfrak{G}'(p)$ — p-commutator group = intersection of all normal subgroups with abelian p-factor group (p. 128)

$\mathfrak{G}/\mathfrak{G}'(p)$ — p-factor commutator group = maximal abelian p-factor group (p. 128)

$\mathfrak{D}_p$ — Intersection of all normal subgroups with index a power of p (p. 129)

$\mathfrak{G}/\mathfrak{D}_p$ — Maximal p-factor group (p. 129)

$\in$ — $x \in \mathfrak{G}$ means: x is an element of $\mathfrak{G}$

$\subset$ — $\mathfrak{U} \subset \mathfrak{G}$ means: $\mathfrak{U}$ is a proper subgroup of $\mathfrak{G}$

$\cup$ — $\mathfrak{U} \cup \mathfrak{V}$ is the sum of the sets $\mathfrak{U}$ and $\mathfrak{V}$

$\cap$ — $\mathfrak{U} \cap \mathfrak{V}$ is the intersection of $\mathfrak{U}$ and $\mathfrak{V}$.

BIBLIOGRAPHY

Any one who is interested in obtaining a view of the entire field of group theory should consult the article by Wilhelm Magnus "Allgemeine Gruppentheorie" which appears in the *Enzyklopädie der Mathematischen Wissenschaften,* Band I, 1. Heft 4, Teil 1, No. 9, pp. 1-51, 1939. The article written for the earlier edition of the *Enzyklopädie* by Burkhardt (IA. 6, pp. 208-226) is also of interest. Both of these articles contain generous bibliographies.

Texts on Group Theory

English

BIRKHOFF and MACLANE. *A Survey of Modern Algebra,* New York, 1941.

BURNSIDE, W. *Theory of Groups of Finite Order,* Cambridge, 1897. Second edition, 1911.

CARMICHAEL, R. D. *Introduction to the Theory of Groups of Finite Order,* Boston, 1937.

HILTON, H. *An Introduction to the Theory of Groups of Finite Order,* Oxford, 1908.

LEDERMAN, W. *Introduction to the Theory of Finite Groups,* New York, 1949.

MATHEWSON, L. C. *Elementary Theory of Finite Groups,* Boston, 1930.

MILLER, BLICHFELDT and DICKSON. *Theory and Application of Finite Groups,* New York 1916. Second edition, 1938.

VAN DER WAERDEN, B. L. *Modern Algebra* I, New York, 1949. (English translation of *Moderne Algebra* I.)

German

BAUMGARTNER, L. *Gruppentheorie,* Berlin, 1921 (Sammlung Göschen No. 837).

SPEISER, A. *Die Theorie der Gruppen von endlicher Ordnung,* Berlin, 1937, also New York, 1945.

VAN DER WAERDEN, B. L. *Moderne Algebra* I. 3rd ed. Berlin, 1937.

French

DUBREIL, P. *Algèbre,* Paris, 1946.

GALOIS, E. *Oeuvres mathématiques,* Paris, 1897, pp. 25-61.

JORDAN, C. *Traité des substitutions,* Paris, 1870.

DE SEGUIER, J. A. *Théorie des groupes finis.* Vol. I, Paris, 1904. Vol. II, Paris, 1912.

SERRET, J. A. *Cours d'algèbre supérieure.* Vol. II, Paris, 7th ed. 1928.

Russian

GRAVE, P. A. *Theory of Finite Groups,* Kiew 1908.

SCHMIDT, O. J. *Abstract Group Theory,* Kiew 1916. 2nd ed. 1933.

KUROSH, A. G. *Theory of Groups* (Teoriya Grupp.), Moscow-Leningrad, 1944. (English translation in preparation by *Chelsea Publishing Company*).

Japanese

SONO, S. *Group Theory,* Tokyo, 1928.

Another general reference should be mentioned: the two volumes of G. A. MILLER *Collected Works,* University of Illinois Press, 1934. The remaining references are not general but are either direct sources or amplifications of the topics taken up in this book. They are listed according to chapter and section.

CHAPTER I

§ 1. P. LORENZEN. *Ein Beitrag zur Gruppenaxiomatik.* Math. Zeit. 49 (1944) p. 313-327.

K. PRACHAR. *Zur Axiomatik der Gruppen.* Akad. Wiss. Wien. S-B IIa. 155 (1947) p. 97-102.

§ 10. G. FROBENIUS. *Über einen Fundamentalsatz der Gruppentheorie.* Berl. Sitz. 1903 p. 987, and 1907 p. 428.

P. DUBUQUE. *Une généralisation des théorèmes de Frobenius et Weisner.* Rec. Math. (Moscow) 5(47) (1939) p. 189-196.

C. S. FU. *On Frobenius' theorem.* Quart. J. Math. Oxford. Ser. 1. 17 (1946) p. 253-256.

B. A. KRUTIK. *Über einige Eigenschaften der endlichen Gruppen.* Rec. Math. (Math. Sbornik) N. S. 0152 (1942) p. 239-247.

S. LUBELSKI. *Verallgemeinerung eines Frobeniusschen gruppentheoretischen Satzes.* Act. Acad. Lima 6 (1945) p. 133-137.

CHAPTER II

§ 4. Definition and discussion of the principal properties of the Φ-subgroup from Frattini. See: Miller, Blichfeldt, Dickson, *op. cit.* p. 52. Also see: B. NEUMANN, *Some remarks on infinite groups.* Lond. Math. Soc. 12 (1937), and O. ORE, *Contributions to the theory of groups of finite order.* Duke Math. J. 5 (1934) p. 431-460.

Paper on the holomorph of a group: GARRETT BIRKHOFF. A theorem on transitive groups. Proc. Camb. Phil. Soc. 29 (1933) p. 257-259.

§ 5. The Jordan-Hölder Theorem: C. JORDAN. Journal de math. (2) 14 (1869) p. 139, shows that the orders of the factors in different composition series are the same.

O. HÖLDER, Math. Ann. 34 (1889) shows that the composition factors of a finite group are unique up to order in the sense of isomorphism.

SCHREIER. *Über den Jordan-Hölderschen Satz.* Hamb. Abh. 6 p. 300, gives the definition of refinement and the refinement theorem.

H. ZASSENHAUS. *Zum Satz von Jordan-Hölder-Schreier.* Hamb. Abh. 10:106. gives the explicit procedure for obtaining refinements with the theorem on four groups.

O. ORE. *Structures and group theory.* Duke Math. Journal, Part I, Vol. 3, p. 149-174, and Part II, Vol. 4, p. 247-269, give the general structure theory.

A. KUROSH. Composition systems in infinite groups. Rec. Math. (Mat. Sbornik) N. S. 16 (58), p. 59-72 (1945).

§ 6. The definition of commutator form and the theorems come from P. HALL. *A contribution to the theory of groups of prime-power orders.* Proc. Lond. Math. Soc. II 36 (1933) p. 29-95.

R. BAER. The higher commutator subgroups of a group. Bull. Amer. Math. Soc. 50 (1944) p. 143-160.

For the extension of the notion of solvability to the infinite case see: R. BAER. *Nilpotent groups and their generalizations.* Trans. Amer. Math. Soc. 47 (1940) p. 393-434.

H. FITTING. In the Jahr. Deutsch. Math. Verein. 48 (1938) p. 77-141.

K. A. HIRSH. *On infinite solvable groups.* Proc. Lond. Math. Soc. (2), Part I, 44 (1938) p. 53-60; Part II, 44 (1938) p. 336-344; Part III, 49 (1946) p. 184-194.

P. HALL. *The construction of soluble groups.* J. Reine Angew. Math. 182, p. 206-214 (1940).

W. MAGNUS. *Neuere Ergebnisse über auflösbare Gruppen.* Jahr. D. Math. Verein. 47 (1937), p. 69-78.

O. SCHMIDT. *Infinite solvable groups.* Rec. Math. (Mat. Sb) N. S. 17 (59) (1945), p. 363-375.

§ 7. Theorem 16: E. WITT, *Über die Kommutativität endlicher Schiefkörper.* Hamb. Abh. 8 (1931), p. 413.

Almost fields: ZASSENHAUS, *Über endliche Fastkörper.* Hamb. Abh. 11, p. 187-220.

Rings of matrices: N. JACOBSON, *The Theory of Rings.* Math. Surveys 2, Amer. Math. Soc. (1943). See especially the bibliography.

CHAPTER III

§ 2. See the paper of Fitting cited in the footnote.

F. KIOKEMEISTER. *A note on the Schmidt-Remak Theorem.* Bull. Amer. Math. Soc. 53 (1947) p.957-958.

O. ORE. *A remark on the normal decompositions of groups.* Duke Math. J. 5 (1939) p. 172-173.

§§ 3-5. IYANAGA. *Zum Beweis des Hauptidealsatzes.* Hamb. Abh. 10 (1934).

§§ 6-8. SCHREIER. *Über die Erweiterung von Gruppen.* Teil I: Monatshefte für Math. u. Phys., Bd. 34. Teil II: Hamb. Abh. 4, p. 321.

R. BAER. *Erweiterung von Gruppen und ihren Isomorphismen.* Math. Zeit. 38 (1934) p. 375-416. *Groups with abelian central quotient group.*

Trans. Amer. Math. Soc. 44 (1938) p. 357-386.

Y. A. GOL'FAND. *On an isomorphism between extensions of groups.* Doklady Ak. Nauk. S.S.S.R. (N. S.) 60, 1123-1125 (1948).

S. EILENBERG and S. MACLANE. *Group extensions and homology.* Ann. of Math. (2) 43 (1942) p. 757-831. *Cohomology theory in abstract groups.* I. Ann. of Math. (2) 48 (1947) p. 51-78. II. (Group extensions with a non-abelian kernel) Ann. of Math. (2) 48 (1947) p. 326-341.

B. H. NEUMANN. *Adjunction of elements to groups.* J. Lond. Math. Soc. 18 (1943) p. 4-11.

K. SHODA. *Über die Schreiersche Erweiterungstheorie.* Proc. Imp. Acad. Tokyo 19 (1943) p. 518-519.

§ 9. See IYANAGA. *op. cit.*

CHAPTER IV

Theorem 13: WIELAND. Math. Zeit. 41 (1936).

§ 1. R. BAER. *Sylow theorems for infinite groups.* Duke Math. J. 6 (1940) p. 598-614.

A. P. DIETZMAN (Dicman). *On an extension of Sylow's theorem.* Ann. of Math. (2) 48 (1947) p. 137-146. And *On Sylow's theorem*: Doklady Akad. Nauk S.S.S.R. (N. S.) 59 (1948), p. 1235-1236.

P. GOLDBERG. The Silov p-groups of locally normal groups. Rec. Math. (Math Sbornik) N. S. 19 (61) (1946) p. 451-460.

H. WIELANDT. *p-Sylowgruppen und p-Faktorgruppen.* J. Reine Angew. Math. 182 (1940), p. 180-193.

§ 3. See Baer reference under II, 6. Also Fitting and P. Hall.

O. SCHMIDT. Über unendliche spezielle Gruppen. Rec. Math. (Mat. Sbornik) N. S. 8 (59) (1940) p. 363-375.

§§ 4-5. See first cited paper of P. Hall.

CHAPTER V

§ 1. G. HANNINK. *Verlagerung und Nichteinfachheit von Gruppen.* Monatsh. Math. Phys. 50 (1942) p. 207-233.

§ 2. O. GRÜN. *Beiträge zur Gruppentheorie.* I. Crelle (1935) 1.

§ 3. ZASSENHAUS. *Über endliche Fastkörper, op. cit.*

§ 4. IYANAGA. *op. cit.*

E. WITT. *Bemerkungen zum Beweis des Hauptidealsatzes von S. Iyanaga.* Hamb. Abh. 11 p. 221.

AUTHOR INDEX

INDEX