DETERMINATION OF A CERTAIN FAMILY OF FINITE METABELIAN GROUPS

BY

G. SZEKERES

Introduction. The problem of constructing all the finite metabelian groups (that is, groups with an abelian commutator subgroup) is fundamentally settled by the Schreier theory of group extensions. In fact, a metabelian group may be considered as the extension of an abelian group $\mathfrak{A}$ by an abelian group $\mathfrak{F}$; this is the simplest nontrivial case of a group extension. According to Schreier's theory, an arbitrary group $\mathfrak{G}$ which is the extension of $\mathfrak{A}$ by $\mathfrak{F}$ is obtained by the following procedure:

First, we have to find an automorphism group of $\mathfrak{A}$ which is the homomorphic image of $\mathfrak{F}$, that is, if $\bar{\sigma}$ is the automorphism corresponding to $\sigma \in \mathfrak{F}$, then $(AB)^{\bar{\sigma}} = A^{\bar{\sigma}}B^{\bar{\sigma}}$, $(A^{\bar{\tau}})^{\bar{\sigma}} = A^{\bar{\sigma}\bar{\tau}} = A^{\overline{\sigma\tau}}$ for every $A, B \in \mathfrak{A}$, $\sigma, \tau \in \mathfrak{F}$. Secondly, we have to find a factor system $C_{\sigma,\tau}$ in A, satisfying $C_{\sigma,\tau}C_{\sigma\tau,\rho} = C_{\tau,\rho}^{\bar{\sigma}}C_{\sigma,\tau\rho}$ for every ρ, σ, τ (see [18, p. 90])(1). If S_σ is a symbol denoting a certain representative of σ in $\mathfrak{G}$, then the relations $S_\sigma A S_\sigma^{-1} = A^{\bar{\sigma}}$, $S_\sigma S_\tau = C_{\sigma,\tau}S_{\sigma\tau}$ uniquely determine an abstract group $\mathfrak{G}$ with the required properties.

Unfortunately, the general formulation of the Schreier theory does not indicate (except in the most trivial cases) how to determine and specify the automorphisms and factor systems so that each $\mathfrak{G}$ shall be obtained in *one and only one* way. The invariant characterization of solvable groups, even in the relatively simple case of metabelian groups, still remains one of the most important and most difficult problems of abstract group theory. At the present, it seems that the problem can be successfully approached only if we impose certain restrictions upon the family of groups to be determined. In a recent paper [12] I have determined all the groups $\mathfrak{G}$ which have an abelian invariant subgroup $\mathfrak{A}$ of the type $(p, \cdots, p)$ such that $\mathfrak{G}/\mathfrak{A}$ be cyclic. In the present paper a more extensive class of metabelian groups will be determined and completely characterized by numerical invariants. Whereas no restriction will be imposed upon the structure of the abelian invariant subgroup $\mathfrak{A}$, it is assumed that $\mathfrak{G}/\mathfrak{A}$ is cyclic and its order n is not divisible by the square of any prime number which divides the order of $\mathfrak{A}$. In particular, the latter condition is fulfilled if either n is squarefree, or if n and the order of $\mathfrak{A}$ are relatively prime.

Among the more important cases included in the above category (others will be mentioned in part 3) perhaps the most notable is the case of p-groups

Presented to the Society, April 30, 1949; received by the editors December 22, 1947, and, in revised form, January 21, 1949.

(1) Numbers in brackets refer to the bibliography at the end of the paper.

which contain an abelian subgroup of index p. These have been determined if the abelian subgroup is of the type $(p, \cdots, p)$ [9], or cyclic [3, p. 134], or of the type (p^{n-1}, p) [8], or if the group is of order p^n, $n \leqq 5$ [1, 2], or of class $n-1$ [17]. Recently P. Hall [6] introduced a general classification of p-groups by means of a relation called isoclinism, and determined the families of isoclinic p-groups containing abelian subgroups of index p. This is still not a solution of the structure problem, since there are too many different groups which belong to the same family of isoclinic groups (for example all the abelian p-groups belong to the same family). The present paper contains for the first time a complete enumeration of these groups.

Some general remarks about notations:

Groups and rings will be denoted by German letters, elements of additive groups by *Roman* capitals. Greek letters will denote elements of rings or multiplicative groups which act as operators on abelian groups.

$\{A, B, \cdots\}$ is the subgroup generated by the elements in brackets, or in the case of abelian operator groups the smallest admissible subgroup containing $A, B, \cdots$. $A \oplus B$ is the direct sum of A, B.

$\mathfrak{G}$ shall denote a group which has an invariant commutative subgroup with cyclic quotient group of order n. The following procedure, a modification of the Schreier principle, will be used to construct an arbitrary $\mathfrak{G}$:

Let $\mathfrak{Z}[x]$ denote the ring of polynomials in x with integral coefficients and $\overline{\mathfrak{R}}_{n,h}[x]$ the (finite) quotient ring $\mathfrak{Z}[x]/(x^n-1, h)$. The abelian group $\mathfrak{A}$ of order h is assumed to possess a ring of of endomorphisms $\mathfrak{R}$ which is a homomorphic image of $\overline{\mathfrak{R}}_{n,h}[x]$. We write $\mathfrak{A}$ additively with unit element 0 and denote by ρA the endomorphism induced by the operator $\rho \in \mathfrak{R}$ on $A \in \mathfrak{A}$. Let $\sigma \in \mathfrak{R}$ be the operator which corresponds to x by the homomorphism $\overline{\mathfrak{R}}_{n,h}[x] \to \mathfrak{R}$. Then by the definition of $\overline{\mathfrak{R}}_{n,h}[x]$, σ^n is the unit automorphism of $\mathfrak{A}$, that is, $\sigma^n A = A$ for every $A \in \mathfrak{A}$.

We now define a set of symbols (r, A), $r \geqq 0$, $A \in \mathfrak{A}$ as the elements of an abstract group $\mathfrak{G}$ under the following rules of composition:

$$(r_1, A_1)(r_2, A_2) = (r_1 + r_2, A_1 + \sigma^{r_1} A_2), \tag{1}$$

$$(n, 0) = (0, H) \tag{2}$$

where H is an element of $\mathfrak{A}$ satisfying

$$\sigma H = H. \tag{3}$$

Multiplying both sides of (2) either from the right or from the left by (r, A) we obtain

$$(r + n, A) = (r, A + H) \tag{4}$$

which implies that the elements of $\mathfrak{G}$ can be brought to the form

$$(r, A), \qquad 0 \leqq r < n, \qquad A \in \mathfrak{A}.$$

We have to show that $\mathfrak{G}$ is a group. Clearly, the elements $(0, A)$ form a commutative subgroup $\mathfrak{A}'$ which is isomorphic to $\mathfrak{A}$. Put $S=(1, 0)$, then by (1), (3), (4), $S^r=(r, 0)$, $S^{-r}=(r, 0)^{-1}=(n-r, -H)$, hence $S^r(0, A)S^{-r}=(0, \sigma^r A)$. Thus the transformation of $\mathfrak{A}'$ by S^r induces the automorphism σ^r in $\mathfrak{A}'$. Since $S^n=(0, H)$ by (2) and $(0, \sigma H)=(0, H)$, it follows from Schreier's theorem (see [18, p. 93]) that $\mathfrak{G}$ is a group which contains $\mathfrak{A}'$ as an invariant subgroup. Moreover, $\mathfrak{G}/\mathfrak{A}'$ is cyclic and its order is n. The element $(0, H)$ represents the factor system of the extension.

That every group $\mathfrak{G}$ is obtained by the method just described is again a consequence of Schreier's theorem since σ can be taken as an arbitrary automorphism of order n or a divisor of n. In fact, we can construct $\mathfrak{R}$, the ring of σ-endomorphisms

$$\rho = a_0 + a_1\sigma + \cdots + a_{n-1}\sigma^{n-1}, \qquad a_0, a_1, \cdots, a_{n-1} \text{ integers},$$

in one and only one way so that the binary operation ρA, $\rho \in \mathfrak{R}$, $A \in \mathfrak{A}$, shall satisfy the postulates

$$(5) \qquad \begin{gathered} (\rho_1 + \rho_2)A = \rho_1 A + \rho_2 A, \qquad \rho_1(\rho_2 A) = (\rho_1\rho_2)A, \\ oA = 0, \qquad \iota A = A, \qquad (t\rho)A = \rho(tA). \end{gathered}$$

Here o and ι denote the 0 and 1-element of the ring $\mathfrak{R}$, and t is an integer. The last of the conditions (5) shows that $(h\iota)A = \iota(hA) = 0$ for every A, hence $h\iota = o$. Therefore $(\sigma^n - \iota, h\iota) = \mathfrak{C}$ and $\mathfrak{R}$ is a homomorphic image of $\overline{\mathfrak{R}}_{n,h}[x]$.

The first step in the above procedure of constructing the group $\mathfrak{G}$ is to determine the operator rings $\mathfrak{R}$ of $\mathfrak{A}$ which are the homomorphic images of $\overline{\mathfrak{R}}_{n,h}[x]$. This is equivalent to the problem of determining the automorphisms σ of $\mathfrak{A}$ which satisfy $\sigma^n = \iota$, or rather the classes of automorphisms conjugate to a σ in the group of all the automorphisms of $\mathfrak{A}$. For, if λ is an arbitrary automorphism of $\mathfrak{A}$, then the element λA is carried by σ into $\sigma(\lambda A) = \lambda(\lambda^{-1}\sigma\lambda A)$. This shows that we could equally well arrive at the group $\mathfrak{G}$ by starting from the conjugate automorphism $\sigma' = \lambda^{-1}\sigma\lambda$ instead of σ.

There is, however, another way of approach to the problem which seems to be more natural from the algebraic point of view: Instead of departing from a definite abelian group and determining the above class of conjugate automorphisms, we may regard $\mathfrak{A}$ from the outset as an $\mathfrak{R}$-group (without specifying its structure as an abstract group), and determine the different types of such operator groups. Replacing σ by its conjugate $\lambda^{-1}\sigma\lambda$ implies that we pass to an $\mathfrak{R}$-group A' which is $\mathfrak{R}$-isomorphic to $\mathfrak{A}$. Therefore we have to consider two $\mathfrak{R}$-groups as being of the same type, if they are $\mathfrak{R}$-isomorphic to each other. Here $\mathfrak{R}$-isomorphism is understood in the usual sense; we assume that the same ring of operators $\mathfrak{R}$ acts upon both $\mathfrak{A}$ and $\mathfrak{A}'$.

There is another definition which naturally suggests itself when we investigate the abstract structure of operator groups. Suppose that $\mathfrak{A}$ has an operator ring $\mathfrak{R}$ and $\mathfrak{A}'$ has an operator ring $\mathfrak{R}'$ and there is an isomorphism

(1–1 homomorphism) between $\mathfrak{R}$ and $\mathfrak{R}'$. Then we can define an $(\mathfrak{R}, \mathfrak{R}')$-isomorphism between $\mathfrak{A}$ and $\mathfrak{A}'$ by postulating $\rho A \to \rho' A'$ if $\rho \to \rho'$, $A \to A'$ (see [7, p. 5, footnote]). Of particular interest is the case when $\mathfrak{R}'$ is obtained by means of an automorphism of $\mathfrak{R}$. For example if $(u, n) = 1$, $\sigma' = \sigma^u$ induces an automorphism of $\mathfrak{R}$ by the 1–1 mapping

$$a_0 + a_1\sigma + \cdots + a_{n-1}\sigma^{n-1} \to a_0 + a_1\sigma'^v + \cdots + a_{n-1}\sigma'^{v(n-1)}$$

where $uv \equiv 1 \pmod{n}$, which converts $\mathfrak{A}$ into an $\mathfrak{R}'$-group, $\mathfrak{R}'$ being a polynomial ring of the operator σ'. Such a situation is confronted if we take the coset represented by $S' = (u, 0)$ instead of $S = (1, 0)$ as the generating coset of $\mathfrak{G}/\mathfrak{A}$. The discussion of this situation is left to §2. Until then we consider only ordinary $\mathfrak{R}$-isomorphism, since the solution of the problem of $\mathfrak{R}$-groups takes then a more convenient form.

After we have determined the varous types of $\mathfrak{R}$-groups the next step is to select the element H in a suitable way. We could take for H an arbitrary element satisfying equation (3), but of course the problem is to have a canonical form for H which is an invariant of the group $\mathfrak{G}$.

Finally, we have to settle the following question: It might happen that a group $\mathfrak{G}$ has several different abelian invariant subgroups with cyclic quotient group, hence $\mathfrak{G}$ can be represented in more than one way by a system $[\mathfrak{A}, H]$. Then we must find conditions for the equivalence of two different systems $[\mathfrak{A}, H]$.

In §§1 and 2, we shall have a complete answer to all these questions, provided that (n, h) is squarefree.

1. It will be assumed that the ring $\mathfrak{R}$ is a homomorphic image of $\overline{\mathfrak{R}}_{n,h}[x]$, hence

$$\sigma^n = \iota \tag{1.1}$$

where σ is the operator corresponding to x, and the operators of $\mathfrak{R}$ have the form

$$\rho = a_0 + a_1\sigma + \cdots + a_{n-1}\sigma^{n-1}, \qquad a_i \text{ integral.} \tag{1.2}$$

In order to find the different types of $\mathfrak{R}$-groups, we have to determine the different types of indecomposable $\mathfrak{R}$-groups. For, both $\mathfrak{R}$ and $\mathfrak{A}$ are finite, hence the Krull-Schmidt theorem applies to $\mathfrak{A}$ and the indecomposable components occurring in its direct decomposition are uniquely determined by $\mathfrak{A}$, as far as their types and multiplicities are concerned.

There is a decomposition of $\mathfrak{A}$ that can be accomplished in every case: A finite commutative operator group is the direct sum of its p-primary components $\mathfrak{A}^{(p)}$. Hence we can assume that the order of $\mathfrak{A} = \mathfrak{A}^{(p)}$ is a power of a prime number p, p^l say. Then the operator ring of $\mathfrak{A}^{(p)}$, $\mathfrak{R}_p$, is a homomorphic image of $\overline{\mathfrak{R}}_{n,p^l}[x]$.

In order to obtain a further decomposition of $\mathfrak{A}^{(p)}$, we slightly modify the

ring $\mathfrak{R}_p$. Let A be an element of order p^m, and

$$\alpha = a_0 + a_1 p + a_2 p^2 + \cdots, \qquad 0 \leqq a_i < p,$$

a p-adic integer in the regular representation. We can give the formal product αA a natural significance by requiring that it shall satisfy the following postulates:

$$\begin{gathered} \alpha 0 = 0, \qquad \epsilon A = A \qquad (\epsilon = \text{p-adic identity}), \\ (\alpha_1 + \alpha_2)A = \alpha_1 A + \alpha_2 A, \qquad (\alpha_1 \alpha_2)A = \alpha_1(\alpha_2 A). \end{gathered} \tag{1.3}$$

Notably $(p^m \alpha')A = \alpha'(p^m \epsilon A) = \alpha'(p^m A) = 0$ for any p-adic whole number α', hence

$$\alpha A = \alpha^{(m)} A \tag{1.4}$$

where $\alpha^{(m)} = a_0 + \cdots + a_{m-1} p^{m-1}$ is the mth convergent (in the p-adic sense) of α. Conversely, if αA is defined by (1.4) then the postulates (1.3) are automatically satisfied.

Let $\mathfrak{P}[x]$ denote the ring of polynomials in x with p-adic integral coefficients and write $\overline{\mathfrak{R}}'_{n,p^f}[x] = \mathfrak{P}[x]/(\epsilon x^n - \epsilon, p^f \epsilon)$. Clearly, $\overline{\mathfrak{R}}'_{n,p^f}[x]$ is isomorphic to $\overline{\mathfrak{R}}'_{n,p^f}[x]$ and we can construct an operator ring $\mathfrak{R}'_p$ which is isomorphic to $\mathfrak{R}_p$ by assigning to each operator (1.2) of $\mathfrak{R}_p$ the operator $\rho' = \alpha_0 + \alpha_1 \sigma + \cdots + \alpha_{n-1} \sigma^{n-1}$ in $\mathfrak{R}'_p$, where α_i is the p-adic equivalent of a_i. It follows from (1.4) that $\mathfrak{A}^{(p)}$ can equally well be regarded as an $\mathfrak{R}'_p$-group or as an $\mathfrak{R}_p$-group.

The idea of assigning the p-adic integers as operators to a p-primary group has been variously used for the studying of infinite abelian groups, notably by H. Pruefer, see also H. Rauter [10]. In the case of finite p-primary groups it seemingly does not make any difference whether we take the ordinary integers or the p-adic integers as operators, since the p-adic residues modulo p^f are identical with the residues of ordinary integers modulo p^f. Nevertheless we shall see immediately that the change of $\mathfrak{R}_p$ to $\mathfrak{R}'_p$ has decided advantages since it makes it possible to apply certain well known facts about the reducibility of polynomials over $\mathfrak{P}$ to the further decomposition of $\mathfrak{A}^{(p)}$ into direct summands.

Write

$$n = mp^k, \qquad (m, p) = 1 \tag{1.5}$$

and let

$$x^m - 1 \equiv \bar{\phi}_0 \bar{\phi}_1 \cdots \bar{\phi}_t \pmod{p}, \qquad \phi_0 = x - 1 \tag{1.6}$$

be the factorization of $x^m - 1$ into modulo p irreducible polynomials $\bar{\phi}_r$. These can be normalised by the condition that the highest coefficient of $\bar{\phi}_r$ shall be 1. We have

$$x^n - 1 = x^{mp^k} - 1 \equiv (x^m - 1)^{p^k} \equiv \bar{\phi}_0^{p^k} \cdots \bar{\phi}_t^{p^k} \pmod{p}.$$

By the reducibility criterion of Hensel (see van der Waerden [14] p. 259) there exist uniquely determined polynomials $\phi_0 = x-1, \phi_1, \cdots, \phi_t$ respectively $\Phi_0, \Phi_1, \cdots, \Phi_t$ in $\mathfrak{P}[x]$ such that

$$(1.7)\qquad \begin{aligned} x^m - 1 &= \phi_0\phi_1 \cdots \phi_t, \qquad x^n - 1 = \Phi_0\Phi_1 \cdots \Phi_t, \\ \phi_r &\equiv \bar{\phi}_r \pmod{p}, \qquad \Phi_r \equiv \bar{\phi}_r^{p^k} \pmod{p}, \qquad r = 0, \cdots, t, \end{aligned}$$

where ϕ_r is irreducible in $\mathfrak{P}[x]$(2). Write

$$(1.8)\qquad \psi_r = \Phi_0 \cdots \Phi_{r-1}\Phi_{r+1} \cdots \Phi_t = \frac{1}{\Phi_r}(x^n - 1), \qquad r = 0, \cdots, t.$$

Since $\psi_0, \cdots, \psi_t$ are polynomials with leading coefficient 1 which have no common divisor of degree greater than 0 modulo p, there exist polynomials $\lambda_0, \cdots, \lambda_t$ in $\mathfrak{P}[x]$ such that

$$(1.9)\qquad \lambda_0\psi_0 + \cdots + \lambda_t\psi_t = 1.$$

Let A be an arbitrary element of $\mathfrak{A}^{(p)}$ and write $A_r = \lambda_r(\sigma)\psi_r(\sigma)A$. Then $\Phi_r(\sigma)A_r = \lambda_r\psi_r\Phi_r(\sigma)A = \lambda_r(\sigma)(\sigma^n - 1)A = 0$ by (1.8) and (1.1), and $A = A_0 + \cdots + A_t$ by (1.9). Hence, writing $\mathfrak{A}_r^{(p)} = \lambda_r\psi_r(\sigma)\mathfrak{A}^{(p)}$, we have

$$(1.10)\qquad \Phi_r(\sigma)\mathfrak{A}_r^{(p)} = 0, \qquad r = 0, \cdots, t,$$

and

$$\mathfrak{A}^{(p)} = \mathfrak{A}_0^{(p)} \oplus \cdots \oplus \mathfrak{A}_t^{(p)}.$$

We shall call $\mathfrak{A}_r^{(p)}$ the ϕ_r-component of $\mathfrak{A}^{(p)}$, and say that $\mathfrak{A}_r^{(p)}$ belongs to the irreducible polynomial ϕ_r. This is justified by the following theorem:

THEOREM 1. *Let $\mathfrak{A}_\phi$ belong to $\phi = \phi_r$, hence, by* (1.10) *and* (1.7), *be annihilated by $\Phi = \Phi_r(\sigma) \equiv \phi_r^{p^k} \pmod{p}$, then there is an $i > 0$ such that $\phi^i(\sigma)\mathfrak{A}_\phi = 0$.*

Here $i = 1$ if $k = 0$ (that is, $(n, p) = 1$) and $i \leqq lp^k$ if $k > 0$ in (1.5), where l is the maximum exponent order of elements in $\mathfrak{A}_\phi$, that is, $p^l\mathfrak{A}_\phi = 0$.

Proof. By (1.7), $\Phi - \phi^{p^k} \equiv 0 \pmod{p}$, $(\Phi - \phi^{p^k})^l \equiv 0 \pmod{p^l}$, $\phi^{lp^k} \equiv 0\ (\Phi, p^l)$, hence $\phi^{lp^k}(\sigma)\mathfrak{A}_\phi = 0$. If $k = 0$, then $\phi = \Phi$ and the statement is trivial.

As a corollary we have the result that the operator ring $\mathfrak{R}_\phi'$ of $\mathfrak{A}_\phi$ is a homomorphic image of $\mathfrak{P}[x]/(\phi^i(x), p^l)$.

All the previous discussions were independent of the number theoretical nature of n. Henceforth we shall have to assume that n is not divisible by the square of any prime number that divides the order of $\mathfrak{A}$, that is, $k = 0$ or 1 in (1.5).

Case I. $k = 0$, $(n, p) = 1$.

(2) We have written here 1 instead of ϵ to denote the p-adic identity. We shall always do this if there is no danger of ambiguity. Also we shall use ordinary integers to denote their p-adic equivalents.

We have $i=0$ in Theorem 1, hence

$$\phi(\sigma)\mathfrak{A}_\phi = 0. \tag{1.11}$$

Let h be the degree of ϕ. We shall show that an indecomposable $\mathfrak{A}_\phi$ is cyclic, that is, is generated by a single element A_0 of order p^l, and every element of $\mathfrak{A}_\phi$ can be represented in the form

$$A = f(\sigma)A_0$$

where f is a polynomial of degree less than h whose coefficients are residues modulo p^l. The order of $\mathfrak{A}_\phi$ is p^{hl} and its type as an abstract group is $(p^l, \cdots, p^l)$.

Proof. Because of (1.11), $\mathfrak{R}'_\phi$ is the homomorphic image of $\mathfrak{P}[x]/(\phi(x))$. Since $\phi(x)$ is an irreducible divisor of x^n-1, this latter is a principal ideal ring, its ideals being (p^l), $l \geqq 0$. Hence the fundamental theorem of abelian groups applies to this case (see [15, p. 126]) and the only indecomposable groups are the cyclic ones.

Thus, the situation here is analogous to the case discussed in my previous paper [12] where $\mathfrak{A}$ had no elements of order p^2. There the operator ring $\mathfrak{A}$ was homomorphic to $\Pi[x]$, $\Pi = GF(p)$, which is likewise a principal ideal ring.

Difficulties of more serious nature arise when $\mathfrak{A}_\phi$ involves elements of higher exponent orders and n is divisible by p. Here a complete solution has been found only when p divides n to exactly the first power. A solution for the structure problem of $\mathfrak{A}_\phi$ when n is divisible by p^2 would be of great importance for the theory of metabelian groups.

Case II. $n = pm$, $(m, p) = 1$.

$\mathfrak{R}'_\phi$ is a homomorphic image of $\mathfrak{P}[x]/(\phi^i(x), p^l)$ which is not a principal ideal ring if $i>1$, hence the fundamental theorem of abelian groups does not necessarily hold. In fact, we shall see that an indecomposable $\mathfrak{A}_\phi$ is not necessarily generated by a single element. Nevertheless we shall be able to find a canonical form for $\mathfrak{A}_\phi$ which will make possible the complete classification and enumeration of the different types of these groups (Definitions 1 and 2, Theorem 4).

Since ϕ is a divisor of x^m-1, irreducible in $\mathfrak{P}[x]$, we have

$$x^m - 1 = \phi\psi \tag{1.12}$$

where ϕ and ψ are relatively prime modulo p. From (1.12) we have

$$x^n - 1 = x^{mp} - 1 = (1 + \phi\psi)^p - 1 = p\phi\psi + C_{p,2}\phi^2\psi^2 + \cdots + \phi^p\psi^p. \tag{1.13}$$

Write

$$\pi(x) = \frac{x^n - 1}{x^m - 1} = p + C_{p,2}\phi\psi + \cdots + \phi^{p-1}\psi^{p-1}. \tag{1.14}$$

We show that

$$\phi(x)\pi(x) \equiv 0(\Phi(x)). \tag{1.15}$$

Since ψ and ϕ are relatively prime modulo p and $\Phi \equiv \phi^p \pmod{p}$, ψ and Φ are also relatively prime modulo p, hence there is a $\lambda(x)$ such that $\lambda\psi \equiv 1(\Phi)$. By (1.12) and (1.14),

$$\pi\phi\psi = x^n - 1 \equiv 0(\Phi),$$

hence multiplying by λ we obtain (1.15).

Next, we show that

$$p \equiv \pi(\Phi, \phi^{p-1}). \tag{1.16}$$

From (1.14) we have $p \equiv \pi(p\phi, \phi^{p-1})$, hence by (1.15), $p\phi \equiv \pi\phi \equiv 0$ $(\Phi, p\phi^2, \phi^p)$, $p \equiv \pi(\Phi, p\phi^2, \phi^{p-1})$. From the previous congruence, $p\phi^2 \equiv 0$ $(\Phi, p\phi^3, \phi^{p+1})$, hence $p \equiv (\Phi, p\phi^3, \phi^{p-1})$. Repeating the argument, we finally obtain (1.16).

(1.15) implies $\phi(\sigma)\pi(\sigma) = 0$. In the following, we shall suppress the variable σ if the polynomial over $\mathfrak{P}$ is obviously one of σ, hence an operator of $\mathfrak{R}$. Thus, the previous equation will simply be written as

$$\phi\pi = 0. \tag{1.17}$$

Congruence (1.16) becomes

$$p \equiv \pi(\phi^{p-1}), \quad \text{or} \quad p = \pi + \phi^{p-1}\gamma(\sigma) \tag{1.18}$$

which implies

$$p\phi = \phi^p\gamma. \tag{1.19}$$

The coefficients of the polynomial $\gamma = \gamma(\sigma)$ can be reduced by means of (1.19) to non-negative integers less than p (integer $= p$-adic equivalent of the integer, see footnote 2), and this puts γ into a perfectly well-determined form.

From (1.18) we have $\pi^2 = p\pi$, and generally

$$\pi^j = p\pi^{j-1} = \cdots = p^{j-1}\pi, \qquad p^j = \pi^j + \phi^{j(p-1)}\gamma^j \qquad \text{for } j \geqq 1. \tag{1.20}$$

LEMMA 1. *If $\rho \not\equiv 0$ (p, ϕ) and $B = \rho A$, then $\{A\} = \{B\}$, that is, $A = \lambda B$ for a suitable λ.*

Proof. $\rho(x)$ is a primitive polynomial relatively prime to $\phi(x)$, hence $\lambda(x)$ and $\mu(x)$ can be determined so that $\lambda(x)\rho(x) + \mu(x)\phi^i(x) = 1$, $\lambda(\sigma)\rho(\sigma)A + \mu(\sigma)\phi^i(\sigma)A = A$, where i is the exponent in Theorem 1, hence $\lambda\rho A = A$, $\lambda B = A$.

THEOREM 2. *ϕ and π are nilpotent operators.*

Proof. If l has the same significance as in Theorem 1, that is, $p^l\epsilon = 0$, then $\pi^{l+1} = p^l\pi = 0$ by (1.20). The statement concerning ϕ is contained in Theorem 1.

Theorem 2 implies that every operator ρ of $\mathfrak{R}_\phi'$ can be written in the form

$$\rho = \xi_0 + \xi_1\phi + \cdots + \xi_{i-1}\phi^{i-1} \tag{1.21}$$

where i is the exponent in Theorem 1 and $\xi_0, \cdots, \xi_{i-1}$ are polynomials of σ with degree less than h. The coefficients of ξ_0 can be reduced to non-negative integers less than p^l and those of $\xi_1, \cdots, \xi_{i-1}$ to non-negative integers less than p. Hence the order of $\mathfrak{R}_\phi'$ is not greater than $p^{h(l+i-1)}$. The above ϕ-adic form of $\mathfrak{R}_\phi'$ is similar to the representation found recently by H. S. Vandiver for principal ideal rings [13].

A further consequence of Theorem 2 is that to every $A \neq 0$ there is an $i = i(A) \geqq 0$ and $j = j(A) \geqq 0$, such that

$$\phi^i A \neq 0, \qquad \phi^{i+1}A = 0, \qquad \pi^j A \neq 0, \qquad \pi^{j+1}A = 0.$$

We call $i(A)$ and $j(A)$ the ϕ- and π-exponents of A.

DEFINITION 1. A finite $\mathfrak{R}_\phi'$-group $\mathfrak{C} = \mathfrak{C}_\phi$ is called an *open ϕ-π chain* if it is generated by $k > 0$ elements $A_1, \cdots, A_k$ (called a chain basis of $\mathfrak{C}$) satisfying the following conditions:

1. Let $i_1 = i(A_1)+1$, $i_r = i(A_r)$ for $r > 1$, $j_r = j(A_r)$ for $r < k$, $j_k = j(A_k)+1$, then $i_r > 0$, $j_r > 0$ for $r = 1, \cdots, k$.

2. Write $C_r = \phi^{i_r}A_r$, $D_r = \pi^{j_r}A_r$ (hence $C_1 = 0$, $D_k = 0$). Then $D_r = C_{r+1}$ for $r = 1, \cdots, k-1$.

3. Write $\mathfrak{D} = \{D_1, \cdots, D_{k-1}\}$ and denote by A_r^* the coset of $\mathfrak{D}$ in $\mathfrak{C}$ which is represented by A_r. Then

$$\mathfrak{D} = \{D_1\} \oplus \cdots \oplus \{D_{k-1}\}$$

and

$$\mathfrak{C}/\mathfrak{D} = \{A_1^*\} \oplus \cdots \oplus \{A_k^*\}.$$

These conditions uniquely define for any given set of chain-exponents $[i_1, j; \cdots; i_k, j_k]$ and given ϕ, an $\mathfrak{R}_\phi'$-group $\mathfrak{C}$. The elements of $\mathfrak{C}$ can be represented explicitly by the set of expressions

$$A = \sum_{r=1}^{k} \alpha_r A_r + \sum_{r=1}^{k} \phi\beta_r A_r + \sum_{r=1}^{k} \pi\gamma_r A_r + \sum_{r=1}^{k-1} \delta_r D_r \tag{1.22}$$

where α_r, β_r, γ_r, δ_r run through all the polynomials of σ with the following restrictions:

The degrees of α_r, γ_r and δ_r are less than h, that of β_r is less than $h(i_r - 1)$.

The coefficients of α_r, β_r, δ_r are non-negative integers less than p, those of γ_r are non-negative integers less than p^{i_r-1}.

The sum of two expressions (1.22) can be reduced to an expression of the same form by writing each β_r in the ϕ-adic form (1.21) and using the formulas (1.18), (1.19) and (1.20). The set $[i_1, j_1; \cdots; i_k, j_k]$ will be called the in-

variants of $\mathfrak{C}$. Evidently the order of $\mathfrak{C}$ is $p^{h(\Sigma i_r+\Sigma j_r-1)}$.

DEFINITION 2. A finite $\mathfrak{R}_\phi'$-group $\mathfrak{C}=\mathfrak{C}_\phi$ is called a *closed ϕ-π chain* if it has $k>0$ generating elements $A_1, \cdots, A_k$ (called a chain basis of $\mathfrak{C}$), satisfying the following conditions:

1. Let $i_r=i(A_r)$, $j_r=j(A_r)$ for $r=1, \cdots, k$, then $i_r>0$, $j_r>0$.

2. Let $\bar{k}$ be the smallest divisor of k, $k=d\bar{k}$ such that $i_r=i_s, j_r=j_s$ whenever $r\equiv s \pmod{\bar{k}}$ (in particular, $\bar{k}=k$ if the set $[i_1, j_1; \cdots; i_k, j_k]$ is not periodic).

Write again $C_r=\phi^{i_r}A_r$, $D_r=\pi^{j_r}A_r$. Then

$$D_r = C_{r+1} \qquad \text{for } r = 1, \cdots, k-1$$

and

$$D_k = D_{d\bar{k}} = \sum_{s=0}^{d-1} \lambda_s C_{s\bar{k}+1}$$

where the coefficients λ_s are residues modulo (p, ϕ), hence represent elements $\bar{\lambda}_s$ of a $GF(p^h)$, and satisfy the following conditions:

(a) $\bar{\lambda}_0 \not\equiv 0$, that is, $\lambda_0 \not\equiv 0 (p, \phi)$.

(b) The polynomial $f(z)=z^d-\sum_{s=0}^{d-1}\bar{\lambda}_s z^s$ in $GF(p^h)$ is either irreducible or a power of an irreducible polynomial. We shall call $f(z)$ the *characteristic polynomial* of the closed ϕ-π chain.

3. Write $\mathfrak{D}=\{D_1, \cdots, D_k\}$ and denote by A_r^* the coset of $\mathfrak{D}$ in $\mathfrak{C}$ which is represented by A_r. Then

$$\mathfrak{D} = \{D_1\} \oplus \cdots \oplus \{D_k\}$$

and

$$\mathfrak{C}/\mathfrak{D} = \{A_1^*\} \oplus \cdots \oplus \{A_k^*\}.$$

Again, these conditions uniquely determine, for any given set of exponents $[i_1, j_1; \cdots; i_{\bar{k}}, j_{\bar{k}}]$ and characteristic polynomial $f(z)$, an $\mathfrak{R}_\phi'$-group $\mathfrak{C}$. The elements of $\mathfrak{C}$ can be written explicitly as

$$(1.22^*) \qquad A = \sum_{r=1}^{k} \alpha_r A_r + \sum_{r=1}^{k} \phi\beta_r A_r + \sum_{r=1}^{k} \pi\gamma_r A_r + \sum_{r=1}^{k} \delta_r D_r$$

where the restrictions on the coefficients and degrees of α_r, β_r, γ_r, δ_r are the same as under (1.22). The order of $\mathfrak{C}$ is

$$p^{h\sum_{r=1}^{k}(i_r+j_r)} = p^{hd\sum_{r=1}^{\bar{k}}(i_r+j_r)}.$$

It should be noted that it is quite possible to construct a closed ϕ-π chain by means of an arbitrary characteristic polynomial $f(z)$ with nonzero constant term. The reason why we imposed the additional condition 2b on $f(z)$ is to make $\mathfrak{C}$ indecomposable as will be seen later.

THEOREM 3. *Let $\mathfrak{C}$ be a closed ϕ-π chain belonging to the set of exponents $[i_1, j_1; \cdots; i_{\bar{k}}, j_{\bar{k}}]$ and characteristic polynomial $f(z)$. Let $\mathfrak{C}'$ belong to $[i_2, j_2; \cdots; i_{\bar{k}}, j_{\bar{k}}; i_1, j_1]$ and the same $f(z)$. Then $\mathfrak{C}$ and $\mathfrak{C}'$ are $\mathfrak{R}_\phi'$-isomorphic.*

Proof. Let $A_1, \cdots, A_k$ $(k = d\bar{k})$ be the chain basis of $\mathfrak{C}$. To prove the theorem, we have to find a set of new generating elements $A_1', \cdots, A_k'$ which also satisfy conditions 1, 2, 3 but with exponents belonging to $\mathfrak{C}'$.

Write $A_r' = A_{r+1}$ for $r = 1, \cdots, k-1$ and $A_k' = A_{d\bar{k}}' = \sum_{s=0}^{d-1} \lambda_s A_{s\bar{k}+1}$. Since $\lambda_0 \not\equiv 0$ (p, ϕ) and $\lambda_0 A_1 = A_{d\bar{k}}' - \sum_{s=1}^{d-1} \lambda_s A_{s\bar{k}}'$, it follows from Lemma 1 that A_1, hence the whole group $\mathfrak{C}$, is generated by $A_1', \cdots, A_k'$. Since

$$i_1 = i_{\bar{k}+1} = \cdots = i_{(d-1)\bar{k}+1}, \quad j_1 = j_{\bar{k}+1} = \cdots = j_{(d-1)\bar{k}+1},$$

we have

$$\begin{aligned} C_k' &= \phi^{i_1} A_k' = \sum_{s=0}^{d-1} \lambda_s C_{s\bar{k}+1} \not\equiv 0, \\ D_k' &= \pi^{i_1} A_k' = \sum_{s=0}^{d-1} \lambda_s D_{s\bar{k}+1} \not\equiv 0, \\ \phi^{i_1+1} A_k' &= 0, \qquad \pi^{i_1+1} A_k' = 0. \end{aligned} \tag{1.23}$$

Hence, denoting by i_r', j_r' the ϕ- and π-exponents of A_r', we have

$$i_r' = i_{r+1}, \qquad j_r' = j_{r+1}, \qquad \text{for } r = 1, \cdots, k-1, \text{ and } i_k' = i_1, j_k' = j_1.$$

Furthermore, $D_{k-1}' = D_k = \sum_{s=0}^{d-1} \lambda_s C_{s\bar{k}+1} = C_k'$ and

$$D_k' = \pi^{i_k'} A_k' = \pi^{i_1} A_k' = \sum_{s=0}^{d-1} \lambda_s D_{s\bar{k}+1} = \sum_{s=0}^{d-1} \lambda_s C_{s\bar{k}+2} = \sum_{s=0}^{d-1} \lambda_s C_{s\bar{k}+1}' \qquad \text{if } \bar{k} > 1,$$

$$\begin{aligned} D_k' = D_d' &= \sum_{s=0}^{d-1} \lambda_s D_{s+1} = \lambda_0 C_2 + \cdots + \lambda_{d-2} C_d + \lambda_{d-1}(\lambda_0 C_1 + \cdots + \lambda_{d-1} C_d) \\ &= \lambda_0 C_1' + \cdots + \lambda_{d-2} C_{d-1}' + \lambda_{d-1} C_d' \qquad \text{if } \bar{k} = 1. \end{aligned}$$

Hence, condition 2 is satisfied with the same $f(z)$. Condition 3 is obvious from (1.23), since $\lambda_0 \not\equiv 0$ (that is, $\mathfrak{D}' = \mathfrak{D}$) and since $A_1', \cdots, A_k'$ are generators of $\mathfrak{C}$ and the order of $\{A_k'^*\}$ is the same as the order of $\{A_1^*\}$.

Theorem 3 implies that we obtain the same group if we perform an arbitrary cyclic permutation on the set of exponents $[i_1, j_1; \cdots; i_k, j_k]$. Hence the closed ϕ-π chain $\mathfrak{C}$ is completely determined by the primitive cycle $[i_1, j_1; \cdots; i_{\bar{k}}, j_{\bar{k}}]$ and characteristic polynomial $f(z)$. They will be called the invariants of $\mathfrak{C}$.

The structure problem of finite $\mathfrak{R}_p'$-groups is completely settled, for the case $n = mp$, $(m, p) = 1$, by the following fundamental theorem:

THEOREM 4. *Let $\phi(x)$ be an irreducible divisor of $x^m - 1$ in $\mathfrak{P}[x]$, $n = mp$,*

$(m, p)=1$. *Under this assumption an indecomposable finite* $\mathfrak{R}_\phi'$*-group* $\mathfrak{C}_\phi$ *is either an open or a closed* ϕ-π *chain. Conversely, every open or closed* ϕ-π *chain is indecomposable and* $\mathfrak{R}_\phi'$*-isomorphic chains have necessarily the same invariants.*

The proof of the theorem will require much space and is fairly independent of the rest of the paper. Therefore we continue with the discussion of the structure of the metabelian group $\mathfrak{G}$ and leave the proof of Theorem 4 to the last two sections of the paper.

2. Our next step is to select the element H, which is supposed to satisfy

$$(\sigma - 1)H = 0 \tag{2.1}$$

according to equation (3) of the introduction.

We decompose a given H into the sum of its "projections" upon the ϕ-components of $\mathfrak{A}$:

$$H = \sum H_\phi, \qquad H_\phi \in \mathfrak{A}_\phi.$$

(2.1) implies $(\sigma-1)H_\phi=0$ for every ϕ. Since $x-1$ is relatively prime to every $\phi(x)\neq x-1$, the projections H_ϕ must vanish with the exception of those which belong to $\phi_0=x-1$.

Let $\mathfrak{A}_0^{(p)}$ denote the p-primary component of $\mathfrak{A}$ belonging to ϕ_0, and $H^{(p)}$ the $\mathfrak{A}_0^{(p)}$ projection of H. $\mathfrak{A}_0^{(p)}$ is either an ordinary p-primary abelian group $((\sigma-1)\mathfrak{A}_0^{(p)}=0)$ if $(n, p)=1$, or else the direct sum of open and closed ϕ_0-π chains if $(n, p)=p$. In the latter case

$$H^{(p)} = H_1^{(p)} + H_2^{(p)} + \cdots$$

where the elements $H_r^{(p)}$ denote the projections of $H^{(p)}$ into the single chain-components $\mathfrak{C}_r^{(p)}$ of $\mathfrak{A}_0^{(p)}$. By (1.22) and (1.22*), $H_r^{(p)}$ is a sum of elements of the form $\Sigma\alpha_s A_s+\Sigma\phi_0\beta_s A_s+\Sigma\pi\gamma_s A_s$ or, since $\phi_0 H_r^{(p)}=0$,

$$\begin{aligned} H_r^{(p)} &= \sum_s \pi\gamma_{rs}A_{rs} && \text{if } \mathfrak{C}_r^{(p)} \text{ is a closed chain, and} \\ H_r^{(p)} &= b_r\phi_0^{i_r}A_{r1} + \sum_s \pi\gamma_{rs}A_{rs} && \text{if } \mathfrak{C}_r^{(p)} \text{ is an open chain.} \end{aligned} \tag{2.2}$$

In the last formula we have written i_r for the ϕ_0-exponent of the first chain basis element A_{r1} of $\mathfrak{C}_r^{(p)}$, and b_r to denote a polynomial modulo $\phi_0=\sigma-1$, that is, an integer which is supposed to be non-negative and less than p.

The form (2.2) for $H_r^{(p)}$ can be simplified still further. If we choose instead of $S=(1, 0)$ another representative of the same coset in $\mathfrak{G}:S'=(1, A)$, then we have by (1) and (4) of the introduction,

$$\begin{aligned} (0, H') = (1, A)^n &= (1, A)(1, A)\cdots(1, A) = (n, A + \sigma A + \cdots + \sigma^{n-1}A) \\ &= (0, A + \sigma A + \cdots + \sigma^{n-1}A + H), \end{aligned}$$

hence

$$H' = \frac{\sigma^n - 1}{\sigma - 1} A + H = A' + H. \tag{2.3}$$

Write $A = \sum_p A^{(p)}$, $A' = \sum_p A'^{(p)}$, $A^{(p)}, A'^{(p)} \in \mathfrak{A}^{(p)}$. We have

$$A'^{(p)} = \frac{\sigma^n - 1}{\sigma - 1} A^{(p)} = \frac{\sigma^n - 1}{\sigma^m - 1} \frac{\sigma^m - 1}{\sigma - 1} A^{(p)} = \pi \frac{\sigma^m - 1}{\sigma - 1} A^{(p)}.$$

Since $(\sigma^m - 1)/(\sigma - 1) A_\phi = 0$ if $\phi \neq \phi_0$, the operator $(\sigma^m - 1)/(\sigma - 1)$ projects $A^{(p)}$ into $A_0^{(p)}$. Hence

$$\begin{aligned} A'^{(p)} &= \pi \frac{\sigma^m - 1}{\sigma - 1} A^{(p)} = \pi \frac{(\phi_0 + 1)^m - 1}{\phi_0} A^{(p)} \\ &= \pi(m + C_{m,2}\phi_0 + \cdots + \phi_0^{m-1}) A^{(p)} = \pi m A^{(p)}, \end{aligned}$$

since $\pi\phi_0 = 0$ in $\mathfrak{A}_0^{(p)}$. Since $(m, p) = 1$, $m\mathfrak{A}^{(p)} = \mathfrak{A}^{(p)}$ by Lemma 1 in §1, hence we can choose $A^{(p)}$ so that

$$A'^{(p)} = mA^{(p)} = -H^{(p)} \qquad \text{if } (n, p) = 1$$

and

$$A'^{(p)} = \pi m A^{(p)} = -\sum_{r,s} \pi \gamma_{rs} A_{rs} \qquad \text{if } (n, p) = p.$$

Substituting this into (2.3), we have by (2.2)

$$H_r'^{(p)} = b_r \phi_0^{i_r} A_{r1} \qquad \text{if } (n, p) = p \text{ and } C_r^{(p)} \text{ is an open chain}$$

and $H_r'^{(p)} = 0$ in every other case.

Thus we have the result that if the representative S of the coset $\bar{\sigma}$ of $\mathfrak{A}'$ in $\mathfrak{G}$ is suitably chosen, then $H^{(p)}$ has the following form:

$$H^{(p)} = \sum_r b_r \phi_0^{i_r} A_{r1}, \tag{2.4}$$

where we have the sum over open chains $\mathfrak{C}_r^{(p)}$ of $\mathfrak{A}_0^{(p)}$ and i_r denotes the ϕ_0-exponent of the first basis element A_{r1} of $\mathfrak{C}_r^{(p)}$.

This is still not the simplest form of $H^{(p)}$. In deriving (2.4), we have departed from a certain chain decomposition of $\mathfrak{A}_0^{(p)}$ and varied the representative S, hence, the element H itself. Now we want to keep S and H fixed, and change the chain decomposition of $\mathfrak{A}_0^{(p)}$ appropriately so that $H^{(p)}$ shall finally have its canonical form. Generally a group $\mathfrak{A}_\phi$ possesses several different decompositions into open and closed chains and we have here the problem of finding these decompositions if a certain one is given. In particular we are interested in knowing how to find an arbitrary open chain subroup of $\mathfrak{A}_\phi$ which is a direct summand of $\mathfrak{A}_\phi$, and which can be substituted for one of the

open chains occurring in the original decomposition of $\mathfrak{A}_\phi$.

Now the proof of the fundamental theorem in §§4 and 5 will require a theory of substitutions of one system of open chains for another one, in a much more general form than is actually needed for our present purpose. Therefore we anticipate part of the theory, notably the definitions of left dominance and left resultant and the trivial Corollary 1 of Theorem 8* in §4. Suppose that the numeration of the chains $\mathfrak{C}_r^{(p)}$ with nonvanishing b_r in (2.4) is chosen so that $\mathfrak{C}_1^{(p)\circ} \geqq \mathfrak{C}^{(p)\circ} \geqq \cdots$ (for the notations see Definitions 5 and 7b in §4). Since the operators ξ in Definition 7 are simply integers if $\phi = \phi_0$, we can form the left resultant

$$\mathfrak{C}_1'^{(p)} = b_1 \cdot \mathfrak{C}_1^{(p)} \mid + b_2 \cdot \mathfrak{C}_2^{(p)} \mid + \cdots$$

and replace $\mathfrak{C}_1^{(p)}$ by $\mathfrak{C}'^{(p)}_1$ in the chain decomposition of $\mathfrak{A}_0^{(p)}$ (Corollary 1 or Theorem 8*). It is readily seen from the definition of the left resultant that

$$\phi_0^{i_1} A'_{11} = b_1 \phi_0^{i_1} A_{11} + b_2 \phi_0^{i_2} A_{21} + \cdots = H^{(p)}.$$

This shows that with the new chain decomposition we have in (2.4) a single term instead of a sum, unless every $b_r = 0$.

THEOREM 5. *$H = S^n$ in its simplest form is either* 0 *or*

$$H = \sum_p \phi_0^{i_1} A_1^{(p)} \tag{2.5}$$

where $A_1^{(p)}$ is the first chain basis element of an open ϕ_0-π chain in $\mathfrak{A}_0^{(p)}$, and i_1 is the ϕ_0-exponent of $A_1^{(p)}$. The summation involves one or several different primes p.

If $\mathfrak{A}$ is a given $\mathfrak{R}$-group and n_p denotes the number of different types of open ϕ_0-π chains which occur in the decomposition of $\mathfrak{A}_0^{(p)}$, then the number of essentially different ways H can be chosen is $\prod_p (1+n_p)$, where the product is formed for all the occurring prime numbers p.

Theorems 4 and 5 enable us to construct all the groups $\mathfrak{G}$ which have the property postulated in the introduction. Each $\mathfrak{G}$ is determined by a certain system $[\mathfrak{A}, H]$ where $\mathfrak{A}$ is an $\mathfrak{R}$-group and H is an element of $\mathfrak{A}$ having the form (2.5) of Theorem 5. The structure of $\mathfrak{A}$ can be formally characterised in the following way.

To each prime number p and to each modulo p irreducible divisor ϕ of $x^n - 1$, we assign a set of numerical invariants $F_p(\phi)$ which is either a set of positive integers $l_1 \leqq l_2 \leqq \cdots$ if $(n, p) = 1$, or a set of chain invariants (and characteristic polynomials) if $(n, p) = p$. The chain invariants and the coefficients of the characteristic polynomials can assume any values that are consistent with the conditions set up in Definitions 1 and 2, and also the multiplicities of the different types of chains can be arbitrary. Of course it is

assumed that the total number of types appearing in the system Ω of all the sets $F_p(\phi)$ is finite. Each system $[\Omega, H]$ defines exactly one abstract group $\mathfrak{G}$, and the only problem that remains to be settled is to find all the systems equivalent to a given one. Two systems $[\Omega, H]$ and $[\Omega', H']$ are called equivalent if they determine isomorphic groups.

There are two factors which might conceivably affect the system of invariants of $\mathfrak{G}$: First, we can start from another generating element $\bar{\sigma}^u$ of $\mathfrak{G}/\mathfrak{A}$ instead of $\bar{\sigma}$, and secondly we may start from an altogether different abelian invariant subgroup $\mathfrak{A}'$ instead of $\mathfrak{A}$.

The first change involves the replacing of σ by

$$\sigma' = \sigma^u, \qquad (u, n) = 1, \tag{2.6}$$

and the replacing of $\mathfrak{R}$ by $\overline{\mathfrak{R}}$, the ring of polynomials of σ'. As already mentioned in the introduction, the 1–1 mapping

$$\sum a_r\sigma^r \to \sum a_r\sigma'^r = \sum a_r\sigma^{ur}, \qquad \sum a_r\sigma'^r \to \sum a_r\sigma'^{vr}, \qquad uv \equiv 1 \pmod{n}$$

is an automormphism of $\mathfrak{R}$ which induces an $(\mathfrak{R}, \overline{\mathfrak{R}})$-automorphism of $\mathfrak{A}$. To indicate this fact we shall write $\mathfrak{A}'$ instead of $\mathfrak{A}$ whenever we consider it as an $\overline{\mathfrak{R}}$-group.

The ϕ-component of $\mathfrak{A}$ is transformed by (2.6) into the ϕ_u-component of $\mathfrak{A}'$. $\phi_u(x)$ is the irreducible polynomial which has ζ^u as a root if ζ is a root of $\phi(\zeta) = 0$. For, suppose that ϕ_u is defined by the last condition, then $\phi_u(x^u)$ is divisible by $\phi(x)$,

$$\phi_u(x^u) = \mu(x)\phi(x) \qquad \text{where } \mu(x) \not\equiv 0(\phi(x), p). \tag{2.7}$$

Hence, if $\phi^j(\sigma)A = 0$, for some j, then also $\phi_u^j(\sigma')A = \phi_u^j(\sigma^u)A = 0$, that is, $\mathfrak{A}'$ belongs to $\phi_u(\sigma')$.

If $(n, p) = 1$, then the only change in the structure of $\mathfrak{A}_\phi$ induced by the transformation (2.6) is the permutation $\phi \to \phi_u$ of the "label indices" ϕ.

If however $(n, p) = p$, and $\mathfrak{A}_\phi$ is composed of ϕ-π chains, then the chain components themselves might be affected.

Let i be the ϕ-exponent of the element $A \in \mathfrak{A}_\phi$. By (2.7)

$$\begin{aligned} \phi_u^i(\sigma')A &= \mu^i(\sigma)\phi^i(\sigma)A \not\equiv 0, \\ \phi_u^{i+1}(\sigma')A &= \mu^{i+1}\phi^{i+1}(\sigma)A = 0, \end{aligned} \tag{2.8}$$

hence the ϕ_u-exponent of A is the same as its ϕ-exponent.

By the definition of π we have

$$\pi(x) = \frac{x^n - 1}{x^m - 1} = \frac{x^{mp} - 1}{x^m - 1} = 1 + x^m + \cdots + x^{m(p+1)},$$

hence

$$\pi(\sigma) = 1 + \sigma^m + \cdots + \sigma^{m(p-1)}$$

and

$$\pi(\sigma^u) = 1 + \sigma^{um} + \cdots + \sigma^{um(p-1)} = \pi(\sigma)$$

since $\sigma^n = 1$. Hence

$$\pi(\sigma') = \pi(\sigma), \quad \text{or} \quad \pi' = \pi, \tag{2.9}$$

the operator is invariant under the isomorphism $\mathfrak{R} \to \overline{\mathfrak{R}}$.

Let $\mathfrak{C}$ be an open ϕ-π chain, $A_1, \cdots, A_k$ its chain basis elements, $[i_1, j_1; \cdots; i_k, j_k]$ its invariants. We shall prove that $\mathfrak{C}'$ is an open ϕ_u-π' chain with the same invariants. Write

$$A_k' = A_k, \qquad A_r' = (\mu(\sigma))^{\Sigma_{s>r} i_s} A_r \qquad \text{for } r < k. \tag{2.10}$$

Since $\mu(\sigma) \not\equiv 0$ (ϕ, π), A_r can be expressed from the above equation by A_r' (Lemma 1 of §1), hence $A_1', \cdots, A_k'$ are generating elements of $\mathfrak{C}'$. We have by (2.7), (2.9) and (2.10)

$$C_r' = \phi_u^{i_r}(\sigma') A_r' = \mu^{i_r} \phi^{i_r} \mu^{\Sigma_{s>r} i_s} A_r = \mu^{\Sigma_{s \geqq r} i_s} C_r,$$

$$D_r' = \pi^{i_r}(\sigma') A_r' = \pi^{i_r} \mu^{\Sigma_{s>r} i_s} A_r = \mu^{\Sigma_{s>r} i_s} D_r = \mu^{\Sigma_{s>r} i_r} C_{r+1} = C_{r+1}'.$$

This proves our assertion. It should be noted that the element H can be brought to exactly the same form as it had before the substitution (2.6).

If $\mathfrak{C}$ is a closed chain with invariants $[i_1, j_1; \cdots; i_{\bar{k}}, j_{\bar{k}}]$ and characteristic polynomial $f(z) = z^d - \sum_{s=0}^{d-1} \lambda_s z^s$, then again defining A_r' by (2.10) for $r = 1, \cdots, k = d\bar{k}$, we obtain as in the previous case that $\mathfrak{C}'$ has the same invariant $[i_r, j_r]$ as $\mathfrak{C}$. On the other hand,

$$C_{s\bar{k}+1}' = \phi_u^{i_1}(\sigma') A_{s\bar{k}+1}' = \mu^{\Sigma_{t \geqq s\bar{k}+1} i_t} C_{s\bar{k}+1} = \mu^{(d-s)(i_1 + \cdots + i_{\bar{k}})} C_{s\bar{k}+1}$$

and $D_k' = \pi^{i_k} A_k' = D_k$. By the condition 2 of Definition 2 we have $D_k = \sum_{s=0}^{d-1} \lambda_s C_{s\bar{k}+1}$, hence $D_k' = \sum_{s=0}^{d-1} \lambda_s \mu^{-(d-s)\bar{i}} C_{s\bar{k}+1}'$, where

$$\bar{i} = i_1 + \cdots + i_{\bar{k}}. \tag{2.11}$$

Hence, if the characteristic polynomial of $\mathfrak{C}$ was

$$f(z) = z^d - \sum_{s=0}^{d-1} \lambda_s z^s, \tag{2.12}$$

then that of $\mathfrak{C}'$ is

$$\bar{f}(z) = z^d - \sum_{s=0}^{d-1} \mu^{-(d-s)\bar{i}} \lambda_s z^s. \tag{2.12*}$$

For the sake of simplicity we have written here λ_s and μ to denote the corresponding elements of $GF(p^h)$. Obviously in that correspondence it does not matter whether we consider λ_s and μ as polynomials of σ modulo $\phi(\sigma)$,

or as polynomials of σ' modulo $\phi_u(\sigma')$.

DEFINITION 3. We call two systems $[\Omega, H]$ and $[\Omega', H']$ *similar* if Ω' is derived from Ω by:

1. performing the permutation $\phi \rightarrow \phi_u$ on the label indices ϕ, and

2. transforming the characteristic polynomials of each closed chain simultaneously by means of (2.12)$\rightarrow$(2.12*) where μ is defined by (2.7) and $\bar{\imath}$ by (2.11).

The form (2.5) of H is the same in both systems.

With this definition, we can summarise the above result as follows.

THEOREM 6. *Similar systems* $[\Omega, H]$ *are equivalent.*

Corresponding to the $\Phi(n)$ transformations (2.6) ($\Phi(n)$ denotes the Euler function) there are generally $\Phi(n)$ similar ones to an arbitrary $[\Omega, H]$. Of course, not all the transforms of $[\Omega, H]$ need to be different. For example, all the $\Phi(n)$ transforms are identical if $F_p(\phi)$ is vacuous for $\phi \neq \phi_0$ and $F_p(\phi_0)$ does not involve any closed chains for any p.

Now we turn to the last remaining problem and assume that $\mathfrak{G}$ contains more than one abelian invariant subgroup with the postulated properties. The quaternion group is the simplest example to show that this case can actually occur. We may avoid such ambiguous representations of $\mathfrak{G}$ if we find a procedure by which to select one of the $\mathfrak{A}$'s in a well-defined manner, and exclude all the rest by suitable restrictions on the system $[\Omega, H]$. The problem does not present any serious difficulties since the explicit form of $\mathfrak{G}$ readily allows us to find any abelian invariant subgroup with cyclic quotient group. I shall only summarize the result, without going into details.

The following definition and theorem will show which of the possible systems $[\Omega, H]$ shall be eliminated.

DEFINITION 4. We say that a system of invariants $[\Omega, H]$ is not admissible if it satisfies at least one of the following conditions I or II:

I. There is a prime divisor p of n, $n = mp^k$, $k > 1$, $(m, p) = 1$ such that every ϕ for which $F_p(\phi)$ is not vacuous is a divisor of $x^{mp} - 1$.

II. There is a prime divisor p of n, $n = mp$, $(m, p) = 1$ such that:

1. Every ϕ for which $F_p(\phi)$ is not vacuous is a divisor of $x^m - 1$.

2. Every ϕ-π chain occurring in $F_p(\phi)$ is an open chain of the type $[1, j]$ with the possible exception of a single ϕ_0-π chain belonging to $F_p(\phi_0)$ which has one of the following types:

a. A closed chain with a single basis element and invariants $[1, j_1]$, $f(z) = z - \lambda$, $(\lambda, p) = 1$.

b. An open chain with a single basis element and invariants $[2, j_1]$.

c. An open chain with two basis elements and invariants $[1, j_0; 1, j_1]$.

3. In the last two cases b and c, $H^{(p)}$ is the basis element of an open chain of the type $[1, j_2]$ in $F_p(\phi_0)$ with $j_2 \geqq j_1$.

THEOREM 7. *If* $\mathfrak{G}$ *has two or more abelian invariant subgroups to which non-*

similar systems $[\Omega, H]$ *are associated, then there is exactly one among the systems which is admissible.*

Hence, if we agree to exclude all the nonadmissible systems $[\Omega, H]$, the remaining admissible systems are, apart from similarity, uniquely associated with $\mathfrak{G}$.

It can be readily shown that if $\mathfrak{A}$ is nonmaximal, that is, if there is another abelian invariant subgroup $\mathfrak{A}'$ with the postulated properties which contains $\mathfrak{A}$ as a proper subgroup, then the system $[\Omega, H]$ associated with $\mathfrak{A}$ satisfies either condition I of Definition 4, or condition II with the restriction that only open chains of the type $[1, j]$ occur in $F_p(\phi)$ (and no exceptional types $2a$, b, c). Hence, if the system associated with $\mathfrak{A}$ is admissible then $\mathfrak{A}$ is certainly maximal.

3. In this section we shall consider problems of somewhat special character which will complement and illuminate the foregoing theory. Most of the results will be stated without proof; a rigourous proof can be easily established in each case.

Let us suppose first that n is relatively prime to the order of $\mathfrak{A}$. Then each $F_p(\phi)$ consists of a set of positive integers $l_1 \leqq l_2 \leqq \cdots$ and $\mathfrak{A}_\phi^{(p)}$ as an abstract group is the direct sum of h isomorphic subgroups (h = degree of ϕ), each being of the type $(p^{l_1}, p^{l_2}, \cdots)$. The only choice for H is $H=0$.

As an interesting application let us determine all the solvable groups $\mathfrak{G}$ which have the property that the normaliser of every element different from the unit is abelian. This problem was raised by L. Weisner [16] who proved that every solvable group $\mathfrak{G}$ with the above property (I will call it a Weisner group) has an abelian invariant subgroup $\mathfrak{A}$ such that $\mathfrak{G}/\mathfrak{A}$ is cyclic. Moreover, he showed that if $\mathfrak{A}$ is a maximal abelian invariant subgroup, then the order n of $\mathfrak{G}/\mathfrak{A}$ is relatively prime to the order of $\mathfrak{A}$. Not all such groups, however, have the above-mentioned property. A simple argument shows that the necessary and sufficient condition for $\mathfrak{G}$ to be a Weisner group is that every ϕ for which $F_p(\phi)$ is not vacuous shall not be a divisor of any x^m-1, where m is a proper divisor of n. This implies that ϕ must have for its root a primitive nth root of unity, and the degree h of ϕ is the exponent to which p belongs modulo n. $\mathfrak{A}^{(p)}$ as an abstract group is the direct sum of h isomorphic subgroups.

To obtain an arbitrary Weisner group, we have to take an abstract abelian group of order p^d which is characterised by the partition $d = x_1 + 2x_2 + \cdots + dx_d$, and assign to each member of the partition a certain ϕ. Since there are $k=\phi(n)/h$ different polynomials having a primitive nth root of unity for its root, the distribution of the ϕ's among the members of the above partition can be performed in $C_{k+x_1-1,x_1}\, C_{k+x_2-1,x_2} \cdots C_{k+x_d-1,x_d}$ different ways. Finally, since by Theorem 6 there are at most $\Phi(n)$ groups isomorphic to a given group obtained by this construction, the total number of Weisner groups of order $n\prod p_i^{h_i d_i}$ $(n, p_i)=1$, h_i the exponent to which p_i be-

longs modulo n, is not less than $(1/\Phi(n))\prod_i(\sum(C_{k_i+x_1-1,x_1}\ C_{k_i+x_2-1,x_2}\cdots C_{k_i+x_{d_i}-1,x_{d_i}}))$, to sum for every partition $d_i=x_1+2x_2+\cdots+d_ix_{d_i}$.

Another, somewhat similar problem was considered recently by L. Rédei [11] who determined all the solvable groups which themselves are non-abelian but all their proper subgroups are abelian. If $\mathfrak{A}$ is a maximal invariant subgroup of such a group $\mathfrak{G}$, then $\mathfrak{A}$ is abelian and $\mathfrak{G}/\mathfrak{A}$ is of prime order p. It can be easily shown that the order of $\mathfrak{A}$ is p^hq^k, $h\geqq 0$, $k\geqq 0$, q prime.

If $k=0$, that is, $\mathfrak{G}$ is a p-group, then $h>1$ and Ω consists of a single set $F_p(\phi_0)$. The following admissible systems will represent Rédei groups: (a) $F_p(\phi_0)$ has a single open ϕ_0-π chain of the type $[1, j_1; 1, j_2]$, $j_1+j_2=h-1$, and $H=A_1$(=the first basis element of the chain). (b) $F_p(\phi_0)$ has a single open chain of the type $[2, h-1]$ and $H=0$ or $H=\phi_0A$. (c) $F_p(\phi_0)$ has two open chains $\mathfrak{C}_1$: $[2, j_1]$, $\mathfrak{C}_2$: $[1, j_2]$, $j_2<j_1$, $j_1+j_2=h-1$ and $H=A_2$ (=the basis element of $\mathfrak{C}_2$). There are altogether $(h-2)+2+[(h-2)/2]=h-1+[h/2]$ groups of this type, in accordance with Rédei's results.

If $k>0$ and $[\Omega, H]$ represents a Rédei group, then $\Omega=\{F_p(\phi_0), F_q(\phi)\}$, where $F_q(\phi)$ contains a single invariant $l=1$, and $F_p(\phi_0)$ is either vacuous (if $h=0$) or has an open ϕ_0-π chain $\mathfrak{C}$ of the type $[1, h]$. In the first case $H=0$, in the second case $H=$the basis element of $\mathfrak{C}$. ϕ is an arbitrary irreducible divisor of degree k of x^p-1, hence k is the exponent to which q belongs modulo p. Since the system Ω belonging to different ϕ's are evidently similar, there is exactly one group of this type to every given p, q and h. Of course, if h happens to be the exponent to which p belongs modulo q, then there is a second Rédei group of the same order p^hq^k. This also confirms Rédei's result.

Let us consider now the case when n is squarefree and $\mathfrak{A}$ is a maximal abelian invariant subgroup. The central $\mathfrak{Z}$ of $\mathfrak{G}$ consists of all the elements of $\mathfrak{A}$ satisfying $(\sigma-1)A=0$. Hence, $\mathfrak{Z}$ is a subgroup of $\mathfrak{A}_0=\sum\oplus\mathfrak{A}_0^{(p)}$ formed by the elements with ϕ_0-exponent 0. If $\mathfrak{C}$ is a closed ϕ_0-π chain, then $\mathfrak{Z}\cap\mathfrak{C}=\pi\mathfrak{C}$. If $\mathfrak{C}$ is an open ϕ_0-π chain and A_1 is its first basis element with ϕ_0-exponent i, then $\mathfrak{Z}\cap\mathfrak{C}=\{\phi_0^iA_1, \pi\mathfrak{C}\}$. If $(n, p)=1$, then $\mathfrak{Z}^{(p)}=\mathfrak{Z}\cap\mathfrak{A}^{(p)}=\mathfrak{A}_0^{(p)}$, $\mathfrak{Z}=0$ if and only if $\mathfrak{A}_0=0$.

The commutator subgroup $\mathfrak{K}$ of $\mathfrak{G}$ consists of all the elements of $(\sigma-1)\mathfrak{A}$. Hence, $\mathfrak{K}=\sum_{\phi\neq\phi_0}\oplus\mathfrak{A}_\phi\oplus\sum_p\oplus\phi_0\mathfrak{A}_0^{(p)}$. By means of the chain representation of $\mathfrak{A}_0$, it is easy to verify the validity of the following relation:

$$\mathfrak{K}\cong\mathfrak{A}/\mathfrak{Z}.$$

I owe this relation to H. F. Tuan, who proved it for the case that $\mathfrak{G}$ is a non-abelian p-group and $\mathfrak{A}$ is an abelian subgroup of index p.

For the rest of this section we shall consider groups of this latter type only, that is, we shall assume that $\mathfrak{A}$ is a p-group with index p in $\mathfrak{G}$. The most important simplification in this case is that $\phi(x)$ is necessarily a divisor of $x-1$, hence $\phi=\phi_0=\sigma-1$ and Ω consists of a single set $F_p(\phi_0)$. There is no

permutation of the ϕ-indices in Definition 3 and $\mu=u$ in (2.7), which simplifies the form of the transformation (2.12)$\rightarrow$(2.12*). If $p=2$, then $\mu=u=1$, hence $F_p(\phi_0)$ has no transforms other than itself. Condition I in Definition 4 is meaningless now and condition II.1 is automatically satisfied.

The commutator subgroup is simply $\mathfrak{R}=\phi_0\mathfrak{A}$, and the lower central series is $\mathfrak{G}, \rho_0\mathfrak{A}, \phi_0^2\mathfrak{A}, \cdots$. Hence, the class of $\mathfrak{G}$ is $c=i+1$, where i is the maximum of ϕ_0-exponents of the elements in $\mathfrak{A}$. If $c<p$, that is, $i<p-1$, then $\mathfrak{G}$ is regular (see [5]). It can be shown that, conversely, if there is an element in $\mathfrak{A}$ with ϕ_0-exponent not less than $p-1$, then $\mathfrak{G}$ is not regular. In the regular case we have by (1.18) $\pi=p$, hence the operator π is simply a multiplication by p. Now we see more clearly why we had to introduce the operator π in §1; it replaces p in the nonregular case. The introduction of π accounts for the remarkable fact that no exceptional treatment was necessary for nonregular groups (notably for 2-groups) during any phase of our work.

Suppose now that the order of $\mathfrak{A}$ is p^c, then $F_p(\phi_0)$ contains either a single closed chain of the type $[1, c-1], f(z)=z-\lambda$, (λ in $GF(p)$), or a single open chain of the type $[1, c]$. In the first case $H=0$, and the transforms (2.12*) of $f(z)$ are $\bar{f}(z)=z-v^{c-1}\lambda$, $v=1, \cdots, p-1$, which give $p-1/(c-1, p-1)$ similar systems to each $F_p(\phi_0)$. Hence there are exactly $(c-1, p-1)$ different groups of this kind. In the second case we have either $H=0$ or $H=\phi_0^{c-1}A_1$, which gives two additional groups. This confirms a recent result of A. Wiman [17].

For a given finite n it is easy to enumerate the possible types of open and closed ϕ_0-π chains of order p^m, $m\leqq n$, hence to determine the number of different groups of order p^{n+1} which have abelian subgroups of order p^n. One can, for example, easily verify the known result [2] that for $n=4$ the number of different groups is 37 if $p=2$, $p+39$ if $p>2$, $p\not\equiv 1 \pmod 3$ and $p+41$ if $p\equiv 1 \pmod 3$. For $n=5$ the following values are obtained: 119 if $p=2$, 137 if $p=3$, $4p+137$ if $p\equiv 1$, $4p+127$ if $p\equiv 5$, $4p+135$ if $p\equiv 7$, and $4p+125$ if $p\equiv 11 \pmod{12}$.

Generally, let $N(p)$ denote the number of different groups of order p^{n+1} which have an abelian subgroup of order p^n. For a fixed n, $N_n(p)$ can be expressed as a polynomial of p, the degree of the polynomial and its coefficients being dependent on n. The coefficients also depend on the class of residues modulo $(n-1)!$ to which p belongs. It can be shown that if $m=[n/2]$, then the degree of $N_n(p)$ is $m-1$ and the coefficient of p^{m-1} is 1 if n is even, 4 if n is odd. The above examples (for $m=2$) serve to illustrate this rule. The lower coefficients cannot be given explicitly, since they depend on complicated partition functions of n. Nevertheless, the former rule determines at least asymptotically the behaviour of $N_n(p)$ for fixed n and large primes p.

It is more difficult to find an asymptotic formula for fixed p and large exponents n. A lower bound can be obtained by considering only such groups in which $\mathfrak{A}$ has no other chains but open ones. It is easy to verify by induction that the number of different types of open chains of order p^m is 2^{m-1}. Hence,

the number of different groups of order p^{n+1} whose $\mathfrak{A}$ is a single open chain is 2^n (since H can be chosen in exactly two different ways).

Generally M_n, the number of different groups whose $\mathfrak{A}$ consists of open chains only, is independent of p. Of course, the above value $M_n \geqq 2^n$ can be improved considerably if we allow for partitions into the sum of open chains. Straightforward combinatorial analysis shows that the total number of these partitions is

$$Q_n = \sum \prod_{i=1}^{n} C_{x_i+2^{i-1}-1,\,x_i} \tag{3.1}$$

where the summation runs over the unrestricted partitions $n = \sum_{i=1}^{n} ix_i$ of n. Hence, $2Q_n \leqq M_n \leqq nQ_n$, where the factors 2 and n express the fact that H can always be chosen in at least 2 and at most n different ways.

It follows easily from (3.1) that

$$2^n \sum_k q_k(n)/2^k < Q_n < 2^n \sum_k p_k(n)/2^k$$

where $p_k(n)$ is the number of partitions of n into exactly k summands, and $q_k(n)$ is the number of partitions of n into k unequal summands. It follows from a result of P. Erdös [4] that $\sum q_k(n)/2^k > c_1^{n^{1/2}}$ for sufficiently large n where c_1 is any positive constant less than $\exp(\pi(1/3)^{1/2} - 2(3)^{1/2}(\log 2)^2/\pi) = 3.61\cdots$. Hence, $M_n > 2^n c_1^{n^{1/2}}$ for sufficiently large n. This rough estimate is especially favourable for $p=2$. It can be shown that if $p=2$, then the total number of partitions into the direct sum of open and closed chains is less than $2^n P(n)$, where $P(n)$ is the total number of unrestricted partitions of n. Hence, $2^n c_1^{n^{1/2}} < N_n(2) < 2^n c_2^{n^{1/2}}$ for sufficiently large n, where c_2 is any constant greater than $\exp(\pi(2/3)^{1/2}) = 13.0\cdots$ by the well known formula of Hardy-Ramanujan.

Note added in proof: I am able to prove now $\log(\sum_k q_k(n)/2^k) \cong (2a \log(3/2) + \log 3)(1/2+a)^{-1/2} n^{1/2}$ where $a = (\log(3/2))^{-2} \int_0^{\log 3/2} (x/(e^x-1))dx = 2.22\cdots$. This improves the constant c_1 to $5.80\cdots$. This result will be published elsewhere.

4. **Proof of the fundamental theorem.** When formulating Theorem 4, we assumed that the operator ring $\mathfrak{R}_\phi'$ is a homomorphic image of $\mathfrak{R}_{\phi,n}[x] = \mathfrak{P}[x]/(x^n-1, \phi^i(x), p^l)$ where $n = mp$, $(m, p) = 1$ and $\phi(x)$ is an irreducible divisor of x^m-1 in $\mathfrak{P}[x]$. $\mathfrak{R}_{\phi,n}[x]$ is a finite, completely primary ring (in the terminology of Jacobson [7, p. 57]) for every n, even if $n = mp^k$ with $k>1$, since the quotient ring of the nil-ideal $\mathfrak{r} = (\phi(x), p)$ is a field. Unfortunately Theorem 4 cannot be formulated so that it will hold for every $\mathfrak{R}_\phi'$ which is the homomorphic image of an arbitrary $\mathfrak{R}_{\phi,n}[x]$. Nevertheless, the assumption $k=1$ is by no means essential for the validity of the fundamental theorem, and it can be replaced by the following, much weaker one:

We suppose that $\mathfrak{R}_\phi'$ is the homomorphic image of $\mathfrak{R}_{\phi,\theta} = \mathfrak{P}[x]/(\phi^i(x), p^l, p\phi(x) - \phi^2(x)\theta(x))$, where $\theta(x)$ is an arbitrarily given polynomial.

The case $k=1$ is obviously included here as the special case $\theta(x) = (\phi(x))^{p-2}\gamma(x)$, where $\gamma(x)$ is the polynomial defined by (1.18). Since $\phi^i(x) \equiv 0 \pmod{\mathfrak{R}_{\phi,\theta}}$ and $p\phi(x) \equiv \phi^2(x)\theta(x) \pmod{\mathfrak{R}_{\phi,\theta}}$, we can normalise $\theta(x)$ by reducing it to the ϕ-adic form

$$\theta(x) = \eta_0(x) + \eta_1(x)\phi(x) + \cdots + \eta_{i-1}\phi^{i-1}(x)$$

where $\eta_0, \eta_1, \cdots$ are polynomials of degree less than h and non-negative coefficients less than p.

Let σ be the operator corresponding to x, then dropping again the variable σ, we have

$$\phi^i = 0, \qquad p^l = 0, \qquad p\phi = \theta\phi^2. \tag{4.1}$$

Hence, writing

$$\pi = p - \theta\phi, \tag{4.2}$$

we have

$$\pi\phi = 0, \tag{4.3}$$

$$\pi^j = p\pi^{j-1} = \cdots = p^{j-1}\pi, \qquad p^j = \pi^j + \theta^j\phi^j \qquad \text{for } j \geqq 1. \tag{4.4}$$

This implies $\pi^{l+1} = \pi p^l = 0$, hence Theorem 2 holds: ϕ and π are nilpotent operators, and the nil-ideal of $\mathfrak{R}'_\phi = \mathfrak{R}'_{\phi,\pi}$ is

$$\mathfrak{r} = (\phi, p) = (\phi, \pi). \tag{4.5}$$

We can define now open and closed ϕ-π chains for the generalized operator π in close analogy to Definitions 1 and 2 in §1. In fact, we can retain these definitions wholly unchanged since the particular form of the operator π had no particular importance there, the only essential point being the validity of Theorem 2 and equation (4.3). Naturally, when calculating the sum of expressions (1.22) or (1.22*), we have to use now equation (4.4) instead of (1.20). For the rest of the paper we shall keep ϕ and π fixed and suppose that every group $\mathfrak{A}, \mathfrak{C}, \cdots$ is an $\mathfrak{R}'_{\phi,\pi}$-group.

THEOREM 4. *Every finite $\mathfrak{R}'_{\phi,\pi}$-group is the direct sum of open and closed ϕ-π chains. Every open or closed ϕ-π chain is indecomposable, and two chains are $\mathfrak{R}'_{\phi,\pi}$-isomorphic only if they possess the same set of invariants.*

As a preliminary step in the proof of Theorem 4, we shall develop in this section the "linear algebra" of open chains[3] which was indicated in §2.

The open chains $\mathfrak{C}_1, \cdots, \mathfrak{C}_k$ are called independent if

$$\mathfrak{C}_r \cap \{\mathfrak{C}_1, \cdots, \mathfrak{C}_{r-1}\} = \{0\} \qquad \text{for } r = 2, \cdots, k.$$

---

[3] Since ϕ and π are fixed, there is no fear of confusion if open and closed ϕ-π chains are simply called open and closed chains.

DEFINITION 5. Let $\mathfrak{C}_1$ and $\mathfrak{C}_2$ be open chains, their invariants $[i_{1,1}, j_{1,1}; \cdots; i_{1,l}, j_{1,l}]$ and $[i_{2,1}, j_{2,1}; \cdots; i_{2,m}, j_{2,m}]$ respectively. We say that $\mathfrak{C}_1$ is left dominant over $\mathfrak{C}_2$,

$$\mathfrak{C}_1 {}^{\circ}{>} \mathfrak{C}_2,$$

if either the first nonzero term of the sequence

$$i_{2,r} - i_{1,r}, \qquad j_{1,r} - j_{2,r}, \qquad r = 1, 2, \cdots, \min [l, m],$$

is positive, or all the terms are 0 and $l > m$.

Similarly $\mathfrak{C}_1$ is said to be right dominant over $\mathfrak{C}_2$,

$$\mathfrak{C}_2 {<}^{\circ} \mathfrak{C}_1,$$

if either the first nonvanishing term of the sequence

$$j_{2,m-r} - j_{1,l-r}, \qquad i_{1,l-r} - i_{2,m-r}, \qquad r = 0, 1, \cdots,$$

is positive, or all the terms are 0 and $l > m$.

If, in either case, all the terms vanish and $l = m$, then the two chains are isomorphic, $\mathfrak{C}_1 \cong \mathfrak{C}_2$. The definition is obviously transitive: if $\mathfrak{C}_1 {}^{\circ} \geqq \mathfrak{C}_2$, $\mathfrak{C}_2 {}^{\circ} \geqq \mathfrak{C}_3$, then $\mathfrak{C}_1 {}^{\circ} \geqq \mathfrak{C}_3$ and similarly for the right dominance. It is also clear that the definition of left and right dominance applies to *types* of open chains.

DEFINITION 6. Let A_a, $a = 1, \cdots, l$, be the chain basis elements of the open chain $\mathfrak{C}$, i_a, j_a the chain exponents of A_a. Write

$$\begin{aligned} Q_a &= \pi^{i_a} A_a = \phi^{i_{a+1}} A_{a+1} && \text{for } a = 1, \cdots, l-1, \\ Q_0 &= \phi^{i_1 - 1} A_1 && \text{if } i_1 > 1, \\ Q_l &= \pi^{i_l - 1} A_l && \text{if } j_l > 1. \end{aligned}$$

(If $i_1 = 1$ or $j_l = 1$ then Q_0, Q_l are not defined.)

Write

$$\begin{aligned} \mathfrak{C}^a &= \{A_1, \cdots, A_a\} && \text{for } a = 1, \cdots, l-1, \\ \mathfrak{C}^0 &= \{Q_0\} && \text{if } i_1 > 1, \\ \mathfrak{C}^l &= \{A_1, \cdots, A_l\} = \mathfrak{C} && \text{if } j_l > 1, \\ {}^a\mathfrak{C} &= \{A_{a+1}, \cdots, A_l\} && \text{for } a = 1, \cdots, l-1, \\ {}^0\mathfrak{C} &= \{A_1, \cdots, A_l\} = \mathfrak{C} && \text{if } i_1 > 1, \\ {}^l\mathfrak{C} &= \{Q_l\} && \text{if } j_l > 1. \end{aligned}$$

We shall call $\mathfrak{C}^a$ the left chain and ${}^a\mathfrak{C}$ the right chain associated with Q_a.

Suppose that $\mathfrak{A}$ is the direct sum of open chains. We are going to define now certain open chain subgroups of $\mathfrak{A}$ which will turn out to be direct summands of $\mathfrak{A}$. This will enable us to obtain new chain decompositions for $\mathfrak{A}$.

In the following the letters ξ, η, ζ, τ shall denote operators reduced

modulo (ϕ, π), that is, σ-polynomials of degree less than h and non-negative coefficients less than p.

Let $\mathfrak{C}$ be an open chain, A_a, $a=1, \cdots, l$, its chain basis. Then we denote by $\xi\cdot\mathfrak{C}$ the open chain with the basis elements ξA_a, $a=1, \cdots, l$. It is to be noted that $\xi\cdot\mathfrak{C}$ is not quite the same as $\xi\mathfrak{C}$, since the former refers to a definite basis of $\mathfrak{C}$. Clearly, if $\xi\neq 0$ then $\xi\cdot\mathfrak{C}\cong\xi\mathfrak{C}\cong\mathfrak{C}$.

DEFINITION 7. Let $\mathfrak{C}_1$, $\mathfrak{C}_2$ be independent open chains, their chain basis elements $A_{1,1}, \cdots, A_{1,l}$ and $A_{2,1}, \cdots, A_{2,m}$ respectively, their invariants denoted as in Definition 5.

a. Suppose that $\mathfrak{C}_1\cong\mathfrak{C}_2$ hence $l=m$. Then we define the *resultant* $\mathfrak{C}=\xi_1\cdot\mathfrak{C}_1 \mid +\mid \xi_2\cdot\mathfrak{C}_2$, $\xi_1\neq 0$ of $\xi_1\cdot\mathfrak{C}_1$ and $\xi_2\cdot\mathfrak{C}_2$ as the subgroup generated by the elements $B_a=\xi_1A_{1,a}+\xi_2A_{2,a}$, $a=1, \cdots, l$. Clearly, the elements B_a form a basis of an open chain which is isomorphic to $\mathfrak{C}_1$.

b. Suppose that $\mathfrak{C}_1{}^\circ>\mathfrak{C}_2$ and let t be the greatest index such that $i_{1,a}=i_{2,a}$, $j_{1,a}=j_{2,a}$ for every $a<t$. We define the *left resultant* $\mathfrak{C}=\xi_1\cdot\mathfrak{C}_1\mid+\xi_2\cdot\mathfrak{C}_2$, $\xi_1\neq 0$ of $\xi_1\cdot\mathfrak{C}_1$ and $\xi_2\cdot\mathfrak{C}_2$ as the open chain with the following chain basis elements:

$$B_a = \xi_1A_{1,a} + \phi^{i_{2,a}-i_{1,a}}\xi_2A_{2,a} \qquad \text{for } a \leqq t,$$

$$B_a = \xi_1A_{1,a} \qquad \text{for } a > t.$$

The elements B_a generate an open chain which is isomorphic to $\mathfrak{C}_1$. For

$$\begin{aligned}
\phi^{i_{1,a}}B_a &= \phi^{i_{1,a}}\xi_1A_{1,a} + \phi^{i_{2,a}}\xi_2A_{2,a} = \xi_1C_{1,a} + \xi_2C_{2,a} && (\text{if } a \leqq t)\\
&= \phi^{i_{1,a}}\xi_1A_{1,a} = \xi_1C_{1,a} && (\text{if } a > t),\\
\pi^{j_{1,a}}B_a &= \pi^{j_{1,a}}\xi_1A_{1,a} + \pi^{j_{1,a}}\xi_2A_{2,a} = \xi_1D_{1,a} + \xi_2D_{2,a} && (\text{if } a < t)\\
&= \pi^{j_{1,a}}\xi_1A_{1,a} = \xi_1D_{1,a} && (\text{if } a > t)\\
&= \pi^{j_{1,t}}\xi_1A_{1,t} + \pi^{j_{1,t}}\phi^{i_{2,t}-i_{1,t}}\xi_2A_{2,t} = \xi_1D_{1,t} && (\text{if } a = t).
\end{aligned}$$

Only this last formula needs some elaboration. By the definition of left dominance, if $A_{2,t}$ exists then either $i_{2,t}>i_{1,t}$ or $i_{2,t}=i_{1,t}$, $j_{1,t}>j_{2,t}$. In both cases $\pi^{j_{1,t}}\phi^{i_{2,t}-i_{1,t}}\xi_2A_{2,t}=0$.

The chain conditions 1–3 of Definition 1 can easily be verified by means of the above equations and the assumption $\mathfrak{C}_1\cap\mathfrak{C}_2=\{0\}$.

c. Suppose that $\mathfrak{C}_2<^\circ\mathfrak{C}_1$, then we define the *right resultant* $\mathfrak{C}=\xi_1\cdot\mathfrak{C}_1+\mid\xi_2\cdot\mathfrak{C}_2$, $\xi_1\neq 0$, as the open chain with the following basis elements:

$$B_{l-a} = \xi_1A_{1,l-a} + \pi^{i_{2,m-a}-i_{1,l-a}}\xi_2A_{2,m-a} \qquad \text{for } a \leqq t,$$

$$B_{l-a} = \xi_1A_{1,l-a} \qquad \text{for } a > t.$$

Here, t is the greatest integer such that

$$i_{1,l-a} = i_{2,m-a}, \qquad j_{1,l-a} = j_{2,m-a} \qquad \text{for every } a < t.$$

Again, the elements B_{l-a} generate an open chain which is isomorphic to $\mathfrak{C}_1$.

d. Let $A_{1,a}$, $A_{2,b}$ be chain basis elements of $\mathfrak{C}_1$, $\mathfrak{C}_2$ which are either supposed

to be independent or $\mathfrak{C}_1=\mathfrak{C}_2$. Let ${}^a\mathfrak{C}_1$, ${}^b\mathfrak{C}_2$ be the right chains associated with $Q_{1,a}$, $Q_{2,b}$ (Definition 6) and write $\bar{\imath}_{1,a}$, $\bar{\jmath}_{1,a}$, $\bar{\imath}_{2,b}$, $\bar{\jmath}_{2,b}$ for the ϕ- and π-exponents (*not* the chain exponents) of $A_{1,a}$ and $A_{2,b}$. Suppose further that one of the following conditions I–III is satisfied:

$$\text{I.}\quad \bar{\imath}_{2,b} < \bar{\imath}_{1,a}, \qquad \bar{\jmath}_{2,b} < \bar{\jmath}_{1,a},$$

$$\text{II.}\quad {}^a\mathfrak{C}_1 \circ\!> {}^b\mathfrak{C}_2, \qquad \bar{\imath}_{2,b} < \bar{\imath}_{1,a}, \qquad \bar{\jmath}_{2,b} = \bar{\jmath}_{1,a},$$

$$\text{III.}\quad {}^a\mathfrak{C}_1 \circ\!> {}^b\mathfrak{C}_2, \qquad \bar{\jmath}_{2,b} > \bar{\jmath}_{1,a}.$$

Then we define the *inner resultant* $\mathfrak{C}=\xi_1\cdot\mathfrak{C}_1 \,|_a+_b|\, \xi_2\cdot\mathfrak{C}_2$, $\xi_1\neq 0$, as the open chain generated by the following basis elements:

In case I: $B_r=\xi_1 A_{1,r}$ for $r\neq a$, $B_a=\xi_1 A_{1,a}+\xi_2 A_{2,b}$.

In cases II and III: $B_r=\xi_1 A_{1,r}$ for $r<a$, $B_a=\xi_1 A_{1,a}+\pi^{\bar{\jmath}_{2,b}-\bar{\jmath}_{1,a}}\xi_2 A_{2,b}$, $B_{a+r}=\xi_1 A_{1,a+r}+\phi^{\bar{\imath}_{2,b+r}-\bar{\imath}_{1,a+r}}\xi_2 A_{2,b+1}$ for $0<r\leqq t$, $B_{a+r}=\xi_1 A_{1,a+r}$ for $r>t$, where t is the greatest integer such that $\bar{\imath}_{1,a+s}=\bar{\imath}_{2,b+s}$, $\bar{\jmath}_{1,a+s}=\bar{\jmath}_{2,b+s}$ for every $0<s<t$.

It is easily seen, as under b, that the B_r generate an open chain which is isomorphic to $\mathfrak{C}_1$. It can happen that $\mathfrak{C}_1$ and $\mathfrak{C}_2$ possess several pairs of indices a, b satisfying I, II or III, then a certain resultant belongs to each of these pairs.

The definition of the inner resultant includes the definition of the left and right resultants as special cases if we admit ${}^a\mathfrak{C}_1\cong{}^b\mathfrak{C}_2$ in II and III, and $\bar{\imath}_{2,b}=\bar{\imath}_{1,a}$ for $a=b=1$ in I and II. Occasionally when forming general resultants, we shall use the notion $|+|$ in this broader sense, to denote both left, right and inner resultants.

In each of the above defined resultants there was a principal term $\xi_1\cdot\mathfrak{C}_1$ with $\xi_1\neq 0$, and the resultant was isomorphic to the principal component $\mathfrak{C}_1$. We can easily generalize the definitions to any number of independent chain components $\mathfrak{C}_1, \cdots, \mathfrak{C}_k$, whereby $\xi_1\cdot\mathfrak{C}_1$ is the principal term, and each $\mathfrak{C}_r$ can occur several times depending on the pair of indices a, b. The resultant is formed by successively adding the new term to the resultant of the former ones. Hence, after each step the resultant remains isomorphic to the principal component $\mathfrak{C}_1$. It is readily seen that it does not matter in what order we add the terms to $\xi_1\cdot\mathfrak{C}_1$. If the numeration of the chains is chosen so that $\mathfrak{C}_1\cong\cdots\cong\mathfrak{C}_t$, then the resultant can be written in the form

$$\mathfrak{C}=\sum_{r=1}^{t}|+|\,\xi_r\mathfrak{C}_r|+|\sum_{s=1}^{k}\sum_{a,b}|\,{}_a+_b|\,\eta_{s;a,b}\mathfrak{C}_s$$

where the sign $|+|$ includes left and right resultants as well. The second summation runs through such indices a, b only which satisfy the conditions of Definition 7d.

The resultant $\mathfrak{C}$ is a direct summand of $\mathfrak{A}=\mathfrak{C}_1\oplus\cdots\oplus\mathfrak{C}_k$. More generally, the following theorem holds:

THEOREM 8. *Suppose that* $\mathfrak{C}_1, \cdots, \mathfrak{C}_k$ *are independent open chains,*

$\mathfrak{A}=\mathfrak{C}_1\oplus\cdots\oplus\mathfrak{C}_k$. *Write*

$$\mathfrak{C}_r'=\sum_{\mathfrak{C}_s\cong\mathfrak{C}_{s_0}}|+|\xi_{rs}\cdot\mathfrak{C}_s|+|\sum_{t=1}^{k}\sum_{a,b}|_a+_b|\eta_{rt;ab}\cdot\mathfrak{C}_t, \tag{4.6}$$

$$r=1,\cdots,k,\ \xi_{r,s_0}\not\equiv 0,$$

where $\xi_{rs_0}\cdot\mathfrak{C}_{s_0}$ *is the principal term and the second summation runs through only such indices which are consistent with Definition 7. Then a necessary and sufficient condition for*

$$\mathfrak{A}=\mathfrak{C}_1'\oplus\cdots\oplus\mathfrak{C}_k' \tag{4.7}$$

is that

$$\det|\xi_{rs}|\not\equiv 0(\phi,\pi). \tag{4.8}$$

We shall prove the theorem in the following weaker form:

THEOREM 8*. *Under the assymption* (4.6), $\det|\xi_{rs}|\not\equiv 0(\phi,\pi)$ *implies* (4.7). *Conversely,* (4.7) *implies* (4.6) *if we assume that the multiplicity of the types of chains occurring in the decomposition* (4.7) *is equal to the multiplicity of the same types in the original decomposition.*

Theorem 8* is equivalent to Theorem 8 if the fundamental theorem is assumed. We agree therefore that only the second, weaker form of Theorem 8 will be used for the proof of Theorem 4.

Proof. Suppose first that (4.8) holds. Let us arrange $\mathfrak{C}_1,\cdots,\mathfrak{C}_k$ into types $\mathfrak{K}_1,\mathfrak{K}_2,\cdots$, each type $\mathfrak{K}_v$ consisting of a class of isomorphic chains. $\mathfrak{C}_r\in\mathfrak{K}_v$ shall denote that $\mathfrak{C}_r$ has the type $\mathfrak{K}_v$. All the chains $\mathfrak{C}_s$ with $\xi_{rs}\not\equiv 0$ in (4.6) have the same type $\mathfrak{K}_u$, and $\mathfrak{C}_r'\in\mathfrak{K}_u$. Let us choose the numeration of the chains $\mathfrak{C}_r$ and $\mathfrak{C}_r'$ so that if $u<v$ and $\mathfrak{C}_r\in\mathfrak{K}_u$, $\mathfrak{C}_s\in\mathfrak{K}_v$ or $\mathfrak{C}_r'\in\mathfrak{K}_u$, $\mathfrak{C}_s'\in\mathfrak{K}_v$, then $r<s$. It then follows from (4.8) that the matrix $|\xi_{rs}|$ is completely reduced along the diagonal to square matrix elements $|\xi_{rs}|_u$, each $|\xi_{rs}|_u$ belonging to a certain class $\mathfrak{K}_u$, and

$$\det|\xi_{rs}|_u\not\equiv 0(\phi,\pi). \tag{4.9}$$

This implies that the number of chains $\mathfrak{C}_r'\in\mathfrak{K}_u$ is the same as the number of chains $\mathfrak{C}_s\in\mathfrak{K}_u$, hence the additional assumption in Theorem 8* is certainly valid if (4.8) holds. Therefore, to prove (4.7) it is sufficient to show that $\mathfrak{C}_1',\cdots,\mathfrak{C}_k'$ are independent, that is,

$$\sum_{r=1}^{k}B_r=0,\qquad B_r\in\mathfrak{C}_r' \tag{4.10}$$

is impossible unless $B_r=0$ for $r=1,\cdots,k$.

Suppose that we have a relation (4.10) with not every $B_r=0$. Suppose further that some of the nonzero elements B_r have positive ϕ- (or π-) ex-

ponents. Let $i>0$ (or $j>0$) be the maximum of ϕ- (π-) exponents of $B_r \neq 0$.

Then multiplying (4.10) by ϕ^i (or π^j), we have

$$\sum_{r=1}^{k} E_r = 0, \quad E_r \in \mathfrak{C}_r', \quad \phi E_r = 0, \quad \pi E_r = 0 \qquad \text{for } r = 1, \cdots, k \tag{4.11}$$

with at least one $E_r \neq 0$. We shall show that (4.11) is impossible unless $E_r = 0$ for $r = 1, \cdots, k$.

An element $E \in \mathfrak{C}_s$ satisfying $\phi E = 0$, $\pi E = 0$ has obviously the form

$$E = \sum_a \rho_a Q_{sa} \tag{4.12}$$

(called subsequently the Q-representation of E), where Q_{sa} is the ath Q-element of $\mathfrak{C}_s$ in Definition 6. Every Q-element of $\mathfrak{C}_r'$, Q_{rb}' say, can be expressed as a sum of expressions (4.12). In order to prove that (4.11) is impossible unless every $E_r = 0$, we have to show that, conversely, every Q_{sa} can be expressed by means of the elements Q_{rb}'.

We assign to each Q_{sa} a positive integer o_{sa}, called the index of Q_{sa}, with the following property:

Let $\mathfrak{C}_s^a$, ${}^a\mathfrak{C}_s$ be the left and right chains associated with Q_{sa}, and $\mathfrak{C}_t^b$, ${}^b\mathfrak{C}_t$ the chains associated with Q_{tb}. Then we put $o_{sa} > o_{tb}$ if either $\mathfrak{C}_t^b < {}^\circ\mathfrak{C}_s^a$, or $\mathfrak{C}_t^b \cong \mathfrak{C}_s^a$, ${}^a\mathfrak{C}_s{}^\circ > {}^b\mathfrak{C}_t$. If both $\mathfrak{C}_t^b \cong \mathfrak{C}_s^a$ and ${}^b\mathfrak{C}_t \cong {}^a\mathfrak{C}_s$, that is, $\mathfrak{C}_s \cong \mathfrak{C}_t$ and $a = b$, then we put $o_{sa} = o_{tb}$.

Since the definition is transitive and there are altogether a finite number of indices, it is possible to determine the integers o_{sa} so as to satisfy the above condition. We can even choose them so that Q_{sa} with the lowest index shall have the index 1, and the rest of the indices shall be consecutive numbers.

To prove that every Q_{sa} has a Q'-representation, we shall employ induction with respect to the index of Q_{sa}. It follows immediately from the definition of the left, right and inner resultants that the index of every Q_{sa} occurring with nonzero coefficient in the Q-representation of Q_{rb}' in (4.6) is lower or equal to the index of $Q_{s_0 b}$ ($\mathfrak{C}_{s_0}$ being the principal component in (4.6)). Equality $o_{sa} = o_{s_0 b} = o_{rb}$ is valid only if $\mathfrak{C}_s$ itself is a principal component.

We obtain from (4.6), if $\mathfrak{K}_u$ is the type of $\mathfrak{C}_r'$:

$$Q_{rb}' = \sum_{\mathfrak{C}_{s'} \in \mathfrak{K}_u} \xi_{rs'} Q_{s'b} + \overline{Q}_{rb} \tag{4.13}$$

where $\overline{Q}_{rb}$ is a sum of Q-terms with indices $< o_{rb}$.

The matrix $|\xi_{rs}|_u$ is nonsingular by (4.9) hence has an inverse $|\bar{\xi}_{rs}|_u$ modulo (ϕ, π). From (4.13) we obtain

$$\sum_r \bar{\xi}_{sr} Q_{rb}' = \sum_{r,s'} \xi_{sr} \xi_{rs'} Q_{s'b} + \sum_r \bar{\xi}_{sr} \overline{Q}_{rb} = Q_{sb} + \sum_r \xi_{sr} \overline{Q}_{rb}.$$

Hence, each Q_{sb} with $\mathfrak{C}_s \in \mathfrak{K}_u$ can be expressed by means of the Q_{rb}' and Q-terms

whose indices are less than o_{sb}. The latter have Q'-representations by the induction hypothesis, provided that Q_{sb} has one if $o_{sb}=1$. But $o_{sb}=1$ implies $\overline{Q}_{rb}=0$, that is, $Q_{sb}=\sum_r \xi_{sr}Q'_{rb}$, which is the required Q'-representation.

To prove the converse of the theorem, suppose that $\det|\xi_{rs}|\equiv 0(\phi,\pi)$; we shall show that $\mathfrak{C}'_1, \cdots, \mathfrak{C}'_k$ are not independent, that is, (4.11) holds with $E_r\neq 0$ for some r. Because of the additional assumption in Theorem 8*, $|\xi_{rs}|$ is again reduced along the diagonal to square matrix elements $|\xi_{rs}|_u$, and $\det|\xi_{rs}|_u\equiv 0\ (\phi,\pi)$ for at least one u. Let Q_{r_0a} have the smallest possible index among all those Q-elements which belong to chains $\mathfrak{C}_s\in\mathfrak{K}_u$ with $\det|\xi_{rs}|_u\equiv 0\ (\phi,\pi)$. Without loss of generality we may assume that $\mathfrak{C}_{r_0}$ belongs to the class $\mathfrak{K}_1$,

$$\det|\xi_{rs}|_1\equiv 0(\phi,\pi) \tag{4.14}$$

and $\mathfrak{C}_1, \cdots, \mathfrak{C}_l, \mathfrak{C}'_1, \cdots, \mathfrak{C}'_l$ are the chains having the type $\mathfrak{K}_1$. (4.14) implies that

$$\sum_{r=1}^{l}\xi_{rs}\alpha_r\equiv 0(\phi,\pi), \qquad s=1,\cdots,l, \tag{4.15}$$

has a solution not identically $\equiv 0\ (\phi,\pi)$.

We have, as in (4.13)

$$Q'_{ra}=\sum_{s=1}^{l}\xi_{rs}Q_{sa}+\overline{Q}_{ra}, \qquad r=1,\cdots,l, \tag{4.16}$$

where the Q-representation of $\overline{Q}_{ra}$ involves only such Q-elements which have indices less than o_{sa}. Write $E_r=\alpha_rQ'_{ra}$ for $r=1,\cdots,l$; then $E_r\in\mathfrak{C}'_r$ and at least one $E_r\neq 0$. From (4.15) and (4.16) we obtain $E_1+\cdots+E_l=\sum_{r=1}^{l}\alpha_rQ'_{ra}=\sum_{r,s}\alpha_r\xi_{rs}Q_{sa}+\sum_r\alpha_r\overline{Q}_{ra}=\sum_{r=1}^{l}\alpha_r\overline{Q}_{ra}$. We can write this last sum as

$$\sum_{t,b}\beta_{tb}Q_{tb} \tag{4.17}$$

where $o_{tb}<o_{r_0a}=o_{1a}$ for every term with $\beta_{tb}\neq 0$. All we have to prove is that (4.17) is a sum of elements $E_{r'}\in\mathfrak{C}'_{r'}$ with $r'>l$.

If $o_{1a}=1$, then (4.17) is vacuous and there is nothing to prove. Suppose therefore $o_{1a}>1$. From the definition of Q_{r_0a} it follows that if $o_{tb}<o_{1a}$ and $\mathfrak{C}_t\in\mathfrak{K}_u$, then $\det|\xi_{tt'}|_u\neq 0\ (\phi,\pi)$. Thus, it follows by the same argument that was employed at the proof of the first half of the theorem that Q_{tb} has a Q'-representation. Moreover the proof shows that every Q'-element in this representation belongs to a $\mathfrak{C}'_{r'}$ which is not in $\mathfrak{K}_1$, hence $r'>l$.

The following corollaries are easy consequences of Theorem 8*:

COROLLARY 1. *Suppose that* $\mathfrak{A}=\mathfrak{C}_1\oplus\cdots\oplus\mathfrak{C}_k$, *and* $\mathfrak{C}_1^{\circ}\geqq\mathfrak{C}_r$, $r=2,\cdots,k$. *Write* $\mathfrak{C}'_1=\xi_1\cdot\mathfrak{C}_1|+\xi_2\cdot\mathfrak{C}_2|+\cdots|+\xi_k\cdot\mathfrak{C}_k$, $\xi_1\neq 0$ *and* $\mathfrak{C}'_r=\mathfrak{C}_r$ *for* $r=2,\cdots,k$, *then* $\mathfrak{A}=\mathfrak{C}'_1\oplus\cdots\oplus C'_k$.

The same is true if $\mathfrak{C}_r \leqq {}^{\circ}\mathfrak{C}_1$ for every r and we put $\mathfrak{C}_1' = \xi_1 \cdot \mathfrak{C}_1 + \left| \cdots \right. + \left| \xi_k \cdot \mathfrak{C}_k \right.$.

COROLLARY 2. *Suppose that* $\mathfrak{A} = \mathfrak{C}_1 \oplus \cdots \oplus \mathfrak{C}_k$, $\mathfrak{C}_1 \cong \mathfrak{C}_2 \cong \cdots \cong \mathfrak{C}_k$. *Write* $\mathfrak{C}_r' = \sum_{s=1}^{k} \left| + \right| \xi_{rs} \cdot \mathfrak{C}_s$, $r = 1, \cdots, k$, $\det \left| \xi_{rs} \right| \not\equiv 0 \ (\phi, \pi)$. *Then* $\mathfrak{A} = \mathfrak{C}_1' \oplus \cdots \oplus \mathfrak{C}_k'$.

THEOREM 9. *Suppose that* $\mathfrak{A}$ *has two different decompositions into the direct sum of open chains*:

$$\mathfrak{A} = \mathfrak{C}_1 \oplus \cdots \oplus \mathfrak{C}_k = \mathfrak{C}_1' \oplus \cdots \oplus \mathfrak{C}_k', \qquad \mathfrak{C}_r \cong \mathfrak{C}_r' \text{ for } r = 1, \cdots, k,$$

and write (with the same notations as before)

$$Q_{ra}' = \sum_{t,b} \xi_{ra;tb} Q_{tb}. \tag{4.18}$$

Then $\xi_{ra;tb} \not\equiv 0$ *only if* $\mathfrak{C}_r^{\prime a} {}^{\circ}\!\geqq \mathfrak{C}_t^{b}$, ${}^{b}\mathfrak{C}_t \leqq {}^{\circ} \mathfrak{C}_r'$.

Proof. The elements of $\mathfrak{C}_r$ can be written in the ϕ-π-adic form

$$C = \sum_{a=1}^{c(r)} \xi_a A_{ra} + \sum_{a=1}^{c(r)} \sum_{t=1}^{i_{ra}-1} \eta_{at} \phi^t A_{ra} + \sum_{a=1}^{c(r)} \sum_{t=1}^{j_{ra}-1} \zeta_{at} \pi^t A_{ra} + \sum_{a=1}^{c(r)-1} \tau_a Q_{ra}. \tag{4.19}$$

An arbitrary $A \in \mathfrak{A}$ is a sum of expressions (4.19); this shall be called the representation (4.19) of A. For $e>0$ we have $\phi^e C = \sum_{a=1}^{c(r)} \phi^e \xi_a A_{ra} + \sum_{a=1}^{c(r)} \sum_{t=1}^{i_a - e} \eta_{at} \phi^{t+e} A_{ra}$, which shows that $A = \phi^e B$ has a solution $B \in \mathfrak{A}$ only if each term in the representation (4.19) of A has the form $\phi^e T$. It is also seen that if a term $\phi^e T$ appears in the representation (4.19) of A, then the term T occurs in the representation (4.19) of B. The same holds true for the solutions B' of $A = \pi^f B'$.

Suppose now that $a>1$, $b>1$, and $\xi_{ra;tb} \not\equiv 0$ in (4.18). Since $\pi^{j_{ra}} A_{ra}' = Q_{ra}'$, $\pi^{j_{ra}} B = Q_{tb}$ has a solution $B \in \mathfrak{A}$, hence $j_{tb} \geqq j_{ra}'$ and $\xi_{ra;tb} \pi^{j_{tb} - j_{ra}} A_{tb}$ appears as a term in the representation (4.19) of A_{ra}'. The ϕ-exponent of this term (like the ϕ-exponent of any other term in the representation (4.19) of A_{ra}') is not greater than i_{ra}', hence if $j_{tb} = j_{ra}'$ then $i_{tb} \in i_{ra}'$. Thus we have either $j_{tb} > j_{ra}'$, or $j_{tb} = j_{ra}'$, $i_{tb} < i_{ra}'$, or $j_{tb} = j_{ra}'$, $i_{tb} = i_{ra}'$. In the first two cases ${}^{b}\mathfrak{C}_t \leqq {}^{\circ a}\mathfrak{C}_r'$, in the third case the representation (4.19) of $Q_{r,a-1}' = \phi^{i_{ra}} A_{ra}'$ involves the term $\xi_{ra;tb} \phi^{i_{tb}} A_{tb} = \xi_{ra;tb} Q_{t,b-1}$, that is, $\xi_{r,a-1;t,b-1} = \xi_{ra;tb} \not\equiv 0$, and we can repeat the whole argument which is also valid, with a slight modification, if $a=1$ or $b=1$. Finally we obtain ${}^{b}\mathfrak{C}_t < {}^{\circ a}\mathfrak{C}_r'$. The other relation $\mathfrak{C}_r^{a} {}^{\circ}\!\geqq \mathfrak{C}_t^{b}$ is obtained in a similar manner.

In the rest of this section we shall state a number of lemmas which will be needed for the proof of Theorem 4.

An $\mathfrak{R}_{\phi,\pi}'$-group is called simple if it has no $\mathfrak{R}_{\phi,\pi}'$-admissible subgroups besides $\{0\}$.

LEMMA 2. *A simple $\mathfrak{R}'_{\phi,\pi}$-group $\mathfrak{A}_0 \neq \{0\}$ is generated by a single element $\mathfrak{A}_0$ satisfying*

$$\phi A_0 = 0, \qquad \pi A_0 = 0, \tag{4.20}$$

and conversely. As an abstract group, $\mathfrak{A}_0$ is of the type $(p, \cdots, p)$ and its order is p^h.

For, $\mathfrak{A}_0$ certainly has an element $\mathfrak{A}_0$ with property (4.18) and this generates $\mathfrak{A}_0$ since the latter is simple. Conversely, if A_0 is a generator of $\mathfrak{A}_0$ satisfying (4.20) and $\lambda A_0 \neq 0$, then $\lambda \not\equiv 0$ (ϕ, p) by (4.5), hence by Lemma 1 of §1, $\mathfrak{A}_0$ is generated by λA_0, that is, $\mathfrak{A}_0$ is simple.

LEMMA 3. *If $\mathfrak{A}$ satisfies $\phi\mathfrak{A} = 0$, $\pi\mathfrak{A} = 0$, then $\mathfrak{A}$ is the direct sum of simple subgroups.*

This is a corollary of the corresponding theorem on ordinary abelian p-groups which have no elements of order greater than p, and it can be proved similarly.

The following two subgroups are characteristic subgroups of an arbitrary $\mathfrak{A}$:

$$\mathfrak{D} = \mathfrak{D}(\mathfrak{A}) = \pi\mathfrak{A} \cap \phi\mathfrak{A}, \qquad \mathfrak{H} = \mathfrak{H}(\mathfrak{A}) = \pi\mathfrak{A} + \phi\mathfrak{A}.$$

$\mathfrak{D}$ is a group of the type in Lemma 3. If $\mathfrak{C}$ is a chain, then $\mathfrak{D}(\mathfrak{C})$ is identical with the subgroup $\mathfrak{D}$ in Definitions 1 and 2.

$\mathfrak{H}$ is the common part of all the (admissible) subgroups with simple quotient groups in $\mathfrak{A}$, hence it is the principal subgroup of $\mathfrak{A}$.

LEMMA 4. (*Theorem of Burnside*). 1. *$\mathfrak{A}/\mathfrak{H} = \{A_1^*\} \oplus \cdots \oplus \{A_k^*\}$ where A_r^* is a coset modulo $\mathfrak{H}$ and each $\{A_r^*\}$ is simple.*

2. *Let $A_1, \cdots, A_k$ be arbitrary representatives of the cosets A_r^* in $\mathfrak{A}$, then $\mathfrak{A} = \{A_1, \cdots, A_k\}$. $A_1, \cdots, A_k$ is a minimal basis of A, that is, every set of generating elements of $\mathfrak{A}$ contains a complete set of representatives of a basis of $\mathfrak{A}/\mathfrak{H}$.*

The first part of the lemma is a trivial consequence of Lemma 3. The second part is a straightforward generalization of Burnside's well known theorem. Nevertheless, a direct proof might be of some interest.

It is sufficient to prove that $A_1, \cdots, A_k$ generate $\mathfrak{H}$. Write $A' = \{A_1, \cdots, A_k\}$ and suppose that there is a $C_0 \in \mathfrak{H}$, $C \notin \mathfrak{A}'$. We have $C_0 = \phi C_1 + \pi C_2$, hence either ϕC_1 or πC_2 is not an element of $\mathfrak{A}'$. We may suppose without loss of generality that $\phi C_1 \notin \mathfrak{A}'$. Let A^* be a coset modulo $\mathfrak{A}/\mathfrak{A}'$ which has the greatest possible ϕ-exponent, and A a representative of A^* in $\mathfrak{A}$. We have seen that this ϕ-exponent is greater than 0. Write $A = \xi_1 A + \cdots + \xi_k A_k + \phi D_1 + \pi D_2$, then $\phi A = \phi(\xi_1 A_1 + \cdots + \xi_k A_k) + \phi^2 D_1 \notin \mathfrak{A}'$, hence the cosets belonging to ϕA and $\phi^2 D_1$ in $\mathfrak{A}/\mathfrak{A}'$ are identical (and $\neq 0^*$). Hence, $i(D_1^*) > i(A^*)$, contrary to our assumption.

The k in this lemma is called the *dimension* of $\mathfrak{A}$. The dimension of a chain is clearly the number of its chain basis elements.

LEMMA 5. *Let $\mathfrak{A}$ be the direct sum of the open and closed chains $\mathfrak{C}_1, \cdots, \mathfrak{C}_k$. Let A_a denote an arbitrary chain basis element of $\mathfrak{C}_r$ with chain exponents i_a, j_a, and B an element of $\mathfrak{A}$ satisfying*

$$\phi^{i_a}B = 0, \qquad \pi^{j_a}B = 0. \tag{4.21}$$

Furthermore, if $\mathfrak{C}_r$ happens to be an open chain with a single basis element A_a, then B will satisfy at least one of the following three conditions:

$$1.\ \phi^{i_a-1}B = 0, \qquad 2.\ \pi^{j_a-1}B = 0, \qquad 3.\ B \in \mathfrak{H}(\mathfrak{A}). \tag{4.22}$$

Then $A_a' = A_a + B$ together with the chain basis elements not equal to A_a of $\mathfrak{C}_r$ form a basis of a chain $\mathfrak{C}_r' \cong \mathfrak{C}_r$ such that $\mathfrak{A} = \mathfrak{C}_1' \oplus \cdots \oplus \mathfrak{C}_k'$ where $\mathfrak{C}_s' = \mathfrak{C}_s$ for $s \neq r$.

Proof. B is uniquely represented as a sum of expressions (1.22) resp. (1.22*). In that representation, B cannot involve A_a with a coefficient $\alpha \not\equiv 0$ (ϕ, π), since otherwise the ϕ- and π-exponent of B would not be less than the respective exponents of A_a, and also B would not be an element of $\mathfrak{H}$, contrary to the assumptions of the lemma. From (4.21) $C_a' = \phi^{i_a}A_a' = \phi^{i_a}A_a$, $D_a' = \pi^{j_a}A_a' = \pi^{j_a}A_a$, and A_a' and the rest of the chain basis elements of $\mathfrak{C}_r$ form a basis of a chain $\mathfrak{C}_r' \cong \mathfrak{C}_r$. Since the representation (1.22) of B does not involve A_a the representation (1.22) of $A_a' = A_a + B$ does involve it with a coefficient $\alpha' \not\equiv 0$ (ϕ, π). Hence, A_a' and the chain basis elements of $\mathfrak{A}$ other than A_a generate $\mathfrak{A}$ by Lemma 4, which completes the proof of Lemma 5.

If A_a is the only basis element of $\mathfrak{C}_r$ and none of the supplementary conditions (4.22) is satisfied then the representation (1.22) of B might involve A_a. In that case A_a can be replaced by B and $\mathfrak{C}_r = \{A_a\}$ by $\mathfrak{C}_r' = \{B\}$ in the chain decomposition of $\mathfrak{A}$.

5. We can proceed now to prove the fundamental theorem. The proof will be carried out in several successive steps and each step will be formulated as a lemma.

Throughout the rest of the paper, the letters ξ, η, ζ, τ will denote operators reduced modulo (ϕ, π), that is σ-polynomials of degree less than h and non-negative coefficients less than p.

LEMMA 6. *An $\mathfrak{R}_{\phi,\pi}$-group generated by a single element A_0 is either an open chain with invariants $[i_0, j_0]$, or a closed chain with invariants $[i_0, j_0]$, $f(z) = z - \lambda$. Two chains $\{A_0\}$, $\{A_1\}$ are $\mathfrak{R}_{\phi,\pi}$-isomorphic only if they have the same invariants.*

This is the simplest case of the fundamental theorem. $\{A_0\}$ is necessarily indecomposable since its dimension is 1.

Proof. Let i, j be the ϕ- and π-exponents of A_0. The elements of $\{A_0\}$ can be written as

$$A = \sum_{r=0}^{i} \xi_r \phi^r A_0 + \sum_{r=1}^{j} \eta_r \pi^r A_0 \tag{5.1}$$

where the second sum is vacuous if $j=0$. For, the sum and difference of two elements (5.1) can be reduced to the same form by (4.3) and (4.4).

The uniqueness of the representation (5.1) depends on whether a relation

$$\sum_{r=0}^{i} (\xi_r - \xi_r')\phi^r A_0 + \sum_{r=1}^{j} (\eta_r - \eta_r')\pi^r A_0 = 0 \tag{5.2}$$

holds with not all the coefficients $\xi_r - \xi_r'$, $\eta_r - \eta_r'$ vanishing. Suppose we have a relation (5.2) with $\xi_r - \xi_r' \neq 0$, $r<i$, and let r be the smallest such number. Then multiplying (5.2) by ϕ^{i-r}, we have $(\xi_r - \xi_r')\phi^i A_0 = 0$, $\xi_r - \xi_r' \not\equiv 0$ (ϕ, π), hence $\phi^i A_0 = 0$, whereas i was the ϕ-exponent of A_0. Similarly we obtain $\eta_r - \eta_r' = 0$ for $r<j$. Thus, the representation (5.1) is either unique, or $i>0$, $j>0$ and there is a relation $\pi^j A_0 = \lambda \phi^i A_0$. In the first case, $\{A_0\}$ is an open chain with invariants $[i+1, j+1]$; in the second case, $\{A_0\}$ is a closed chain with invariants $[i, j]$ and $f(z) = z - \lambda$.

If A is another generating element of $\{A_0\}$, then necessarily $\xi_0 \neq 0$ in its representation (5.1), and clearly the ϕ- and π-exponents of A are identical with those of A_0. Furthermore, if $i>0$ and $j>0$, then $\phi^i A = \xi_0 \phi^i A_0$, $\pi^j A = \xi_0 \pi^j A_0$, hence $\pi^j A_0 = \lambda \phi^i A_0$ implies $\pi^j A = \lambda \phi^i A$. This proves the second half of the lemma.

LEMMA 7. *Let $\mathfrak{A}$ be indecomposable and $\mathfrak{D}(\mathfrak{A}) = \{0\}$. Then $\mathfrak{A}$ is an open chain of dimension* 1.

By the previous lemma this is equivalent to the statement that if $\mathfrak{A}$ has the dimension k and $\mathfrak{D}(\mathfrak{A}) = \{0\}$, then $\mathfrak{A} = \{A_1\} \oplus \cdots \oplus \{A_k\}$, where each $\{A_r\}$ is an open chain.

Proof. If $\phi\mathfrak{A} = \{0\}$, then π is identical with the operator $p\epsilon$, and $\mathfrak{R}_{\phi,\pi}$ is a principal ideal ring, as in case I of §1. Hence, by the fundamental theorem of abelian groups an indecomposable $\mathfrak{A}$ is generated by a single element A_0. Suppose, therefore, that $\phi\mathfrak{A} \neq \{0\}$, hence there are elements in $\mathfrak{A}$ with ϕ-exponents greater than 0. Let $i_1>0$ be the maximum of ϕ-exponents in $\mathfrak{A}$. Among the elements with ϕ-exponent i_1, let A_1 be an element with the smallest π-exponent j_1. We shall prove that $\{A_1\}$ is a direct summand of $\mathfrak{A}$.

We assume that the dimension of $\mathfrak{A}$ is $k>1$, and also that the lemma is true for every $\mathfrak{A}$ with a smaller dimension.

1. $A_1 \in \mathfrak{H}(\mathfrak{A})$. For, suppose that $A_1 = \phi B_1 + \pi B_2$, then $\phi A_1 = \phi^2 B_1 \neq 0$, $\phi^{i_1} A_1 = \phi^{i_1+1} B_1 \neq 0$, whereas i_1 was supposed to be the greatest ϕ-exponent in $\mathfrak{A}$.

Consider the quotient group $\mathfrak{A}^* = \mathfrak{A}/\{A_1\}$. Elements of $\mathfrak{A}^*$ (that is, cosets modulo $\{A_1\}$) shall be distinguished from their representatives in $\mathfrak{A}$ by an asterisk.

2. $\mathfrak{D}(\mathfrak{A}^*) = \{0^*\}$. For, if there were elements $B^* \neq 0^*$, B_1^*, B_2^*, such that

$\phi B_1^* = B^*$, $\pi B_2^* = B^*$, then we have for their representatives in $\mathfrak{A}$, $B = \phi B_1 = \pi B_2 + C$, $C \in \{A_1\}$, that is, $C = \phi B_1 - \pi B_2 \in \mathfrak{H}$. Since $A_1 \notin \mathfrak{H}$, C is necessarily of the form $C = \alpha\phi A_1 + \beta\pi A_1$, hence $B - \alpha\phi A_1 = \phi(B_1 - \alpha A_1) = \pi(B_2 + \beta A_1) \neq 0$, which contradicts $\mathfrak{D}(\mathfrak{A}) = \{0\}$.

Clearly, the dimension of $\mathfrak{A}^*$ is $k-1$, hence by the induction hypothesis $\mathfrak{A}^* = \{A_2^*\} \oplus \cdots \oplus \{A_k^*\}$ where each $\{A_r^*\}$ is an open chain. Let the chain exponents of A_r^* be i_r, j_r for $r = 2, \cdots, k$, hence $i(A_r^*) = i_r - 1$, $j(A_r^*) = j_r - 1$. We show that if we choose the representatives A_r of A_r^* appropriately, then

3. $\phi^{i_r} A_r = 0$, $\pi^{j_r} A_r = 0$, $r = 2, \cdots, k$.

By the definition of i_r, j_r we have $\phi^{i_r} A_r^* = 0^*$, $\pi^{j_r} A_r^* = 0^*$, hence $\phi^{i_r} A_r = C_r \in \{A_1\}$, $\pi^{j_r} A_r = D_r \in \{A_1\}$. If $C_r \neq 0$, then it has the form $C_r = \alpha\phi^i A_1$, $i_1 \geqq i > 0$, $\alpha \not\equiv 0$ (ϕ, π), by 1 and since $\mathfrak{D} = \{0\}$. Also $i \geqq i_r$, since otherwise we have $\phi^{i_1 - i + i_r} A_r = \alpha\phi^{i_1} A_1 \neq 0$, $i_1 - i + i_r > i_1$, contradicting the maximum assumption on i_1.

Choosing $A_r' = A_r - \alpha\phi^{i - i_r} A_1$ as a new representative of A_r^* in $\mathfrak{A}$, we have $\phi^{i_r} A_r' = \phi^{i_r} A_r - \alpha\phi^i A_1 = \phi^{i_r} A_r - C_r = 0$.

This proves the first part of 3. To prove the second half, we remark that $\pi^{j_r} A_r = D_r$ (if not 0) is necessarily of the form

$$D_r = \beta\pi^j A_1, \qquad j_1 \geqq j > 0, \qquad \beta \not\equiv 0 \ (\phi, \pi).$$

We show that $j > j_r$. For, suppose that $j \leqq j_r$, then we have $\pi^{j_1}(\beta A_1 - \pi^{j_r - j} A_r) = \pi^{j_1 - j}(\beta\pi^j A_1 - D_r) = 0$, $\phi^{i_1}(\beta A_1 - \pi^{j_r - j} A_r) \neq 0$, the latter because $\phi^{i_1}\beta A_1 \neq 0$ and $\phi^{i_1}\pi^{j_r - j} A_r = 0$ unless $j_r = j$, $i_1 < i_r$, in which case $\phi^{i_1}(\beta A_1^* - \pi^{j_r - j} A_r^*) = \phi^{i_1} A_r^* \neq 0^*$.

Thus, $i(\beta A_1 - \pi^{j_r - j} A_r) = i_1$, $j(\beta A_1 - \pi^{j_r - j} A_r) < j_1$, which is contrary to the definition of i_1, j_1. Hence $j > j_r$. Choosing $A_r' = A_r - \beta\pi^{j - j_r} A_1$ as a new representative of A_r^*, we have $\pi^{j_r} A_r' = \pi^{j_r} A_r - \beta\pi^j A_1 = D_r - \beta\pi^j A_1 = 0$, $\phi^{i_r} A_r' = \phi^{i_r} A_r - \beta\phi^{i_r}\pi^{j - j_r} A_1 = 0$ since $j > j_r$, $i_r > 0$ and $\phi^{i_r} A_r = 0$.

This completes the proof of 3. As a corollary we obtain the result that with the new representatives A_r, $\{A_r\} \cong \{A_r^*\}$ for $r = 2, \cdots, k$, hence $\mathfrak{A} = \{A_1\} \oplus \{A_2\} \oplus \cdots \oplus \{A_k\}$.

Lemma 7 proves Theorem 4 for the case that $\mathfrak{D}(\mathfrak{A}) = \{0\}$. Henceforth we shall assume that $\mathfrak{D}$ is not $\{0\}$, that is, its dimension m is greater than 0. We shall also assume that Theorem 4 is proved for every group in which the dimension of $\mathfrak{D}$ is smaller than m.

In analogy to the height-exponent of H. Prüfer, we define the ϕ-height and π-height of an element $A \neq 0$ in $\mathfrak{A}$ as the greatest exponents e and f for which solutions C, D of $\phi^e C = A$, $\pi^f D = A$, $C, D \in \mathfrak{A}$ exist. If $e(A)$ denotes the ϕ-height of A and $e(A) < e(B)$, then, evidently, $e(A + B) = e(A)$. If $e(A) = e(B)$, then $e(A + B) \geqq e(A)$, and similar relations hold for the π-height $f(A)$.

We now define a characteristic subgroup $\mathfrak{E} \subset \mathfrak{D}$ in the following manner:

Let $i_0 > 0$ be the maximum of ϕ-heights of the nonzero elements of $\mathfrak{D}$. Let further:

Ω_1 = the set of elements A with ϕ-exponent i_0 and $\phi^{i_0}A \in \mathfrak{D}$;
j_0 = the minimum of π-exponents of the elements of Ω_1;
Ω_2 = the set of elements of Ω_1 with π-exponent j_0;
Ω = the set of elements $A \in \Omega_2$ with $\pi^{j_0}A \in \mathfrak{D}$ if there exist such elements, $\Omega = \Omega_2$ otherwise;
$\mathfrak{E}_1$ = the set of elements $E \in \mathfrak{D}$ for which solutions of $\phi^{i_0}A = E$ exist with $A \in \Omega$.

Let $j_0' > 0$ be the maximum of π-heights of the nonzero elements of $\mathfrak{E}_1$. Let further:
Σ_1 = the set of elements A with π-exponent j_0' and $\pi^{j_0'}A \in \mathfrak{E}_1$;
i_0' = the minimum of ϕ-exponents of the elements in Σ_1;
Σ_2 = the set of elements of Σ_1 with ϕ-exponent i_0';
Σ = the set of elements $A \in \Sigma_2$ with $\phi^{i_0'}A \in \mathfrak{D}$ if there exist such elements, $\Sigma = \Sigma_2$ otherwise;
$\mathfrak{E} = \mathfrak{E}(\mathfrak{A})$ = the set of elements $E \in \mathfrak{E}_1$, for which solutions of $\pi^{j_0'}A = E$ exist with $A \in \Sigma$.

Evidently, $\mathfrak{E}$ is a subgroup of $\mathfrak{D}$ and its dimension is greater than 0. Consider the quotient group $\mathfrak{A}^* = \mathfrak{A}/\mathfrak{E}$. The dimension of its $\mathfrak{D}$-group $\mathfrak{D}^*$ is less than m, since $\mathfrak{E} \subset \mathfrak{D}$ and each representative D of $D^* \in \mathfrak{D}^*$ is an element of $\mathfrak{D}$. Hence we conclude by the induction hypothesis that $\mathfrak{A}^*$ is the direct sum of open and closed chains,

$$\mathfrak{A}^* = \mathfrak{C}_1^* \oplus \cdots \oplus \mathfrak{C}_k^*. \tag{5.3}$$

Let us suppose first that $\mathfrak{E} = \mathfrak{D}$, that is, $\mathfrak{D}(\mathfrak{A}^*) = \{0^*\}$, hence (by Lemma 7) each $\mathfrak{C}_r^*$ in (5.3) is an open chain with a single basis element A_r^*. Let the chain exponents of A_r^* be i_r, j_r, and A_r be a representative of A_r^* in $\mathfrak{A}$. Write

$$\phi^{i_r}A_r = C_r, \qquad \pi^{j_r}A_r = D_r, \tag{5.4}$$

where $C_r, D_r \in \mathfrak{E}$. It is quite possible that for some r, $C_r = 0$ or $D_r = 0$. Let the chains $\mathfrak{C}_1^*, \cdots, \mathfrak{C}_k^*$ be arranged in such an order that in (5.4) $C_r \neq 0$ for $r = 1, \cdots, s$ and $C_r = 0$ for $r > s$. Let the chains $\mathfrak{C}_r^*$ (among the possible chain decompositions (5.3) of A^*) and the representatives A_r be chosen so that s shall have a smallest possible value. We then show that a relation

$$\xi_1 C_1 + \cdots + \xi_s C_s = 0 \tag{5.5}$$

cannot hold unless every $\xi_r = 0$. For, in the contrary case let $\mathfrak{C}_1^*, \cdots, \mathfrak{C}_s^*$ be arranged so that $\xi_s \neq 0$ and $\mathfrak{C}_s^{*\circ} \geqq \mathfrak{C}_r^*$ for every r with $\xi_r \neq 0$. Then (by Corollary 1 of Theorem 8*) we could replace $\mathfrak{C}_s^*$ by $\xi_1 \cdot \mathfrak{C}_1^* | + \cdots | + \xi_s \cdot \mathfrak{C}_s^*$, hence (by Definition 7b) A_s by $A_s' = \sum_{r=1}^{s} \xi_r \phi^{i_r - i_s} A_r$, whence we have $C_s' = \phi^{i_s} A_s' = \sum_{r=1}^{s} \xi_r C_r = 0$, contradicting the minimum assumption on s.

Similarly, if $v_1, \cdots, v_t$ are the indices (not necessarily in numerical order) for which $D_{v_r} \neq 0$, and t has the smallest possible value (with s being minimal), then a relation

$$\eta_1 D_{v_1} + \cdots + \eta_t D_{v_t} = 0 \tag{5.6}$$

cannot hold unless every $\eta_r = 0$. For, in the contrary case let v_t be an index for which $\eta_t \neq 0$ and $\mathfrak{C}^*_{v_r} \leqq {}^\circ\mathfrak{C}^*_{v_t}$ for every r with $\eta_r \neq 0$. If there are several indices with the same property, let v_t be the smallest among them. Again, replacing $\mathfrak{C}^*_{v_t}$ by $\eta_1 \cdot \mathfrak{C}^*_{v_1} + \cdots + \eta_t \cdot \mathfrak{C}^*_{v_t}$ and A_{v_t} by $A'_{v_t} = \sum_{r=1}^{t} \eta_r \pi^{i_{v_r} - i_{v_t}} A_{v_r}$, we have $D'_{v_t} = \sum_{r=1}^{t} \eta_r D_{v_r} = 0$, which contradicts the minimum assumption on t. Moreover, we have $C'_{v_t} = \phi^{i_{v_t}} A'_{v_t} = \sum_{C^*_{v_r} \cong C^*_{v_t}} \eta_r C_r$, and this equals 0 if $v_t > s$ (since in that case every $v_r > s$ in the last sum). Hence, $C_r = 0$ for $r > s$ is not affected by the new change.

It is immediately seen from (5.5) and (5.6) that both of the sets $C_1, \cdots, C_s$ and $D_{v_1}, \cdots, D_{v_t}$ form a basis of $\mathfrak{D} = \mathfrak{E}$, hence $s = t = m$. Furthermore

$$A_r \in \Omega, \qquad A_{v_r} \in \Sigma \qquad \text{for } r = 1, \cdots, m. \tag{5.7}$$

For, $C_r \in \mathfrak{E}$; hence by the definition of $\mathfrak{E}$ there is a $B \in \Omega$ such that $\phi^{i_0} B' = C_r$. Write $B' = \phi^{i_0 - i_r} B$. If $i_r < i_0$, or $i_r = i_0$ and $j_r > j_0 + 1$, then $\phi^{i_r} B' = C_r$, $\pi^{j_r - 1} B = 0$, $\phi^{i_r} B'^* = 0^*$, $\pi^{j_r - 1} B'^* = 0^*$, hence, by Lemma 5 we could replace A^*_r by $A^*_r - B'^*$. We have $C'_r = \phi^{i_r} A'_r = \phi^{i_r}(A_r - B') = C_r - C_r = 0$, $D'_r = \pi^{j_r} A'_r = \pi^{j_r} A_r = D_r$, hence a further C_r would vanish, which is impossible.

The same argument applies in the case $i_r = i_0$, $j_r = j_0 + 1$ if $\pi^{j_0} B \in \mathfrak{D}$. If $\pi^{j_0} B \notin \mathfrak{D}$, then according to the remark after Lemma 5 we can replace A^*_r either by $A^*_r - B^*$ or by B^*. In the first case $C'_r = \phi^{i_r}(A_r - B) = C_r - C_r = 0$, $D'_r = \pi^{j_r}(A_r - B) = D_r$, which is not possible, by the previous argument. In the second case $C'_r = \phi^{i_r} B = C_r$, $D'_r = \pi^{j_r} B = 0$ which is possible only if also $D_r = \pi^{j_r} A_r = 0$. In that case the π-exponent of A_r is $j_0 = j_r + 1$, hence $A_r \in \Omega$. Finally, if $i_r = i_0$, $j_r = j_0$, then $\pi^{j_r} A_r = D_r \neq 0$ (by the definition of j_0), hence $A_r \in \Omega$.

A similar argument shows the validity of the second half of (5.7). An immediate consequence of (5.7) is that either $v_s \leqq m$ for $s = 1, \cdots, m$ or $v_s > m$ for $s = 1, \cdots, m$. For suppose that $v_s = r \leqq m$, that is, $C_r \neq 0$, $D_r \neq 0$, then from (5.7) $A_r \in \Omega$, $A_r \in \Sigma$, whence $i_0 = i'_0$, $j_0 = j'_0$ and $\pi^{j_0} A_r \in \mathfrak{D}$. Hence by the definition of Ω, $\pi^{j_0} A_s \in \mathfrak{D}$, that is, $D_s \neq 0$ for every $s = 1, \cdots, m$, which proves our assertion.

Case I. Suppose first that $v_s > m$ for $s = 1, \cdots, m$. We arrange the basis elements so that $v_1 = m + 1, \cdots, v_m = 2m$. Since both $C_1, \cdots, C_m$ and $D_{m+1}, \cdots, D_{2m}$ form a basis of $\mathfrak{D}$, there is a relation

$$C_r = \sum_{s=1}^{m} \xi_{rs} D_{m+s}, \qquad r = 1, \cdots, m,$$

between them with $\det |\xi_{rs}| \not\equiv 0 \ (\phi, \pi)$.

It is seen that $\mathfrak{C}^*_{m+1} \cong \cdots \cong \mathfrak{C}^*_{2m}$ since they are open chains of the type $[i'_0 + 1, j'_0]$, hence by Corollary 2 of Theorem 8* we can replace $\mathfrak{C}^*_{m+r}$,

$r=1, \cdots, m$, by $\sum_{s=1}^{m}| + |\xi_{rs}\cdot\mathfrak{C}_{m+s}^*$, hence A_{m+r} by $A'_{m+r}=\sum_{s=1}^{m}\xi_{rs}A_{m+s}$ whence

$$D'_{m+r}=\sum_{s=1}^{m}\xi_{rs}D_{m+s}=C_r, \qquad r=1, \cdots, m.$$

Thus, $\mathfrak{A}$ is the direct sum of the open chains $\{A_{m+r}, A_r\}, r=1, \cdots, m$, with invariants $[i_0'+1, j_0'; i_0, j_0+1]$ and the subgroup $\{A_{2m+1}, \cdots, A_k\}$. $\mathfrak{A}$ is indecomposable only if it is an open ϕ-π chain with two basis elements and invariants $[i_0'+1, j_0'; i_0, j_0+1]$.

Case II. The indices $v_1, \cdots, v_m$ are, in some arrangement, identical with $1, \cdots, m$, and

$$i_r=i_0=i_0', \qquad j_r=j_0=j_0' \qquad \text{for } r=1, \cdots, m.$$

The elements $C_1, \cdots, C_m$ resp. $D_1, \cdots, D_m$ form a basis of $\mathfrak{D}$, and $\mathfrak{A}$ is the direct sum of $\{A_1, \cdots, A_m\}$ and $\{A_{m+1}, \cdots, A_k\}$. We show that $\mathfrak{A}'=\{A_1, \cdots, A_m\}$ is a direct sum of closed ϕ-π chains. We have

$$D_r=\sum_{s=1}^{m}\xi_{rs}C_s, \qquad r=1, \cdots, m, \det|\xi_{rs}| \not\equiv 0 \ (\phi, \pi). \tag{5.8}$$

Since $\mathfrak{C}_1^*\cong \cdots \cong\mathfrak{C}_m^*$, we can again introduce new basis elements

$$A_r'=\sum_{s=1}^{m}\tau_{rs}A_s, \qquad r=1, \cdots, m, \tag{5.9}$$

with $\det|\tau_{rs}| \not\equiv 0 \ (\phi, \pi)$.

The coefficients τ_{rs}, ξ_{rs} represent residue classes mod (ϕ, π), hence can be regarded as elements $\bar{\tau}_{rs}$, $\bar{\xi}_{rs}$ of a $GF(p^h)$. Denote by $T=\|\bar{\tau}_{rs}\|$ and $X=\|\bar{\xi}_{rs}\|$ the matrices formed by these elements. After performing the transformation (5.9) of the basis elements, the system of equations (5.8) transforms into

$$D_r'=\sum_{s=1}^{m}\eta_{rs}C_s', \qquad r=1, \cdots, m, \tag{5.10}$$

where $Y=\|\bar{\eta}_{rs}\|=T^{-1}XT$.

Here we can choose T so that Y shall appear reduced to irreducible square submatrices along the diagonal. To this corresponds a decomposition of $\mathfrak{A}'$ into the direct sum of subgroups generated by the respective basis elements of the submatrices of Y. We can choose T so that each submatrix of Y shall assume the second (rational) canonical form (see [15, p. 137]), that is, become a companion matrix of the form

$$\begin{aligned} &\bar{\eta}_{r,r+1}=1 \text{ for } r=1, \cdots, d-1, \qquad \bar{\eta}_{rs}=0 \text{ for } r<d, r\neq s-1, \\ &\bar{\eta}_{ds}=\bar{\lambda}_{s-1}, \qquad\qquad\qquad\qquad\qquad\qquad s=1, \cdots, d, \end{aligned} \tag{5.11}$$

where d is the number of rows and columns of the submatrix and $f(z)=z^d-\sum_{s=1}^{d}\lambda_{s-1}z^{s-1}$ is either irreducible in $GF(p^h)$ or a power of an irreducible polynomial. Thus (5.10) has the following form:

$$D_1'=C_2,\cdots,D_{d-1}'=C_d',\qquad D_d'=\lambda_0C_1'+\cdots+\lambda_{d-1}C_d',$$

that is, $\{A_1,\cdots,A_d\}$ is a closed chain with the invariants $[i_0,j_0]$, $f(z)=z^d-\sum_{s=1}^{d}\lambda_{s-1}z^{s-1}$.

Thus we obtain the following lemma.

LEMMA 8. *An indecomposable* $\mathfrak{A}$ *which satisfies* $\mathfrak{D}(\mathfrak{A})=\mathfrak{E}(\mathfrak{A})\neq\{0\}$ *is either an open chain with the invariants* $[i_0'+1,j_0';i_0,j_0+1]$, *or a closed chain with the invariants* $[i_0,j_0]$; $f(z)$.

The uniqueness of the invariants is obvious; i_0, j_0 and i_0', j_0' are connected in an invariant way with the structure of the group, according to their definition. The uniqueness of the characteristic polynomial is a consequence of the well known fact that the canonical form (5.11) is uniquely determined by the matrix X in (5.8).

Lemma 8 proves Theorem 4 for the case that $\mathfrak{E}=\mathfrak{D}$. Henceforth we shall assume that $\mathfrak{E}$ is a proper subgroup of $\mathfrak{D}$.

To each chain basis element A_r^* of the chains $\mathfrak{C}_s^*$ in (5.3) we select a representative A_r in $\mathfrak{A}$. Let i_r, j_r be the chain exponents of A_r^*. If A_{r-1}^* and A_r^* are two consecutive basis elements of the same chain, then we have $\pi^{i_{r-1}}A_{r-1}^*=\phi^{i_r}A_r^*\neq 0^*$ and

$$D_{r-1}=\pi^{i_{r-1}}A_{r-1}=\phi^{i_r}A_r+E=C_r+E,\qquad E\in\mathfrak{E}. \tag{5.12}$$

We show that by choosing the chain decomposition of A^* and the representatives A_r in $\mathfrak{A}$ appropriately, we can make E vanish in each of the relations (5.12).

Suppose that $E\neq 0$ in (5.12) and put

$$\phi^{i_0}B_1=E,\qquad \pi^{j_0}B_2=E,\qquad B_1\in\Omega,\qquad B_2\in\Sigma.$$

Evidently $D_{r-1}=\pi^{j_{r-1}}A_{r-1}\in\mathfrak{D}$, $C_r=\phi^{i_r}A_r\in\mathfrak{D}$, hence either $i_r<i_0$, or $i_r=i_0$ and $j_r\geqq j_0$. Suppose first that $A_r\notin\Omega$, hence either $i_r<i_0$, or $i_r=i_0$, $j_r>j_0$. Since $B_1\in\Omega$, we obtain

$$\begin{aligned}&\phi^{i_r}(\phi^{i_0-i_r}B_1)=\phi^{i_0}B_1=E,\qquad &&\pi^{j_r}(\phi^{i_0-i_r}B_1)=0,\\ &\phi^{i_r}(\phi^{i_0-i_r}B_1^*)=0^*, &&\pi^{j_r}(\phi^{i_0-i_r}B_1^*)=0^*.\end{aligned} \tag{5.13}$$

By Lemma 5 we can replace A_r^* by $A_r^*+\phi^{i-i_r}B_1^*$ in the chain decomposition of $\mathfrak{A}^*$. Replacing A_r by $A_r'=A_r+\phi^{i-i_r}B_1$, we obtain from (5.12), (5.13) $C_r'=\phi^{i_r}A_r'=C_r+E=D_{r+1}$ and $D_r'=\pi^{j_r}A_r'=\pi^{j_r}A_r$.

Suppose next that $A_r\in\Omega$, then $A_{r-1}\notin\Sigma$ since otherwise we have $D_{r-1}\in\mathfrak{E}$, $D_{r-1}^*=0^*$. Repeating the previous argument with the roles of ϕ and π inter-

changed, and replacing A_{r-1} by $A'_{r-1}=A_{r-1}-\pi^{j_0-j_{r-1}}B_2$, we obtain $C'_{r-1}=\phi^{i_{r-1}}A'_{r-1}=\phi^{i_{r-1}}A_{r-1}$ and $D'_{r-1}=\pi^{j_{r-1}}A'_{r-1}=D_{r-1}-E=C_r$.

In either case we have $D'_{r-1}=C'_r$, hence $E=0$ in (5.12). We also see that the performed operations leave the elements $C_{r-1}=\phi^{i_{r-1}}A_{r-1}$ and $D_r=\phi^{i_r}A_r$ unchanged. Thus, repeating the whole procedure if necessary, we can successively annihilate E in each one of the relations (5.12).

A similar reasoning also shows that if the basis elements $A_1^*, \cdots, A_l^*$ generate a closed chain, and

$$D_l^* = \lambda_0 C_1^* + \lambda_1 C_{l+1}^* + \cdots, \quad D_l = \lambda_0 C_1 + \lambda_1 C_{l+1} + \cdots + E, \qquad E \in \mathfrak{E},$$

then we can annihilate this E too by changing A_l and A_1 appropriately. Thus, the new representatives $A_1, \cdots, A_l$ themselves will generate a closed chain in $\mathfrak{A}$ isomorphic to $\{A_1^*, \cdots, A_l^*\}$. Since $\{A_1, \cdots, A_l\} \cap E = \{0\}$, and $\{A_1, \cdots, A_l\} \cap \{A_{l+1}, \cdots, A_k\} \subset \mathfrak{E}$, the subgroups $\{A_1, \cdots, A_l\}$ and $\{A_{l+1}, \cdots, A_k\}$ have no common elements besides 0, hence

$$\mathfrak{A} = \{A_1, \cdots, A_l\} \oplus \{A_{l+1}, \cdots, A_k\}.$$

We summarise the result as follows:

LEMMA 9. *Let $\mathfrak{A}$ be indecomposable and $\mathfrak{E}(\mathfrak{A})$ be a proper subgroup of $\mathfrak{D}(\mathfrak{A})$. Then every $\mathfrak{C}_r^*$ in* (5.3) *is an open chain and at least one $\mathfrak{C}_r^*$ has more than one basis element. If A_{r-1}^* and A_r^* are two consecutive basis elements of the same chain, then*

$$\pi^{i_{r-1}}A_{r-1} = \phi^{i_r}A_r \tag{5.14}$$

for suitable representatives in $\mathfrak{A}$.

Let A_{ra}^*, $a=1, \cdots, c(r)$ be the chain basis elements of $\mathfrak{C}_r^*$, A_{ra} their representatives in $\mathfrak{A}$ satisfying (5.14), i_{ra}, j_{ra} the chain exponents of A_{ra}^*. Write

$$\begin{aligned} i_r &= i_{r1}, \qquad j_r = j_{r,c(r)}, \qquad && r = 1, \cdots, k, \\ \phi^{i_r}A_{r1} &= C_r, \qquad \pi^{j_r}A_{r,c(r)} = D_r, \end{aligned} \tag{5.15}$$

where $C_r, D_r \in \mathfrak{E}$ and $\{C_1, \cdots, C_k\} = \{D_1, \cdots, D_k\} = \mathfrak{E}$.

As in the proof of Theorem 8*, we divide the open chains $\mathfrak{C}_r^*$ into classes $\mathfrak{K}_1, \cdots, \mathfrak{K}_e$ by requiring that $\mathfrak{C}_r^*$ and $\mathfrak{C}_s^*$ shall belong to the same class $\mathfrak{K}_u$, if and only if $\mathfrak{C}_r^* \cong \mathfrak{C}_s^*$. Let us arrange the types of chains $\mathfrak{K}$ into a sequence $\mathfrak{K}_{u_1}, \mathfrak{K}_{u_2}, \cdots, \mathfrak{K}_{u_e}$ according to the rule that $\mathfrak{K}_{u_l} {}^\circ{>} \mathfrak{K}_{u_m}$ if $l<m$. Such an arrangement is possible because of the transitivity of left dominance. We shall call l the left index of $\mathfrak{K}_{u_l}$.

Similarly a second arrangement $\mathfrak{K}_{v_1}, \mathfrak{K}_{v_2}, \cdots, \mathfrak{K}_{v_e}$ is obtained by the rule that $\mathfrak{K}_{v_m} <^\circ \mathfrak{K}_{v_l}$ if $l<m$; m is called the right index of $\mathfrak{K}_{v_m}$.

Departing from the group $\mathfrak{A}$ we shall construct now an auxiliary $\mathfrak{R}_{\phi,\pi}$-group $\mathfrak{B}$ so as to satisfy the following conditions:

1. $\mathfrak{B}$ is k-dimensional, where k is the number of open chains in (5.3).

2. Denote by l_r the left index of the class $\mathfrak{K}$ to which $\mathfrak{C}_r^*$ belongs and by m_r the right index of the same class. Write $\mathfrak{F}=\mathfrak{D}(\mathfrak{B})$. Then $\mathfrak{B}^*=\mathfrak{B}/\mathfrak{F}=\{B_1^*\}\oplus\cdots\oplus\{B_k^*\}$, where $\{B_r^*\}$ is an open chain with the invariants $[l_r+1, m_r+1]$.

3. $\mathfrak{F}\cong\mathfrak{E}=\mathfrak{E}(\mathfrak{A})$. Moreover, there is a set of representatives $B_1, \cdots, B_k$ in $\mathfrak{B}$ of the cosets B_r^* such that if we write

$$\phi^{l_r+1}B_r = C_r', \qquad \pi^{m_r+1}B_r = D_r', \qquad C_r', D_r' \in \mathfrak{F}, \tag{5.16}$$

then the mapping $C_r'\to C_r$, $D_r'\to D_r$ is a 1–1 $\mathfrak{R}_{\phi,\pi}$-isomorphism between $\mathfrak{F}$ and $\mathfrak{E}$ (C_r, D_r defined in (5.15)).

These conditions uniquely determine the group $\mathfrak{B}$, provided that $\mathfrak{A}$ is given. We only have to define $\mathfrak{B}$ as the set of symbols

$$B = \sum_{s=1}^{k} \xi_s B_s + \sum_{t=1,0<s\leqq l_t}^{k} \eta_{st}\phi^s B_t + \sum_{t=1,0<s\leqq m_t}^{k} \zeta_{st}\pi^s B_t + \sum_{t=1}^{k}{}^{*}\, \tau_t C_t'$$

where ξ, η, ζ, τ are arbitrary reduced operators and the asterisk above the last summation sign indicates that the summation shall run through such indices t only for which the C_t (or the C_t') are linearly independent. The sum of two elements $\mathfrak{B}$ is then obtained by means of the rules of composition of the C_t in $\mathfrak{A}$.

Since $\mathfrak{E}$ is a proper subgroup of $\mathfrak{D}(\mathfrak{A})$ and $\mathfrak{F}=\mathfrak{D}(\mathfrak{B})$ is isomorphic to $\mathfrak{E}$, the dimension of $\mathfrak{F}$ is smaller than the dimension of $\mathfrak{D}(\mathfrak{A})$, hence the induction hypothesis can be applied to $\mathfrak{B}$. We conclude that $\mathfrak{B}$ is the direct sum of ϕ-π chains.

Let the chain basis elements belonging to this chain decomposition be $\overline{B}_1, \cdots, \overline{B}_k$, whereby we agree that basis elements of the same chain shall have consecutive indices. Since the $\overline{B}_r$ represent chain basis elements of $\mathfrak{B}^*=\mathfrak{B}/\mathfrak{F}$, the open chains $\{\overline{B}_r^*\}$ are, apart from their arrangement, isomorphic to the chains $\{B_r^*\}$ (by Lemma 7). Let us arrange the $\mathfrak{C}_r^*$ in (5.3), hence the B_r so that $\{B_r^*\}\cong\{\overline{B}_r^*\}$ for $r=1, \cdots, k$.

By Condition 2 of the definition of $\mathfrak{B}$ and (5.1), $\overline{B}_r^*$ has a unique representation

$$\overline{B}_r^* = \sum_{s=1}^{k} \xi_s B_s^* + \sum_{t=1,0<s\leqq l_t}^{k} \eta_{st}\phi^s B_t^* + \sum_{t=1,0<s\leqq m_t}^{k} \zeta_{st}\pi^s B_t^*. \tag{5.17}$$

Let the ϕ-exponent of $\overline{B}_r^*$ be l, its π-exponent be m. Evidently the ϕ-exponent of each term in (5.17) with nonzero coefficient is not greater than l and its π-exponent is not greater than m. Suppose we have a nonzero term B^* in (5.17) with $i(B^*)<l$, $j(B^*)<m$. Then by Lemma 5 we could replace $\overline{B}_r$ by $\overline{B}_r-B$ in the chain decomposition of $\mathfrak{B}$, hence $\overline{B}_r^*$ by $\overline{B}_r^*-B^*$, and the representation (5.17) of the new $\overline{B}_r^*$ would not contain the term B^* any more.

Hence, we may assume that every nonzero term in (5.17) has either l for its ϕ-exponent or m for its π-exponent (or both).

This implies (since l, m are both positive) $\eta_{st}=0$ unless $s=l_t-l$ and $\zeta_{st}=0$ unless $s=m_t-m$. Furthermore, since the pair of exponents l, m is identical with one of the pairs l_s, m_s, and by definition $l_s\neq l_t$ implies $m_s\neq m_t$ and conversely, we have $\xi_t=0$ unless $l_t=l$, $m_t=m$. Moreover, at least one $\xi_s\neq 0$ since otherwise we have $\overline{B}_r\in\mathfrak{H}(\mathfrak{B})$, which is impossible since $\overline{B}_r$ is a chain basis element. Hence, writing $\eta_{l_t-l,t}=\eta_t$, $\zeta_{m_t-m,t}=\zeta_t$, and indicating the fact that ζ_s, η_t, ζ_t depend on the index r, we obtain from (5.17),

$$(5.18)\qquad \overline{B}_r^* = \sum_{\{B_s^*\}\cong\{\overline{B}_r^*\}} \xi_{rs}B_s^* + \sum_{l_t>l} \eta_{rt}\phi^{l_t-l}B_t^* + \sum_{m_t>m} \zeta_{rt}\pi^{m_t-m}B_t^*.$$

We can write (5.18) in the form of a chain resultant, namely

$$(5.19)\qquad \{\overline{B}_r^*\} = \sum |+| \xi_{rs}\cdot\{B_s^*\} |+ \sum |+ \eta_{rt}\cdot\{B_t^*\} +| \sum +| \zeta_{rt}\cdot\{B_t^*\},$$

where $\det|\xi_{rs}|\not\equiv 0\ (\phi,\pi)$ by Theorem 8*.

For the representatives in $\mathfrak{B}$ we obtain from (5.18)

$$(5.20)\qquad \overline{B}_r = \sum \xi_{rs}B_s + \sum \eta_{rt}\phi^{l_t-l}B_t + \sum \zeta_{rt}\pi^{m_t-m}B_t + F_r, \qquad F_r\in F.$$

Here we may assume $F_r=0$ since otherwise we could evidently replace $\overline{B}_r$ by $\overline{B}_r-F_r$. Writing $\phi^{l+1}\overline{B}_r=\overline{C}_r'$, $\pi^{m+1}\overline{B}_r=\overline{D}_r'$, we obtain from (5.20) and (5.16)

$$(5.21)\qquad \overline{C}_r' = \sum_s \xi_{rs}C_s' + \sum_t \eta_{rt}C_t', \qquad D_r' = \sum \xi_{rs}D_s' + \sum \eta_{rt}D_t'.$$

Equations (5.19), (5.20) and (5.21) show us how to obtain a chain decomposition for the original group $\mathfrak{A}$. We replace the chains $\mathfrak{C}_r^*$ in (5.3) by new chains $\mathfrak{C}_r'^*$ which are being defined as follows:

$$(5.22)\qquad \mathfrak{C}_r'^* = \sum_{s=1}^{k} |+| \xi_{rs}\mathfrak{C}_s^* |+ \sum_{t=1}^{k} |+ \eta_{rt}\mathfrak{C}_t^* +| \sum_{t=1}^{k} +| \zeta_{rt}\mathfrak{C}_t^*$$

where the coefficients ξ, η, ζ are identical with those in (5.19). In the first sum of (5.22) all the chains occurring with $\xi_{rs}\neq 0$ are isomorphic to each other, hence the forming of the resultant $|+|$ is justified. In the second sum only such terms occur for which $\mathfrak{C}_r'^*>\mathfrak{C}_t^*$, since $l_t>l=l_r$ for the nonzero terms, and l_t is the left index of the class to which $\mathfrak{C}_t^*$ belongs. Similarly, in the third sum only such terms occur for which $\mathfrak{C}_t^*<\mathfrak{C}_r'^*$. Hence, the forming of the resultant (5.22) is justified. By Theorem 8*, $\mathfrak{A}^*=\mathfrak{C}_1'^*\oplus\cdots\oplus\mathfrak{C}_k^*$ since $\det|\xi_{rs}|\not\equiv 0(\phi,\pi)$.

Denote by $\overline{B}_{r\alpha}^*$ the chain basis elements of $\mathfrak{C}_r'^*$, and by $\overline{B}_{r\alpha}$ their representa-

tives in $\mathfrak{A}$ which have been selected so as to satisfy (5.14). Write $\mathfrak{C}_r'$ for the open chain generated by $\overline{B}_{r1}, \overline{B}_{r2}, \cdots$. We have from (5.22) and (5.15)

$$\begin{aligned} \phi^{i_r}\overline{B}_{r1} &= \overline{C}_r = \sum_s \xi_{rs}C_s + \sum_t \eta_{rt}C_t, \\ \pi^{j_r}\overline{B}_{r,c(r)} &= \overline{D}_r = \sum_s \xi_{rs}D_s + \sum_t \zeta_{rt}D_t, \end{aligned} \tag{5.23}$$

where for the moment we denote by i_r the ϕ-chain-exponent of $\overline{B}_{r1}^*$ and by j_r the π-chain-exponent of the last basis element $\overline{B}_{r,c(r)}^*$ of $\mathfrak{C}_r'^*$.

Comparing (5.23) with (5.21) we see (from condition 3 of the definition of B) that if $\overline{B}_r$ and $\overline{B}_{r+1}$ are consecutive basis elements of the same chain in $\mathfrak{B}$, that is, $\overline{D}_r' = \overline{C}_{r+1}'$, then we also have $\overline{D}_r = \overline{C}_{r+1}$ in $\mathfrak{A}$. From this we conclude that if $\overline{B}_1, \cdots, \overline{B}_l$ generate a single open chain, then $\overline{C}_1, \cdots, \overline{C}_l$ also generate an open chain. If $\overline{B}_1, \cdots, \overline{B}_{dl}$ generate a closed chain with period l, that is, $\overline{D}_{dl}' = \sum_{s=0}^{d-1} \lambda_s \overline{C}_{sl+1}'$, then the same relation must hold between the corresponding elements $\overline{D}_{dl}$, $\overline{C}_{sl+1}$. Furthermore, since $\{\overline{B}_s^*\} \cong \{\overline{B}_t^*\}$ for $s \equiv t \pmod{l}$ implies $\mathfrak{C}_s'^* \cong \mathfrak{C}_t'^*$ for $s \equiv t \pmod{l}$, the chain section $\{\mathfrak{C}_1', \cdots, \mathfrak{C}_l'\}$ is isomorphic to $\{\mathfrak{C}_{l+1}', \cdots, \mathfrak{C}_{2l}'\}$, and so on, and $\mathfrak{C}_1', \cdots, \mathfrak{C}_{dl}'$ generate in fact a closed chain, d being the number of its primitive periods. In this way we get $\mathfrak{A}$ decomposed into the direct sum of open and closed ϕ-π chains, parallel to the decomposition of the auxiliary group $\mathfrak{B}$.

The proof shows that an indecomposable $\mathfrak{A}$ is certainly an open or closed ϕ-π chain. To complete the proof of Theorem 4, we still have to show that if $\mathfrak{A}$ has two different decompositions into open and closed chains:

$$\mathfrak{A} = \mathfrak{C}_1 \oplus \cdots \oplus \mathfrak{C}_l = \mathfrak{C}_1' \oplus \cdots \oplus \mathfrak{C}_{l'}', \tag{5.24}$$

then $l = l'$ and $\mathfrak{C}_r \cong \mathfrak{C}_r'$ (or, more precisely, $\mathfrak{C}_r$ and $\mathfrak{C}_r'$ have the same invariants) provided that the chains in the second decomposition are suitably arranged. We shall prove this directly from Theorem 9, without making use of the Krull-Schmidt theorem.

It is easily seen by arguments based on (4.19) in the proof of Theorem 9 that if $\sum \xi_{rb}Q_{rb} \in \mathfrak{E}$, then each $Q_{rb} \in \mathfrak{E}$ for which $\xi_{rb} \neq 0$, hence $\mathfrak{E}$ has a basis consisting of Q-elements of the chains $\mathfrak{C}_r$. Thus there are two chain decompositions of $\mathfrak{A}^* = \mathfrak{A}/\mathfrak{E}$,

$$\mathfrak{A}^* = \mathfrak{C}_1^* \oplus \cdots \oplus \mathfrak{C}_k^* = \mathfrak{C}_1'^* \oplus \cdots \oplus \mathfrak{C}_k'^* \tag{5.25}$$

corresponding to the two decompositions in (5.24).

Without loss of generality we may assume that the chains $\mathfrak{C}_a$ in (5.24) are not isomorphic to any one of the chains $\mathfrak{C}_b'$. Then it follows as in Lemma 9 that all the chains $\mathfrak{C}_r^*$, $\mathfrak{C}_r'^*$ in (5.25) are open chains and $\mathfrak{C}_r^* \cong \mathfrak{C}_r'^*$ for $r = 1, \cdots, k$.

Defining the elements C_r, D_r, C_r', D_r' as in (5.15), we see that all the four sets of elements C_r, D_r, C_r', D_r' form a basis of $\mathfrak{E}$, hence

$$
\begin{aligned}
C_r' &= \sum_s \xi_{rs} C_s, \qquad D_r' = \sum_s \eta_{rs} D_s, \\
C_s &= \sum_r \bar{\xi}_{sr} C_r', \qquad D_s = \sum_r \bar{\eta}_{sr} D_r'.
\end{aligned} \tag{5.26}
$$

It follows from Theorem 9 (applied to the double decomposition (5.25) of $\mathfrak{A}^*$) that in (5.26), $\xi_{rs}=0$ if $\mathfrak{C}_s^{*\circ} > \mathfrak{C}_r'^*$, $\eta_{rs}=0$ if $\mathfrak{C}_r'^* < {}^\circ\mathfrak{C}_s^*$, $\bar{\xi}_{sr}=0$ if $\mathfrak{C}_r'^{*\circ} > \mathfrak{C}_s^*$, $\bar{\eta}_{sr}=0$ if $\mathfrak{C}_s^* < {}^\circ\mathfrak{C}_r'^*$. Moreover, the proof of Theorem 9 shows that $\xi_{rs}=\eta_{rs}$, $\bar{\xi}_{sr}=\bar{\eta}_{sr}$ if $\mathfrak{C}_r'^* \cong \mathfrak{C}_s^*$.

From (5.26) we have $C_r' = \sum_{s,t} \xi_{rs}\bar{\xi}_{st} C_t'$, or, because of the linear independence of the C_r', $\xi_{rs}\bar{\xi}_{st} = \delta_{rt}$ (δ_{rt} = the Kronecker symbol). This implies, since $\bar{\xi}_{st}=0$ for $\mathfrak{C}_t'^{*\circ} > \mathfrak{C}_s^*$ and $\xi_{rs}=0$ for $\mathfrak{C}_s^{*\circ} > \mathfrak{C}_r'^*$, that $\det |\xi_{rs}|_u = \det |\xi_{rs}|_{\mathfrak{C}_r^*, \mathfrak{C}_s^* \in \mathfrak{K}_u} \neq 0$ (ϕ, π).

Let us construct now the auxiliary group $\mathfrak{B}$ to the first of the decompositions (5.25). From the first decomposition in (5.24) it follows that the elements B_r form a chain basis of a decomposition of $\mathfrak{B}$. Let us introduce new basis elements in $\mathfrak{B}$ by

$$
B_r' = \sum_{\mathfrak{C}_r^* \cong \mathfrak{C}_s^*} \xi_{rs} B_s + \sum_{l_t < l_r} \xi_{rt} \phi^{l_t - l_r} B_t + \sum_{m_t > m_r} \eta_{rt} \pi^{m_t - m_r} B_t, \qquad r = 1, \cdots, k.
$$

It follows from Theorem 8* that $\mathfrak{B}/\mathfrak{F} = \mathfrak{B}^* = \{B_1'^*\} \oplus \cdots \oplus \{B_k'^*\}$. It is also seen that the chains $\{B_r'\}$ in $\mathfrak{B}$ are linked to each other in the same way as the chain sections $\{A_{r,1}', A_{r,2}', \cdots\}$ in $\mathfrak{A}$, where the $A_{r,a}'$ denote chain basis elements of the second decomposition (5.24) representing the chain basis elements $A_{r,a}'^*$ of $\mathfrak{C}_r'^*$. Hence, the elements B_r generate a second chain decomposition of $\mathfrak{B}$ which is obviously different from the original one, contrary to the induction hypothesis.

BIBLIOGRAPHY

1. G. Bagnera, Annali di Matematica (3) vol. 1 (1898) pp. 137–228.

2. H. A. Bender, *A determination of the group of order p^5*, Ann. of Math. (2) vol. 29 (1928) pp. 61–72.

3. W. Burnside, *Theory of groups of finite order*, Cambridge, 1911.

4. P. Erdös, *On some asymptotic formulas in the theory of partitions*, Bull. Amer. Math. Soc. vol. 52 (1946) pp. 185–188.

5. P. Hall, *A contribution to the theory of groups of prime power orders*, Proc. London Math. Soc. (2) vol. 36 (1932) pp. 29–95.

6. ———, *The classification of prime power groups*, J. Reine Angew. Math. vol. 182 (1940) pp. 130–141.

7. N. Jacobson, *The theory of rings*, Mathematical Surveys, No. 2, American Mathematical Society, 1943.

8. G. A. Miller, *Determination of all the groups of order p^m which contain the abelian group of type $(m-2, 1)$, p being any prime*, Trans. Amer. Math. Soc. vol. 2 (1901) pp. 259–272.

9. ———, *Determination of all the groups of order p^m, p being any prime, which contain the abelian group of order p^{m-1} and of type* $(1, 1, \cdots)$, Bull. Amer. Math. Soc. vol. 8 (1902) pp. 391–394.

10. H. Rauter, *Eine Erweiterung des Begriffes der Abelschen Gruppe: p-Abelsche Gruppen*, Math. Zeit. vol. 31 (1930) pp. 29–38.

11. L. Rédei, *Das "schiefe Produkt" in der Gruppentheorie*, Comment. Math. Helv. vol. 20 (1947) pp. 225–264.

12. G. Szekeres, *On a certain class of metabelian groups*, Ann. of Math. vol. 49 (1948) pp. 43–52.

13. H. S. Vandiver, *On a p-adic representation of rings and abelian groups*, Ann. of Math. vol. 48 (1947) pp. 22–28.

14. B. L. van d. Waerden, *Moderne Algebra*, vol. 1, Berlin, 1937.

15. ———, *Moderne Algebra*, vol. 2, Berlin, 1931.

16. L. Weisner, *Groups in which the normalizer of every element except identity is abelian*, Bull. Amer. Math. Soc. vol. 31 (1925) pp. 413–416.

17. A. Wiman, *Ueber mit Diedergruppen verwandte p-Gruppen*, Arkiv för Mathematik, Astronomi Och Fysik vol. 33A (1946) p. 12.

18. H. Zassenhaus, *Lehrbuch der Gruppentheorie* I, Hamburger mathematische Einzelschriften, vol. 21, 1937.

THE UNIVERSITY OF ADELAIDE,
ADELAIDE, AUSTRALIA.