METABELIAN GROUPS OF ORDER p^m, $p>2$*

BY

CHARLES HOPKINS

INTRODUCTION

A metabelian group is defined as one whose central quotient-group is abelian.† Since the central quotient-group of any group G is simply isomorphic with the group of inner isomorphisms of G, a metabelian group may also be defined as a group whose group of inner isomorphisms is abelian.‡

Any metabelian group G of order $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$ is the direct product of its Sylow subgroups of order $p_i^{\alpha_i}$. In developing a theory of metabelian groups, it is accordingly reasonable to center the attention upon those of order p^m. In view of the fact that many results which are valid for groups of order p^m, $p>2$, do not hold for $p=2$, it seems advantageous to treat separately the cases $p=2$ and $p>2$. In this article we are concerned exclusively with the case $p>2$.

In §§2–5 we develop, by aid of the theory of regular permutation groups, certain general properties of a metabelian group G of order p^m, $p>2$. We mention the following:

(1) G is conformal with an abelian group A;

(2) the operations of any metabelian group which is conformal with A can be derived by making A isomorphic with a certain subgroup of its group of isomorphisms and multiplying together corresponding operations;

(3) the group of isomorphisms of G is a subgroup of the group of isomorphisms of A.

In §§7–9 we define four different types of bases for G and prove that each of these types occurs in every G. (Any set of elements which generate G is said to constitute a basis for G.) Two of these types, the MB-bases and the U-bases, are of fundamental importance in the theory of metabelian groups. In §§10–11 we exhibit certain relationships between these two types of bases and, furthermore, between the U-bases of G and those of A.

In §§12–14 we discuss the topic of abstract defining relations for G: with reference to a U-basis (§12), an MB-basis (§13), and a U-basis for A (§14).

---

* Presented to the Society, December 27, 1933; received by the editors March 22, 1934.

† W. B. Fite, Proceedings of the American Association for the Advancement of Science, vol. 49 (1901), p. 41.

‡ The term "metabelsche Gruppe," as used by Furtwängler and other German mathematicians, denotes a group whose commutator subgroup is abelian.

Two of the fundamental results of this paper—that G is conformal with an abelian group, and that G possesses a U-basis—have been published in a recent article by P. Hall, entitled *A contribution to the theory of groups of prime power order.** The author, however, feels it desirable to present his original proofs of these two results, as the methods involved are of frequent occurrence throughout this paper.

NOTATION, ELEMENTARY RESULTS

1. In order to avoid repeated explanations, the symbols employed in this article will usually preserve their significance throughout, and accordingly will ordinarily be defined only at their initial appearance.

The letter G will always denote a metabelian group of order p^m, $p>2$. The central and the commutator subgroup of G will be designated by Γ and C respectively. The operations of G will usually be denoted by small letters (s, σ etc.); for the automorphisms of G we shall always use capital letters.

The symbol c_{ij} shall denote the commutator $s_i^{-1}s_j s_i s_j^{-1}$ (or $\sigma_i^{-1}\sigma_j\sigma_i\sigma_j^{-1}$). Since each commutator is invariant in G, of the eight formally distinct commutators which arise from any two operations of G, only two, namely c_{ij} and c_{ji}, will be effectively distinct. Obviously c_{ji} equals c_{ij}^{-1}.

We now mention certain elementary results, which we shall tacitly assume throughout this paper.

(a) If $g_1, g_2, \cdots, g_n$ are any set of independent generating operations (I.G.O.) for G,† then C is generated by $c_{12}=g_1^{-1}g_2g_1g_2^{-1}$, $c_{13}, \cdots, c_{1n}, c_{23}, \cdots, c_{2n}, \cdots, c_{n-1,n}$.

(b) Every operation of G can be expressed in the form $g_1^{x_1}g_2^{x_2}\cdots g_n^{x_n}\cdot c_{12}^{x_{12}}c_{13}^{x_{13}}\cdots c_{n-1,n}^{x_{n-1,n}}$.

(c) If σ_a and σ_b are of orders p^{m_a} and p^{m_b} respectively, $m_a \geqq m_b$, then the order of $\sigma_a\sigma_b$ divides p^{m_a}.‡ From this we see that every set of I.G.O. for G must include operations of highest order in G.

(d) The product of any two pth powers in G is itself a pth power in G.§

DEFINITION. *Any operation of a given prime-power group which is not a pth power of an operation in this group is said to be a "principal element" of this given group.*

---

* Proceedings of the London Mathematical Society, (2), vol. 36, parts 1 and 2, pp. 29–95. The results presented in the author's paper were obtained prior to the appearance of Hall's article.

† That the number of elements in any set of I.G.O. for a prime power group is an invariant of the group was proved by G. A. Miller, these Transactions, vol. 16 (1915), p. 21.

‡ W. B. Fite, these Transactions, vol. 3 (1902), p. 338.

§ P. Hall, loc. cit., p. 75.

RESULTS DERIVED FROM THE REPRESENTATION OF G AS A REGULAR PERMUTATION GROUP

2. Let G denote any metabelian group of order p^m, $p>2$. Regarding G as an abstract group, we denote its operations by the symbols $\sigma_1, \sigma_2, \cdots, \sigma_i, \cdots$.

We denote any permutation s_i of G (in the regular representation derived from post-multiplication) by the symbol $\binom{\sigma}{\sigma\sigma_i}$. We may think of s_i as a representation of σ_i. A representation, as a permutation on the p^m symbols $\sigma_1, \sigma_2, \cdots$, of any inner isomorphism S_i of G is afforded by the symbol $\left(\sigma_i^{-1}\binom{\sigma}{\sigma\sigma_i}\right)$.* Clearly S_i transforms the operations of G according to the permutation s_i. The totality of distinct symbols S constitutes a representation H of the group of inner isomorphisms of G. Any element of $I(G)$, the group of isomorphisms of G, can be represented as a permutation on the letters of G by the symbol $\binom{\sigma}{\sigma'}$.

We may identify $I(G)$ with that subgroup of the holomorph $K(G)$ of G whose permutations omit the symbol for the identity of G.† Under G, $I(G)$ is transformed into p^d conjugates, where p^d equals p^m divided by the number of characteristic operations of G. The totality of distinct permutations in these p^d conjugates coincides with the totality of distinct products $\binom{\sigma}{\sigma_k\sigma}\binom{\sigma}{\sigma'}$, where $\binom{\sigma}{\sigma_k\sigma}$ is any permutation in the conjoint of G, while $\binom{\sigma}{\sigma'}$ is any permutation of $I(G)$.

Let p^μ denote the order of H. One readily sees that H has under G exactly p^μ conjugates.

Now $J \equiv \{G, H\}$ is a metabelian group of order $p^{m+\mu}$. Its central is Γ, its commutator subgroup is C; the central quotient-group J/Γ is the direct product of two simply-isomorphic groups, each of which is simply-isomorphic with H. The chief interest in J attaches to the fact that it contains a remarkable set of subgroups, each of which is conformal with G.

Since H is simply-isomorphic with G/Γ, we obtain an isomorphism of G with H by making each operation s of G correspond to that operation S of H which transforms G according to s. Let θ be defined as the operation of making G isomorphic with H in this manner and then multiplying together corresponding operations. That is, $\theta s = sS$. Similarly, we define θ_x by the equation $\theta_x s = sS^x$. (Since H is abelian, $s_1 \sim S_1^x$, $s_2 \sim S_2^x$, $\cdots$ etc. defines an isomorphism of G with H.) Let p^ν be the order of the operation of highest order in H. If

* This notation is fully explained in Speiser, *Theorie der Gruppen von endlicher Ordnung*, 2d edition, p. 25, p. 121; and in Burnside, *Theory of Groups*, 2d edition, pp. 81 ff.

† We agree that all the permutations of G shall begin with the symbol σ_1 for the identity of G. We may define $I(G)$ as that subgroup of $K(G)$ generated by its permutations which omit the initial letter in the permutations of G.

we let x range over all positive integral values, it is clear that not more than p^r of the operations $\theta_x s$ will be distinct.

By the symbol $\theta_x G$ we designate the set of p^m operations which we obtain by applying to each operation of G the operator θ. We note that Γ is common to G and to $\theta_x G$. If we assume for the moment (we shall prove it below) that $\theta_x G$ is a group for which $\theta_x G/\Gamma$ is simply isomorphic with H, then we may define the symbol $\theta_y \theta_x$ by the equation $\theta_y \theta_x s = \theta_y (s S^x) S^y$. Then $\theta_y \theta_x = \theta_x \theta_y = \theta_{x+y}$. Hence we may write $\theta_x = \theta^x$, regarding θ as an operator of period p^r.

THEOREM I. *The permutations $\theta_x G$ constitute a group which is conformal with G.*

That they constitute a group follows from the equation $(\theta^x s_i)(\theta^x s_j) = c_{ij}^{-x} \theta^x (s_i s_j) = \theta^x (c_{ij}^{-x} s_i s_j)$. That this group is conformal with G is evident from the fact that $\theta^x s$ and s have the same order. (For s and S are commutative and have only the identity in common, since s permutes all the letters of G while S omits σ_1. The order of S divides the order of s, since s and S transform the operations of G in the same way.)

THEOREM II. *Each G_x is an invariant subgroup of the holomorph of G.*

Clearly G is commutative with G_x, since G is commutative with Γ and transforms every coset $\Gamma s S^x$ into itself. To show that $I(G)$ transforms G_x into itself, we proceed as follows.

Let $\begin{pmatrix} \sigma \\ \sigma' \end{pmatrix}$ denote any permutation of $I(G)$. The operation $s_i S_i^x$ of G_x may be represented as

$$\begin{pmatrix} \sigma \\ \sigma\sigma_i \end{pmatrix} \begin{pmatrix} \sigma \\ \sigma_i^{-x} \sigma \sigma_i^x \end{pmatrix}, \text{ which equals } \begin{pmatrix} \sigma \\ \sigma_i^{-x} \sigma \sigma_i^{x+1} \end{pmatrix}.$$

Now

$$\begin{pmatrix} \sigma' \\ \sigma \end{pmatrix} \begin{pmatrix} \sigma \\ \sigma_i^{-x} \sigma \sigma_i^{x+1} \end{pmatrix} \begin{pmatrix} \sigma \\ \sigma' \end{pmatrix} = \begin{pmatrix} \sigma' \\ \sigma_i^{-x} \sigma \sigma_i^{x+1} \end{pmatrix} \begin{pmatrix} \sigma_i^{-x} \sigma \sigma_i^{x+1} \\ \sigma_i'^{-x} \sigma' \sigma_i'^{x+1} \end{pmatrix} = \begin{pmatrix} \sigma' \\ \sigma_i'^{-x} \sigma' \sigma_i'^{x+1} \end{pmatrix}$$

$$= \begin{pmatrix} \sigma \\ \sigma_i'^{-x} \sigma \sigma_i'^{x+1} \end{pmatrix} = \begin{pmatrix} \sigma \\ \sigma\sigma_i' \end{pmatrix} \begin{pmatrix} \sigma \\ \sigma_i'^{-x} \sigma \sigma_i'^{x} \end{pmatrix} = s_i' S_i'^x,$$

where S_i' transforms the operations of G according to s_i'. Since s_i' is an operation of G, $s_i' S_i'^x$ is an operation of G_x. This demonstrates our theorem, since K is generated by G and $I(G)$.

THEOREM III. *Each G_x is a regular group.*

Since G is a regular group on the symbols $\sigma_1, \sigma_2, \cdots, \sigma_i, \cdots$, while every permutation of H omits σ_1, it is obvious that every permutation of G

other than the identity must permute σ_1. Suppose that some permutation t of G_x, distinct from the identity, omits the symbol σ_x. Now G contains a permutation $\bar{s}$ which replaces σ_k by σ_1. But $\bar{s}^{-1}t\bar{s}$ is a permutation of G_x which omits σ_1 (see Theorem II). This proves that each permutation of G_x other than the identity permutes all the symbols $\sigma_1, \sigma_2, \cdots, \sigma_{p^m}$. Since G_x is conformal with G, it must be a regular group on these symbols.

3. These p^ν conformal groups $G_1, G_2, \cdots, G_x, \cdots, G_{p^\nu}=G$ constitute a set which we shall refer to as D. As permutation groups in $K(G)$, they are all distinct. We shall prove shortly that regarded as abstract groups exactly $\nu+1$ of them are distinct.

Let $t_i=s_iS_i^x$ and $t_j=s_jS_j^x$ be any two operations of G_x. Now $t_i^{-1}t_jt_i=t_jc_{ij}^{2x+1}$, where $c_{ij}=s_i^{-1}s_js_is_j^{-1}$.* If $2x+1$ is prime to p, then the commutator subgroup of G_x coincides with the commutator subgroup C of G. If $2x+1$ is divisible by p but not by p^2, then the commutator subgroup of G_x is composed of the pth powers of the elements of C. By means of the relation $y\equiv 2x+1 \pmod{p^\nu}$, we may associate with each member of D a value of y as a subscript. The $p^{\nu-1}(p-1)$ members of D for which y is prime to p constitute a subset which we call D_1; the $p^{\nu-2}(p-1)$ members of D for which y is divisible by p, but not by p^2, we shall put into a set D_p, etc. Set D_{p^ν} consists of a single group, namely that G_x for which $2x+1$ is divisible by p^ν. This group, which is abelian, we shall designate by the letter A. Its permutations $t_1, t_2, \cdots, t_i, \cdots$ are connected with those of G by the equation $t_i=\theta^a s_i$, where a is the smallest positive root of $2a+1\equiv 0 \pmod{p^\nu}$. That G_a is abelian is sufficiently important to state as a theorem.

THEOREM I. *The p^m products $t_i=\theta^a s_i$, $i=1, 2, \cdots, p^m$, constitute a regular abelian group A which is conformal with G.*

The conjoint of each group in a given set D_{p^α}, $\alpha=0, 1, \cdots, \nu$, is a member of the same set. If y has the value k for a given group G_x, then y will be congruent to $-k$ modulo p^ν for the conjoint of G_x. (It is easy to prove that the conjoint of G_x is $G_{p^\nu-x-1}$.)

THEOREM II. *The groups in any given set D_{p^α}, $\alpha=0, 1, \cdots, \nu$, are simply isomorphic.*

Let λ be an integer prime to p. If we replace each operation of G_x by its λth power, then we shall obtain all the operations of G_x in some order. Let

$$T_\lambda = \begin{pmatrix} \sigma \\ \sigma^\lambda \end{pmatrix}$$

* It is a simple task to verify the relations $s_i^{-1}S_js_i=S_jc_{ij}$ and $S_i^{-1}s_jS_i=s_jc_{ij}$. Of course $S_i^{-1}S_jS_i=S_j$.

be the permutation on the symbols $\sigma_1, \sigma_2, \cdots$ derived from associating each operation of G with its λth power. Since T_λ defines an automorphism of the abelian group Γ, in determining how T_λ transforms the operations of G_x we shall be concerned only with the non-invariant operations of G_x.

Let $t_i = s_i S_i^x$ be any non-invariant operation of G_x. We may write

$$t_i = \begin{pmatrix} \sigma \\ \sigma_i^{-x}\sigma\sigma_i^{x+1} \end{pmatrix}.$$

Then

$$T_\lambda^{-1} t_i T_\lambda = \begin{pmatrix} \sigma^\lambda \\ \sigma \end{pmatrix}\begin{pmatrix} \sigma \\ \sigma_i^{-x}\sigma\sigma_i^{x+1} \end{pmatrix}\begin{pmatrix} \sigma \\ \sigma^\lambda \end{pmatrix} = \begin{pmatrix} \sigma^\lambda \\ [\sigma_i^{-x}\sigma\sigma_i^{x+1}]^\lambda \end{pmatrix}.$$

Now

$$[\sigma_i^{-x}\sigma\sigma_i^{x+1}]^\lambda = \sigma_i^\lambda [\sigma^{-x}\sigma\sigma_i^x]^\lambda c_{i\sigma}^{\lambda(\lambda+1)/2},$$

where $c_{i\sigma}$ is $\sigma_i^{-1}\sigma\sigma_i\sigma^{-1}$. Moreover,

$$[\sigma_i^{-x}\sigma\sigma_i^x]^\lambda = \sigma_i^{-x}\sigma^\lambda\sigma_i^x.$$

Hence

$$[\sigma_i^{-x}\sigma\sigma_i^{x+1}]^\lambda = \sigma_i^\lambda(\sigma_i^{-x}\sigma^\lambda\sigma_i^x)c_{i\sigma}^{\lambda(\lambda+1)/2}.$$

Since 2 is prime to p, the congruence $2z \equiv 1 \pmod{p^r}$ always admits a unique solution z. Therefore, we are justified in using the symbol $(\lambda+1)/2$, even when $\lambda+1$ is an odd integer. Now

$$\sigma^\lambda c_{i\sigma}^{\lambda(\lambda+1)/2} = \sigma_i^{-(\lambda+1)/2}\sigma^\lambda\sigma_i^{(\lambda+1)/2} = \sigma_i^{-(\lambda+1)/2}(\sigma_i^{-x}\sigma^\lambda\sigma_i^x)\sigma_i^{(\lambda+1)/2}.$$

Hence one may write

$$[\sigma_i^{-x}\sigma\sigma_i^{x+1}]^\lambda = \sigma_i^{-(1-\lambda)/2}(\sigma_i^{-x}\sigma^\lambda\sigma_i^x)\sigma_i^{(1-\lambda)/2+\lambda} = \sigma_i^{-(1-\lambda+2x)/2}\sigma^\lambda\sigma_i^{(1-\lambda+2x)/2}\sigma_i^\lambda.$$

Then

$$T_\lambda^{-1} t_i T_\lambda = \begin{pmatrix} \sigma \\ \sigma_i^{-(1-\lambda+2x)/2}\sigma\sigma_i^{(1-\lambda+2x)/2}\sigma_i^\lambda \end{pmatrix} = s_i^\lambda S_i^{(1-\lambda+2x)/2}.$$

Let us put $1-\lambda+2x \equiv 2\lambda\xi \pmod{p^r}$. Then $s_i^\lambda S_i^{\lambda\xi}$ is an operation of G_ξ. If we write the congruence above in the form $1+2x \equiv \lambda(1+2\xi) \pmod{p^r}$, it is clear that the same power of p divides both $1+2x$ and $1+2\xi$. This demonstrates our theorem. If G_x is the abelian group A, then $1+2x$ (and conse-

quently $1+2\xi$) is divisible by p^ν. We can, therefore, identify the permutation T_λ with that automorphism of A which transforms each operation of A into its λth power.

If we restrict the values of λ to the $p^{\nu-1}(p-1)$ positive integers which are less than p^ν and prime to p, then the permutations T_λ constitute a cyclic group of order $p^{\nu-1}(p-1)$. We may identify each T_λ with the linear substitution X_λ on the subscripts of $G_1, G_2, \cdots, G_x, \cdots$, where X_λ is $x' \equiv a[1-\lambda'(2x+1)] \pmod{p^\nu}$, while a and λ' are defined by the congruences $2a+1 \equiv 0 \pmod{p^\nu}$ and $\lambda\lambda' \equiv 1 \pmod{p^\nu}$. Or we can represent T_λ as the linear substitution $Y_\lambda: y' \equiv \lambda' y \pmod{p^\nu}$. The order of T_λ is obviously the period of λ with respect to p^ν. When λ is $p^\nu-1$, then T_λ represents a substitution of order 2 in the double holomorph of G which transforms each G_x into its conjoint.

4. At this point we review certain results from §§2–3, which will be of service to us in what follows. Commencing with a representation of G as a regular permutation group, whose permutations $s_1, s_2, \cdots$ all begin with the same letter σ_1, we designate the holomorph of G (on these letters) by $K(G)$. We let $I(G)$ denote that representation in $K(G)$ of the group of isomorphisms of G whose permutations all omit σ_1. The subgroup of $I(G)$ which gives the inner isomorphisms of G we shall denote by H. We let $S_1, S_2, \cdots$ denote the permutations of H, where S_i transforms G according to s_i. Furthermore, p^ν denotes the order of the element of highest order in H, while a is the least positive root of $2a+1 \equiv 0 \pmod{p^\nu}$. Theorem I of §3 states that (a) the p^m elements $t_i = \theta^a s_i = s_i S_i^a$ constitute a regular abelian group A on the letters of G. Let $K(A)$ denote the holomorph of A (on these same letters), and let $I(A)$ denote that representation in $K(A)$ of the group of isomorphisms of A whose permutations omit σ_1. Since $I(G)$ is a subgroup of $I(A)$,* H is in $I(A)$. Throughout the remainder of this article the symbols defined above will preserve their significance.

We know that there is only one permutation in $I(G)$ which transforms the permutations of G in a prescribed manner. Hence, given s_i in the equation $t_i = \theta^a s_i$, we see that t_i is uniquely determined. Conversely, given t_i in this equation, s_i is uniquely given by $t_i S_i^{-a}$. We recall that S_i^{-a} is in $I(A)$. We may, therefore, state that (b) the permutations in a given regular representation of G may be obtained from those of A by making A isomorphic with a certain subgroup of $I(A)$ and multiplying together corresponding operations. This result is clearly trivial in the sense that we cannot determine the "certain subgroup" unless we already know the permutations of G. The real point of (b) is expressed in the following theorem.

* See Theorem II of §2.

THEOREM I. *Let $t_1, t_2, \cdots$ denote the permutations of A and let $R_1, R_2, \cdots$ denote the permutations of a subgroup $\overline{R}$ of $I(A)$. Let γ_{ij} denote the commutator $R_i^{-1}t_jR_it_j^{-1}$, and* (c) *let every product $\gamma_{ij}\gamma_{ji}^{-1}$ be invariant under $\overline{R}$. If the correspondence $\Gamma\sim E, \cdots, \Gamma t_i\sim R_i, \cdots$ defines an isomorphism τ of A with $\overline{R}$ for which* (d) *Γ contains every γ_{ij}, then the p^m products*

$$\Gamma E, \cdots, \Gamma t_iR_i, \cdots \tag{1}$$

*constitute a metabelian subgroup $\overline{G}$ of $K(A)$ which is conformal with A.**

From (d) we know that the product of any two elements in the set (1) is itself in the set. That the p^m products (1) are all distinct follows from the fact that A and $\overline{R}$ have only the identity in common. That these products constitute a metabelian group is a consequence of (c). From the existence of τ we know that the order of R_i divides the order of t_i. Although R_i and t_i are not necessarily commutative, a simple computation will show that t_iR_i and t_i have the same order. From this it will follow that $\overline{G}$ is conformal with A.†

To show that we obtain every regular metabelian group in $K(A)$ which is conformal with A by employing, in the procedure of Theorem I, every "permissible" subgroup $\overline{R}$ of $I(A)$, it is clearly sufficient to show that $\overline{G}$ is a regular permutation group. For we know that the permutations of a given regular permutation group G in $K(A)$ can be derived from those of A by the equation $s_i = t_iS_i^{-a}$. In §5 we shall prove that every $\overline{G}$ is a regular group.

That a representation as a regular permutation group of each of the abstractly distinct metabelian groups which are conformal with G may be obtained by the process of Theorem I, is a direct consequence of the following:

THEOREM II. *The holomorph $K(A)$ contains a regular representation of each of those abstractly distinct metabelian groups which are conformal with A.*

---

* The identical operation of any group is denoted by the letter E.

† We observe that t_i and R_i need not be commutative; moreover, the γ_{ij} need not be separately invariant under $\overline{G}$. But it is obvious that every commutator $R_k^{-1}\gamma_{ij}R_k\gamma_{ij}^{-1}$ must be invariant under $\overline{G}$, and hence under $\overline{R}$. That is, the class of $\{A, \overline{R}\}$ cannot exceed 2.

This derivation of $\overline{G}$ from A and $\overline{R}$ is a special example of a more general "composition" of two groups. We refer to the following theorem:

Let Q and Q' be two finite groups of orders m and m' respectively, for which the following conditions hold: (a) *the cross-cut of Q and Q' is the identity*; (b) *Q' transforms Q into itself*; (c) *Q and Q' are isomorphic under the correspondence $\overline{Q}\sim E, \cdots, \overline{Q}q_i\sim q_i', \cdots$, where $\overline{Q}$ contains all commutators $q_j'^{-1}q_kq_j'q_k^{-1}$, q_k and q_j' being any two elements of Q and Q' respectively. Then the m products*

$$\overline{Q}E, \cdots, \overline{Q}q_iq_i', \cdots \tag{1}$$

constitute a group Q'' of order m.

From (c) it is clear that $q_iq_i'q_jq_j'$ can be brought into the form $q_{ij}q_iq_jq_i'q_j'$, where q_{ij} is in $\overline{Q}$. That is, the product of any two elements in (1) is in the set (1). From (a) we see that these m products are distinct, since $q_iq_i' = q_jq_j'$ leads to $q_j^{-1}q_i = q_j'q_i'^{-1} = E$.

Of course, Q'' and Q are usually not conformal. The simplest additional restriction which will ensure their being conformal is probably that given by $q_iq_i' = q_i'q_i$.

Let G and G' be any two such groups, each being represented as a regular permutation group. Then $K(A)$ on the letters of G and $K(A)$ on the letters of G' are conjugate under some permutation. Hence G' occurs as a regular group in the holomorph $K(A)$ (on the letters of G).

5. In this section we develop several theorems which, in the main, are generalizations of theorems in §§2–3. The symbol $\overline{G}$ is the same as in Theorem I of §4.

THEOREM I. *Each $\overline{G}$ is transformed into itself by the permutations of A,* and conversely.*

We regard the elements of $\overline{G}$ as a certain p^m products t_iR_i (see Theorem I of §4). We write $\overline{G}$ in cosets with respect to $\overline{\Gamma}$, where $\overline{\Gamma}$ is the subgroup of $\overline{G}$ (and of A) composed of those products for which R_i is the identity. Then the permutations of A transform each of these cosets into itself. This proves the first part of our theorem. The converse is obvious.

THEOREM II. *Each $\overline{G}$ is a regular group.*

As above, we regard the elements of G as the products t_iR_i. Since each permutation of $I(A)$ omits σ_1, the initial letter in the permutations of A, we see that every permutation in $\overline{G}$ permutes σ_1. If a certain permutation, say $\bar{t}$, of $\overline{G}$ should omit the letter σ_k, then we could find a permutation t in A such that $t^{-1}\bar{t}t$ would omit σ_1. From Theorem I of this section we know that this transform is in G. Hence each permutation of G permutes all the letters of A; G is accordingly regular, since it is conformal with A.

THEOREM III. *All simply-isomorphic regular metabelian groups G' in $K(A)$ which are conformal with A constitute a complete set of conjugates under $I(A)$.*

Let G' and G'' be any two of these simply-isomorphic regular groups in $K(A)$. Since G' and G'' are both regular, they are conjugate under some permutation on the letters of A. Our objective is to show that one such permutation occurs in $I(A)$.

We denote the group of inner isomorphisms of G' by H', and that of G'' by H''. Of course we regard H' and H'' as subgroups of $I(A)$. Let Γ' and Γ'' denote the centrals of G' and G'' respectively. Obviously Γ' and Γ'' are simply-isomorphic subgroups in A. We denote the permutations of G' by $s_1', s_2', \cdots$ and those of H' by $S_1', S_2', \cdots$, where S_i' transforms G' according to s_i'. We adopt a corresponding notation for G'' and H''.

To each permutation of A we assign two symbols, t' and t'', in such a

* Of course, we regard A as derived from a regular representation of a given metabelian group G.

way that the permutations of G' and A (G'' and A) are connected by the equation $t_i' = s_i' S_i'^{\alpha}$ ($t_i'' = s_i'' S_i''^{\alpha}$). We write $\bar{S}_i'$ for $S_i'^{-\alpha}$ and $\bar{S}_i''$ for $S_i''^{-\alpha}$. Then the permutations of G' and of G'' are derivable from those of A by the equations

$$s_i' = t_i' \bar{S}_i' \tag{1}$$

and

$$s_i'' = t_i'' S_i'' \tag{2}$$

respectively.

We may choose our notation so that a simple isomorphism between G' and G'' is defined by the correspondence

$$\Gamma' \sim \Gamma'', \cdots, \Gamma' t_i' \bar{S}_i' \sim \Gamma'' t_i'' \bar{S}_i'', \cdots, \Gamma' t_j' \bar{S}_j' \sim \Gamma'' t_j'' \bar{S}_j'', \cdots . \tag{3}$$

Now (3) requires that H' and H'' be isomorphic under the correspondence

$$\cdots, \bar{S}_i' \sim \bar{S}_i'', \cdots, \bar{S}_j' \sim \bar{S}_j'', \cdots . \tag{4}$$

Since the product $s_i' s_j'$ corresponds to $s_i'' s_j''$, we obtain $\gamma_{ij}' t_i' t_j' \bar{S}_i' \bar{S}_j' \sim \gamma_{ij}'' \cdot t_i'' t_j'' \bar{S}_i'' \bar{S}_j''$, where $\gamma_{ij}' = \bar{S}_i' t_j' \bar{S}_i'^{-1} t_j'^{-1}$ and $\gamma_{ij}'' = \bar{S}_i'' t_j'' \bar{S}_i''^{-1} t_j''^{-1}$. Since γ_{ij}' must correspond to γ_{ij}'' under (3), we get

$$(t_i' t_j')(\bar{S}_i' \bar{S}_j') \sim (t_i'' t_j'')(\bar{S}_i'' \bar{S}_j''). \tag{5}$$

From (4) and (5) we see that (3) involves an automorphism of A, defined by the correspondence

$$\Gamma' \sim \Gamma'', \cdots, \Gamma' t_i' \sim \Gamma'' t_i'', \cdots, \Gamma' t_j' \sim \Gamma'' t_j'', \cdots . \tag{6}$$

Let $\overline{\Pi}$ be the permutation in $I(A)$ which brings about the automorphism (6). Now $\overline{\Pi}$ transforms G' into a simply-isomorphic group $\overline{\Pi}^{-1} G' \overline{\Pi}$, and one readily sees that the permutations of these two groups correspond according to

$$\Gamma' \sim \Gamma'', \cdots, \Gamma' t_i' \bar{S}_i' \sim \Gamma'' t_i'' \overline{\Pi}^{-1} \bar{S}_i' \overline{\Pi}, \cdots . \tag{7}$$

Since $\overline{\Pi}^{-1} \gamma_{ij}' \overline{\Pi}$ equals γ_{ij}'', it follows that $\overline{\Pi}^{-1} \bar{S}_i' \overline{\Pi}$ and $\bar{S}_i''$ transform the permutations of A in the same way. But there is only one permutation in $I(A)$ which transforms A in a prescribed manner. Hence $\bar{S}_i''$ is $\overline{\Pi}^{-1} \bar{S}_i' \overline{\Pi}$ and G'' coincides with $\overline{\Pi}^{-1} G' \overline{\Pi}$. This completes the demonstration of Theorem III.

As a direct consequence of Theorem III we have

THEOREM IV. *A representation $I(G')$ of the group of isomorphisms of every G' occurs as a subgroup of $I(A)$.*

From Theorem III and Theorem IV follows

THEOREM V. *The number of distinct representations of G' in $K(A)$ equals the index of $I(G')$ in $I(A)$.*

THEOREM VI. *Those conjugates of G' (under $I(A)$) which are in the holomorph $K(G')$ of G' are commutative, each with each, and conversely.*

The proof is elementary. Equally obvious is

THEOREM VII. *The holomorph $K(G')$ is invariant in $K(A)$ if, and only if, the commutator subgroup of G' is a characteristic subgroup of A.*

In retrospect: Theorem I of §4 provides, theoretically at least, a means of constructing a regular representation of each of the abstractly distinct metabelian groups which are conformal with a given one G. By using every subgroup $\overline{R}$ of $I(A)$ which satisfies the conditions laid down in this theorem, we obtain the totality of regular metabelian groups in $K(A)$ which are conformal with A. Obviously we obtain this same totality of groups by subjecting the elements of $\overline{R}$ to the following additional restrictions: each γ_{ij} is invariant under $\overline{R}$; $\gamma_{ij}=\gamma_{ji}^{-1}$ (whence follows $\gamma_{ii}=E$).

The process of Theorem I in §4 does not, in general, yield all the metabelian groups in $K(A)$ which are conformal with A. In fact, when A has more than 2 I.G.O., then $K(A)$ always contains non-regular metabelian groups which are conformal with A. We shall not prove this statement; the demonstration is fairly obvious. Instead, we present the following example.

Let A be a representation as a regular permutation group of the abelian group of order 27 and type 1, 1, 1. We begin all the permutations of A with letter a_1; we denote by $I(A)$ the subgroup of $K(A)$ composed of the permutations of $K(A)$ which omit a_1. Now we can find in A three permutations A_1, A_2, A_3 which generate A. Also, we can find in $I(A)$ a permutation π of order 3 which is commutative with A_1 and A_3 and transforms A_2 into A_2A_1. We see that π permutes exactly 18 letters. Since π transforms $\{A_1, A_2\}$ into itself, it follows that $\{A_1, A_2, \pi\}$ is a metabelian group of order 27, each of whose operations is of order 3. This group is clearly not a regular group. It is of course simply isomorphic with the regular permutation group $\overline{G}=\{A_1, A_2, A_3\pi\}$, since all metabelian groups conformal with this given A are abstractly identical.

ARITHMETICAL INVARIANTS OF G

6. Associated with every given metabelian group G are the following uniquely-determined abelian groups: A, C, Γ, G/C, G/Γ (which is simply isomorphic with H). From each of these groups there arises a set of arith-

metical invariants of G. We enumerate the following:

(1) the r invariants $p^{\delta_1}, p^{\delta_2}, \cdots, p^{\delta_r}$ of A;
(2) the l invariants $p^{q_1}, \cdots, p^{q_l}$ of C;
(3) the invariants $p^{\nu}, p^{\nu}, p^{\nu_3}, \cdots, p^{\nu_h}$ of G/Γ;
(4) the invariants of Γ;
(5) the invariants of G/C.

To these we add

(6) the number n of I.G.O. for G. We may assume that for each set the invariants are arranged in descending order of magnitude.

We shall not go into the question of relationships between these six invariants other than to note that q_1 equals ν, while G/Γ must clearly have at least two invariants of highest order.

There are two additional invariants of G which are of considerable importance for the development of our theory. These we now proceed to define. Following the notation of Hall, we denote by $\mathfrak{V}_\alpha$ the subgroup composed of the p^αth powers of the elements of G. These groups $\mathfrak{V}_\alpha$ constitute a series of characteristic subgroups $\mathfrak{V}_1, \mathfrak{V}_2, \cdots, \mathfrak{V}_{\delta_1}=E$ of G, each being contained in those which precede it.* For C we define the series $C_1, C_2, \cdots, C_\nu=E$, where C_α is the subgroup composed of the p^αth powers of the elements of C. Finally we have a third series $\overline{C}_1, \overline{C}_2, \cdots, \overline{C}_\nu=E$, where $\overline{C}_\alpha$ is the subgroup composed of those elements of C which are in $\mathfrak{V}_\alpha$. Obviously $\overline{C}_\alpha$ contains C_α. In what follows we shall be concerned exclusively with the case $\alpha=1$, i.e. with the first term in each of these three series.

The two additional invariants of G, to which we referred above, are the following:

(7) the number l_1 of invariants of $C/\overline{C}_1$;
(8) the number l_2 of invariants of $\overline{C}_1/C_1$.†

Since $C/\overline{C}_1$ and $C/C_1 \div \overline{C}_1/C_1$ are simply-isomorphic, we have $l_1+l_2=l$.

For the case where $C/\overline{C}_1$ is the identity there arise so many important simplifications of the general theory that it is desirable to assign a name to those groups G for which $C \equiv \overline{C}_1$. Such groups we shall call *ω-groups*. An immediate illustration of their significance is provided by

THEOREM I. *The quotient group $G/\mathfrak{V}_1(G)$ is abelian if, and only if, G is an ω-group.*

The proof follows from the fact that $C/\overline{C}_1$ is the commutator subgroup of

* Hall, loc. cit., p. 78.

† Obviously the two quotient-groups $C/\overline{C}_1$ and $\overline{C}_1/C_1$ are of type 1, 1, $\cdots$.

$G/\mathfrak{V}_1(G)$.*

For certain small values of m (for $m=3$ and $m=4$, in particular) these eight invariants characterize G. It would be an interesting problem to determine whether for every order of G there exists a set of arithmetical invariants which completely characterize G: that is, determine G to within an isomorphism.

At this point we mention several useful properties of the ϕ-subgroup $\Phi(G)$ of G. That (a) $\Phi(G)$ is the cross-cut of all subgroups of index p in G, and that (b) G/Φ is of order p^n and type $1, 1, \cdots, 1$, are two familiar results in the theory of prime-power groups. From (b) it follows that $\Phi(G)$ is generated by $\mathfrak{V}_1(G)$ and C.

Now $\Phi(A)$, the ϕ-subgroup of A, coincides with $\mathfrak{V}_1(A)$. Obviously $\mathfrak{V}_1(A)$ is $\theta^a\mathfrak{V}_1(G)$. Since $\theta^a C$ is C itself, we have

THEOREM II. *The quotient-group $\theta^a\Phi(G)/\Phi(A)$ coincides with $C/\overline{C}_1$, and is accordingly of type $1, 1, \cdots, 1$ to l_1 factors.*

From Theorem II follows

THEOREM III. *For G to be an ω-group it is necessary and sufficient that r equal n. If G is not an ω-group, then $r-n$ must equal l_1.*

We mention here two rather obvious results, which will be of use to us in what follows. The first is the following: if $g_1, \cdots, g_n$ are a set of I.G.O. for G, then no product $g_1^{x_1}g_2^{x_2}\cdots g_n^{x_n}$ in which an exponent is prime to p can be in $\Phi(G)$. The second is

THEOREM IV. *If G is an ω-group, then every operation of G can be expressed in the form $g_x = g_1^{x_1}g_2^{x_2}\cdots g_n^{x_n}$.*

To prove this, we note that every operation σ in G can be expressed in the form $g_v c$, where g_v is $g_1^{v_1}g_2^{v_2}\cdots g_n^{v_n}$ and c is some element in C. Since C is in $\mathfrak{V}_1(G)$, c can be expressed as $(g_z c')^p$. Then σ can be brought into the form $g_v g_z{}^p c'^p = g_{v'}c''$. Since the order of c'' is less than the order of c, we can eventually bring σ into the form g_x above.

BASES FOR G

7. Any set of elements $g_1, g_2, \cdots$ which generate G we shall call a basis for G. In the classical theory of abelian groups the term *basis for Q*, where Q is an abelian group, is used to designate a set of elements $q_1, q_2, \cdots$ of Q such that Q is the direct product of the cyclic subgroups $\{q_1\}, \{q_2\}, \cdots$. To

* From a theorem of Hall (loc. cit., p. 83) it results that $\mathfrak{V}_\alpha/\mathfrak{V}_{\alpha+1}$ is abelian for $\alpha>1$. More generally, $\mathfrak{V}_\alpha/\mathfrak{V}_{\alpha+\beta}$ is abelian for $\alpha>1$ and $\alpha\geqq\beta$.

avoid confusion, a basis for Q of this sort we shall refer to as a U-basis for Q. The fact that every abelian group has a U-basis constitutes the so-called fundamental theorem in the theory of abelian groups.

We now define four different types of bases for G. For the first three types we start with a set of I.G.O. for G, namely $g_1, g_2, \cdots, g_n$. Let g_x be any product $g_1^{x_1}g_2^{x_2}\cdots g_n^{x_n}$ in which the g_i occur, without repetitions, in the normal order $g_1, g_2, \cdots$ etc.*

(1) If g_x is an element in C only when each factor $g_i^{x_i}$ is in C, then $g_1, \cdots, g_n$ are said to constitute a *C-basis* for G.

(2) If g_x is in Γ only when each factor $g_i^{x_i}$ is in Γ, then the g's are said to constitute a Γ-*basis* for G.

(3) If g_x is the identity only when each $g_i^{x_i}$ is the identity, the g's are said to constitute a *B-basis* for G.

A set of elements $P_1, P_2, \cdots, P_\rho$ is said to constitute a *uniqueness-basis* (*U-basis*) for G provided that each operation of G can be represented uniquely in the form $P_1^{x_1}P_2^{x_2}\cdots P_\rho^{x_\rho}$, where each exponent is a least positive residue modulo the order of the P to which it belongs.

In what follows we shall prove that each of these four types of bases occurs in any given metabelian group G. To prove the existence of a C-basis is a simple task. We write G in cosets with respect to C and select from every coset which corresponds to an element of a given U-basis for G/C an operation v_i. Now $v_1^{x_1}v_2^{x_2}\cdots$ is clearly in C only if each $v_1^{x_1}$, $v_2^{x_2}$, etc., is in C. It remains only to show that these v's constitute a set of I.G.O. for G. That they do is readily apparent from the relation $G/\Phi(G) \equiv G/C \div \Phi(G)/C$.

To construct a Γ-basis for G we first write G in cosets with respect to Γ; then, from each of those cosets which correspond to the elements of a U-basis for G/Γ, we select an operation of G, obtaining thereby the h operations $u_1, u_2, \cdots, u_h$.

If $h=n$, then $u_1, u_2, \cdots, u_h$ will constitute a set of I.G.O. for G. For $u_x = u_1^{x_1}u_2^{x_2}\cdots u_h^{x_h}$ is non-invariant in G unless each x_i is divisible by p^{r_i}; we know that $\Phi(G)$ is $\{\mathfrak{V}_1(G), C\}$; hence u_x cannot be in $\Phi(G)$ unless each x is divisible by p.

If h is less than n, we can extend $u_1, \cdots, u_h$ to a set of I.G.O. for G by adding a certain $n-h$ elements $u_{h+1}, \cdots, u_n$. To show that these $n-h$ elements may be chosen from Γ, we observe that $G/\{u\}$ and $\Gamma/\overline{\Gamma}$ are simply-isomorphic, where $\{u\}$ is the group generated by $u_1, \cdots, u_h$, and $\overline{\Gamma}$ is the cross-cut of $\{u\}$ and Γ. Consequently $G \equiv \{\Gamma, \{u\}\}$; hence $u_{h+1}, \cdots, u_n$ may be taken from Γ.

* Throughout this paper it is assumed that in any indicated product, such as $A_1^{x_1}\cdots A_r^{x_r}$, $P_1^{x_1}\cdots P_r^{x_r}$ etc. no subscript is repeated.

We shall make no further use of these two types of bases. It is, perhaps, worthwhile to point out that for a given G it is usually impossible to construct a basis whose elements satisfy any two of the conditions (1), (2), (3) above. But there are large and important categories of groups G for which every C-basis is a U-basis. We mention, in particular, those groups G for which $h=n$ and G/Γ is of type $\alpha, \alpha, \cdots, \alpha$. Those groups G in which every element (except the identity) is of order p provide a trivial illustration of the case where every C-basis is simultaneously a Γ-basis and a B-basis.

8. We shall now prove that every metabelian group G contains a B-basis. That is, we shall show that there always exists a set of n I.G.O., $\beta_1, \beta_2, \cdots, \beta_n$ with the property that $\beta_1^{\lambda_1}\beta_2^{\lambda_2}\cdots\beta_n^{\lambda_n}$ is the identity only when each $\beta_i^{\lambda_i}$ is the identity.*

We first prove the theorem for groups having two I.G.O. Every set of I.G.O. must include at least one operation of highest order in G. Let β_1 be such an operation, and let β_2 be an operation in G of lowest possible order such that β_1 and β_2 generate G. We shall now prove that $\{\beta_1\}$ and $\{\beta_2\}$ can have only the identity in common.

Suppose that $\beta_2^{-p^{e_2}}=\beta_1^{bp^{e_1}}$, where $\beta_2^{-p^{e_2}}$ is not the identity. Since β_1 is of highest order in G, we may put $e_1=e_2+e_3$, where $e_3\geqq 0$. Now

$$\left[\beta_2\beta_1^{bp^{e_3}}\right]^{p^{e_2}} = \beta_1^{bp^{e_1}}\beta_2^{p^{e_2}}\left[\beta_2\beta_1^{bp^{e_3}}\beta_2^{-1}\beta_1^{-bp^{e_3}}\right]^{p^{e_3}(p^{e_2}+1)/2}.$$

(Since p is an odd prime, $(p^{e_2}+1)/2$ is an integer; since $\beta_2^{p^{e_2}}$ is commutative with β_1, the order of the element in the brackets divides p^{e_2}.) Clearly β_1 and $\beta_2\beta_1^{bp^{e_3}}$ generate G. But the order of this second operation is less than the order of β_2, contrary to assumption. Our theorem, then, is true when G has two I.G.O.

We proceed by induction, assuming the validity of the theorem for all groups which have less than n I.G.O. Suppose, now, that G has n I.G.O. Among the operations of G which can occur in a set of I.G.O., let $\bar{s}$ be one of the smallest possible order. We consider the totality of sets of I.G.O. in which $\bar{s}$ occurs. For any one of these sets, say $\bar{s}_1, \bar{s}_2, \cdots, \bar{s}_{n-1}, \bar{s}$ the first $n-1$ elements generate a metabelian (or abelian) subgroup $\overline{H}$ of G. Since G is $\{\overline{H}, \bar{s}\}$, it is clear that $\overline{H}$ has exactly $n-1$ I.G.O. Hence for $\overline{H}$ we can find a B-basis, say $\beta_1, \beta_2, \cdots, \beta_{n-1}$. We now show that $\beta_1, \cdots, \beta_{n-1}, \bar{s}=\beta_n$ must constitute a B-basis for G. Let us assume the contrary; that is, let $\beta_1^{\lambda_1}\beta_2^{\lambda_2}\cdots\beta_{n-1}^{\lambda_{n-1}}\beta_n^{\lambda_n}=E$, where at least one of the λ's is not divisible by the order of the β to which it belongs. Certainly one of these λ's must be λ_n, since $\beta_1, \cdots, \beta_{n-1}$

* This result, in a slightly different form, was proved earlier by the author: Annals of Mathematics, vol. 29 (1928), pp. 6–9.

are a B-basis for $\overline{H}$. We have, then, $\beta_n^{\lambda_n} = \bar{\beta}$, where $\bar{\beta}$ is some element of $\overline{H}$. If G contains an element σ such that $\sigma^{\lambda_n} = \beta_n^{-\lambda_n}$, then $\sigma\beta_n$ will be of order λ_n (which is less than the order of $\bar{s}$). Since G is $\{\beta_1, \cdots, \beta_{n-1}, \sigma\beta_n\}$, this will contradict our assumption concerning $\bar{s}$. From this assumption we know that the order of each of the elements $\beta_1, \cdots, \beta_{n-1}$ is at least equal to the order of $\bar{s}$. Hence each constituent $\beta_i^{\lambda_i}$ in $\bar{\beta}$ can be regarded as $[\beta_i^{b_i}]^{\lambda_n}$.

Now $[\beta_1^{b_1}\beta_2^{b_2} \cdots \beta_{n-1}^{b_{n-1}}]^{\lambda_n}$ can be brought into the form $\beta_1^{\lambda_1} \cdots \beta_n^{\lambda_{n-1}} c^{k\lambda_n}$, where c is some element in the commutator subgroup of $\overline{H}$. If $c^{k\lambda_n}$ is the identity, then $\beta_1^{b_1} \cdots \beta_{n-1}^{b_{n-1}}$ will serve as the operation σ. If not, then we can find an element c' in the commutator subgroup of G such that $\beta_1^{b_1} \cdots \beta_{n-1}^{b_{n-1}} c'^{k}$ raised to the power λ_n will equal $\beta_n^{-\lambda_n}$.* We are led, then, to the conclusion that no relation $\beta_1^{\lambda_1}\beta_2^{\lambda_2} \cdots \beta_n^{\lambda_n} = E$ can exist unless each λ is divisible by the order of its β. This demonstrates our theorem.

One naturally asks whether for a certain permutation of the subscripts $1, \cdots, n$ there can exist a relation $\beta_{r_1}^{\mu_1}\beta_{r_2}^{\mu_2} \cdots \beta_{r_n}^{\mu_n} = E$, where at least one exponent is less than the order of its β. This we can answer in the negative. Such a relation could be brought into the form

$$(\beta_1^{\lambda_1} \cdots \beta_n^{\lambda_n})(c_{12}^{k_{12}\lambda_1\lambda_2} \cdots c_{n-1,n}^{k_{n-1,n}\lambda_{n-1}\lambda_n}) = (\beta)(c) = E.$$

Since (β) could not be the identity, we should have $(\beta) = (c)^{-1} \neq E$. Since (β) and (c) would be of the same order, at least two of the λ's would necessarily be prime to p. But (β) could then occur in a set of I.G.O. for G, while (c) obviously cannot have this property.

9. That every metabelian group G possesses a U-basis follows from the recent work of Hall in the field of prime-power groups.† The author, however, wishes to present his original proof, since the details are widely applicable in the following sections.

From the definition, it is clear that either (A) and (B) or (A) and (C) below provide a set of necessary and sufficient conditions for the elements $P_1, P_2, \cdots, P_\rho$ to constitute a U-basis for G:

(A) $P_x = P_1^{x_1}P_2^{x_2} \cdots P_\rho^{x_\rho}$ and $P_y = P_1^{y_1} \cdots P_\rho^{y_\rho}$ represent the same operation of G only when each $x_i - y_i$ is divisible by the order of P_i;

(B) the product of the orders of $P_1, P_2, \cdots, P_\rho$ equals the order of G;

(C) every operation of G is representable in the form P_x.

Although it is not essential, we shall nevertheless find it convenient to

* Cf. (d) of §1.

† Hall, loc. cit., pp. 90–95. Hall proved (a) that every *regular* p-group is conformal with an abelian group; (b) that every regular p-group has a U-basis; (c) that the orders of the elements in a U-basis are the invariants of the conformal abelian group.

regard G as a regular permutation group. We shall, therefore, assume that the symbols which we employ have the meanings given in the first paragraph of §4. For the permutation of H which transforms G according to P_i we shall use the letter S_i. For convenience, we shall usually write T_i in place of S_i^{-a}.

Before demonstrating the existence of a U-basis for G, we shall prove the following result:

THEOREM I. *If $P_1, P_2, \cdots, P_\rho$ constitute a U-basis for G, then $P_1S_1^a$, $P_2S_2^a, \cdots, P_\rho S_\rho^a$ will constitute a U-basis for A.*

For the elements $A_1, A_2, \cdots$ to constitute a U-basis for A the following conditions are clearly sufficient:

(i) the product of the orders of $A_1, A_2, \cdots$ equals the order of A;

(ii) the product $A_x = A_1^{x_1}A_2^{x_2}\cdots$ can be the identity only when each factor $A_1^{x_1}, A_2^{x_2}, \cdots$ is the identity.

Now the orders of P_i and $P_iS_i^a$ are the same. Since the product of the orders of $P_1, P_2, \cdots$ must equal p^m, we see that (i) is satisfied for the elements $P_iS_i^a$.

We proceed to show that (ii) is also satisfied. We know that $P_x = P_y$ requires that $x_i - y_i$ be divisible by the order of P_i. Now $P_x = P_y$ is equivalent to $P_xP_y^{-1} = E$, and this latter equation may be brought into the form

$$(1)\quad P_xP_y^{-1} = P_1^{x_1-v_1}\cdots P_\rho^{x_\rho-v_\rho}\prod_{i<j} c_{ij}^{-v_i(x_j-v_j)} = E,^* \text{ where } c_{ij} = P_i^{-1}P_jP_iP_j^{-1}.$$

In (1) we write z_i in place of $x_i - y_i$, obtaining

$$(2)\qquad P_{y+z}P_y^{-1} = P_1^{z_1}P_2^{z_2}\cdots P_\rho^{z_\rho}\prod c_{ij}^{-y_iz_j} = E.$$

Now the product

$$A_u = (P_1S_1^a)^{u_1}(P_2S_2^a)^{u_2}\cdots(P_\rho S_\rho^a)^{u_\rho}$$

can be reduced to the form

$$(3)\qquad A_u = P_1^{u_1}\cdots P_\rho^{u_\rho}\prod c_{ij}^{-au_iu_j}\prod S_i^{au_i}.$$

Let us suppose that A_u is the identity. Since G and H are isomorphic under the correspondence $P_i \sim S_i^a$, we see that $A_u = E$ requires $\Pi S_i^{au_i} = E$.

Since the P_i are a U-basis for G, we know that equation (2) holds only when z_i is divisible by the order of P_i. By taking y_i equal to au_i and z_j equal to u_j, we see from (3) that A_u can be the identity only when the order of $P_iS_i^a$ divides u_i. This completes our proof.

* Since the elements c_{ij} are commutative, we may use the product sign Π. It is nevertheless desirable to think of the subscripts as occurring in a definite order, preferably the order $12, 13, \cdots, 1\rho, 23, \cdots, 2\rho, \cdots, \rho-1\ \rho$.

Since the orders of the elements in any U-basis for A are an invariant of A, we have, as a corollary,

THEOREM II. *The orders of the elements in any U-basis for G are the invariants* $p^{\delta_1}, p^{\delta_2}, \cdots, p^{\delta_r}$ *of* A.*

We now state two theorems which assert the existence of a U-basis for any G.

THEOREM III. *If G is an ω-group and* $A_1, \cdots, A_r$ *are the elements of any U-basis for A, then* $A_1T_1, A_2T_2, \cdots, A_rT_r$ *will constitute a U-basis for G.*

THEOREM IV. *If G is any metabelian group of order* p^m, $p>2$, *and* $A_1, \cdots, A_r$ *constitute a primary U-basis for A, then a U-basis for G is given by the elements* $A_1T_1, A_2T_2, \cdots, A_rT_r$.

First we state what is meant by the term *primary U-basis for A*.

The U-basis $A_1, \cdots, A_r$ is said to be a *primary U-basis for A* provided that for the associated automorphisms $T_1, \cdots, T_r$ (arising from the equation $s_i = \theta^{-a}A_i = A_iT_i$) any product $T_x = T_1^{x_1}T_2^{x_2} \cdots T_r^{x_r}$ can be the identity only when the exponent of each T_i which is a principal element of H is divisible by p. For the present we shall assume that A possesses at least one primary U-basis; the proof will be given in the following section.

If $A_1, \cdots, A_r$ are any given U-basis for A, then the elements $A_1T_1, \cdots, A_rT_r$ have the property mentioned in (B) above. In determining whether the A_iT_i constitute a U-basis for G, the investigation, therefore, centers upon the equation

$$(A_1T_1)^{x_1}(A_2T_2)^{x_2} \cdots (A_rT_r)^{x_r} = (A_1T_1)^{y_1} \cdots (A_rT_r)^{y_r}. \tag{4}$$

This equation we may bring into the form

$$A_{x-y}\gamma_{x-y}T_{x-y} = E, \tag{5}$$

where

$$A_{x-y} = \prod_{i=1}^{r} A_i^{x_i-y_i}, \quad \gamma_{x-y} = \prod_{i<j} \gamma_{ij}^{(x_i+y_i)(x_j-y_j)},$$

γ_{ij} being

$$T_iA_jT_i^{-1}A_j^{-1}; \quad T_{x-y} = \prod_{1}^{r} T_i^{x_i-y_i}.$$

For convenience we shall write z_i in place of x_i-y_i and u_i in place of x_i+y_i. One easily sees that equation (5) requires $T_z = E$. Hence (5) reduces to

* Cf. Hall, loc. cit., p. 90.

$$A_s\gamma_s = E. \tag{6}$$

If (6) is satisfied only by $A_s = E$, then the A_iT_i will constitute a U-basis for G, since $A_s = E$ requires $z_i \equiv 0 \pmod{p^{b_i}}$. (The A_i constitute a U-basis for A.) Our objective is to show that when the A_i are selected according to the hypothesis of Theorem III or of Theorem IV, then (6) can be satisfied only by $A_s = E$.

(i) We assume that there exist certain values for the z_i and u_j such that A_s equals γ_s^{-1}, where A_s is not the identity. Then A_s and γ_s must be of the same order.

(ia) If G is an ω-group, then C must be a subgroup of $\mathfrak{V}_1(A)$. We observe that each commutator $\gamma_{ij}^{u_iz_j}$ in γ_s arises from T_i^{u} and the constituent $A_j^{z_j}$ of A_s. Since no element of a U-basis for A can be in $\mathfrak{V}_1(A)$, one readily sees that A_s and γ_s cannot be of the same order. For an ω-group, therefore, any U-basis of A leads to a U-basis for G.

(ib) Suppose that G is not an ω-group. We now assume that $A_1, \cdots, A_r$ are the elements of a primary U-basis for A. We wish to show that the assumption

$$A_s = \gamma_s^{-1},\ A_s \neq E, \tag{7}$$

is an impossible one.

As an element of A, each γ_{ij} can be expressed in the form $A_1^{b_1}A_2^{b_2}\cdots A_r^{b_r}$. If the exponent of every γ_{ij} in γ_s is divisible by p^α (but not by $p^{\alpha+1}$), then each exponent z_i in A_s must be divisible by p^α. In this case there must exist an element $\overline{A}_\alpha$ in A, whose order does not exceed p^α, such that $\overline{A}_\alpha A_{s'}$ equals $\gamma_{s'}^{-1}$, where z_i is $p^\alpha z_i'$, while $A_{s'}$ and $\gamma_{s'}$ are derived from A_s and γ_s respectively by substituting z_i' for z_i, leaving u_j unchanged. Then at least one of the exponents in $\gamma_{s'}$ will be prime to p. As we shall see, the argument is unaffected by the presence of the factor $\overline{A}_\alpha$, since $\overline{A}_\alpha$ is of lower order than $A_{s'}$. We shall, therefore, assume that in equation (7) the exponent of one of the γ_{ij}, say of $\gamma_{ab}^{u_az_b}$, is prime to p. Then $A_b^{z_b}$ must be a principal element of A. Since $A_b^{z_b}$ occurs in γ_s^{-1}, some constituent of γ_s, say $\gamma_{cd}^{u_cz_d}$, must contain A_b^{λ}, where λ is some exponent prime to p. Obviously u_cz_d must be prime to p, and γ_{cd} must be a principal element of A. Consequently T_d must be a principal element of H.

We recall that equation (5) is possible only when

$$T_s = T_1^{z_1}T_2^{z_2}\cdots T_d^{z_d}\cdots T_r^{z_r} \text{ is the identity.}$$

But the assumption that $A_1, \cdots, A_r$ are a primary U-basis and the conclusion above that z_d must be prime to p are clearly incompatible. In the case

of a primary U-basis $A_1, \cdots, A_r$, the assumption (i) can never be realized. This completes our demonstration of Theorem IV.

10. Theorem IV of §9 is clearly of little value unless we prove that A contains a primary U-basis. We indicate a method for constructing a primary U-basis, starting with any U-basis $A_1, \cdots, A_r$ of A. The order of A_i is of course p^{δ_i}; we assume the inequalities $\delta_1 \geqq \delta_2 \geqq \cdots \geqq \delta_r$.

It is a well known fact that the r elements

$$A_i' = A_1^{a_{i1}} A_2^{a_{i2}} \cdots A_r^{a_{ir}} \qquad (i = 1, 2, \cdots, r) \tag{1}$$

will constitute a U-basis for A, provided that the a_{ij} are any integers for which (a) the determinant $|a_{ij}|$ is prime to p, and (b) a_{ij} is divisible by $p^{\delta_j - \delta_i}$ for $i > j$. We propose to determine the a_{ij} so that $A_1', \cdots, A_r'$ will be a primary U-basis for A.

If the T_i's satisfy no relation of the form

$$T_1^{\lambda_1} T_2^{\lambda_2} \cdots T_r^{\lambda_r} = E \tag{2}$$

in which a λ is prime to p, then the initial U-basis $A_1, \cdots, A_r$ will be a primary U-basis. In the contrary case, let λ_α be the first λ in the sequence $\lambda_1, \lambda_2, \cdots$ which is prime to p, taking into account the totality of relations of type (2). If T_α is the identity, we eliminate T_α from every relation of type (2) and proceed to the next λ which is prime to p. If not, we replace A_α (in the set $A_1, \cdots, A_r$) by

$$A_\alpha' = A_\alpha^{\lambda_\alpha} A_{\alpha+1}^{\lambda_{\alpha+1}} \cdots A_r^{\lambda_r}.$$

Then for the permutation T_α' of H which is associated with A_α' we shall have the equation

$$T_\alpha' = T_1^{-\lambda_1} T_2^{-\lambda_2} \cdots T_{\alpha-1}^{-\lambda_{\alpha-1}}, \tag{3}$$

where $\lambda_1, \cdots, \lambda_{\alpha-1}$ are all divisible by p. From the remaining relations of type (2) we eliminate T_α by means of the equation $T_\alpha = T_1^{-\lambda_1 \lambda_\alpha^{-1}} \cdots T_r^{-\lambda_r \lambda_\alpha^{-1}}$, arranging, of course, the elements in each new relation according to the sequence $T_1, T_2, \cdots, T_{\alpha-1}, T_{\alpha+1}, \cdots$. If none of the exponents in these new relations is prime to p, our process is at an end; otherwise, we proceed as before until we eventually determine a set of elements $A_1', \cdots, A_r'$ for which a certain h of the T''s, say $T_{\epsilon_1}', T_{\epsilon_2}', \cdots, T_{\epsilon_h}'$, constitute a set of I.G.O. for H, while each of the remaining T''s is of the form

$$T_{\epsilon_1}'^{d_1 p} \cdots T_{\epsilon_h}'^{d_h p}.$$

That $A_1', \cdots, A_r'$ constitute a U-basis for A is obvious from the fact that $|a_{ij}|$ equals $\lambda_\alpha \lambda_\alpha' \cdots$, while $\lambda_\alpha, \lambda_\alpha', \cdots$ are all prime to p. (See (a) above;

the elements below the main diagonal in $|a_{ij}|$ are all zeros.)

From Theorems I and III of §9, in connection with the equation $t_i = \theta^a s_i$, we know that for every ω-group the elements of a U-basis for G correspond to the elements of a U-basis for A, and conversely. That this correspondence is not necessarily a reciprocal one when G is not an ω-group is clear from the following example.

Let G be the metabelian group defined by the relations

$$s_1^p = s_2^p = s_0^p = E,\ s_1^{-1}s_2s_1 = s_2s_0,\ s_1s_0 = s_0s_1,\ s_2s_0 = s_0s_2.$$

Let a be the smallest positive root of the congruence $2a+1 \equiv 0 \pmod{p}$. By an easy computation we can show that $A_1 = s_1S_1^a$, $A_2 = s_2S_2^a$, $A_3 = A_1^{-1}A_2^{-1}s_0^{-a}$ constitute a U-basis for A. But A_1T_1, A_2T_2, A_3T_3 do not constitute a U-basis for G, since $A_x = (A_1T_1)^{x_1}(A_2T_2)^{x_2}(A_3T_3)^{x_3}$ is the identity for $x_1 \equiv x_2 \equiv x_3 \pmod{p}$. In fact, for $x_1 \equiv x_2 \equiv x_3 \equiv 1 \pmod{p}$, A_x reduces to $s_1s_2s_1^{-1}s_2^{-1}s_0$, which is clearly the identity.

Properties associated with a given basis

11. Having demonstrated the occurrence in G of each of the four types of bases, we now propose to develop certain "non-invariant" properties which are associated with a particular choice of a basis for G. From this point on, the letters $\beta_1, \beta_2, \cdots, \beta_n$ shall represent a special kind of B-basis, namely an *MB-basis*, which we define in the following manner: With every B-basis of G there is associated a number χ, which equals the sum of the orders of the elements in this B-basis. Those B-bases for which χ is a minimum in G we shall call MB-bases.

Let the elements of any MB-basis be denoted by $\beta_1, \beta_2, \cdots, \beta_n$, of orders $p^{\eta_1}, \cdots, p^{\eta_n}$ respectively, where $\eta_1 \geqq \eta_2 \geqq \cdots \geqq \eta_n$. We know that every operation of G can be represented in the form $\beta_x' = \beta_x c$, where β_x equals $\beta_1^{x_1}\beta_2^{x_2} \cdots \beta_n^{x_n}$, while c is some element of C. Furthermore, we know that the order of β_x is the order of its constituent $\beta_i^{x_i}$ of highest order. We now prove a result which is of great importance in the following development of the theory.

Theorem I. *If β_x is a principal element of G, then the order of β_x' is the order of that one of its constituents $\beta_1^{x_1}, \beta_2^{x_2}, \cdots, \beta_n^{x_n}, c$ which is of highest order.*

The theorem is clearly true when β_x and c are of unequal orders. So we assume that β_x and c are both of order p^a, while β_x' is of order p^b, $b < a$. For the purpose of demonstrating the impossibility of the inequality $b < a$, it is permissible to assume that (a) among all the products $\beta_y' = \beta_y c$ of a principal element of G into an element of C where β_y' is of lower order than β_y, there is

none whose order is less than p^b.

Let x_α be the first one of the exponents $x_1, x_2, \cdots, x_n$ in β_x which is prime to p. We wish to show that by replacing in our given MB-basis the element β_α by β_x', we shall obtain a B-basis. Since the sum of the orders of the elements in this new basis will be less than Σp^{η_i}, $i=1, 2, \cdots, n$, we shall arrive at a contradiction, since Σp^{η_i} is a minimum in G.

Now $\beta_1, \cdots, \beta_{\alpha-1}, \beta_x', \beta_{\alpha+1}, \cdots, \beta_n$ will generate G. Hence we have only to prove that $\beta_\lambda = E$, where β_λ is $\beta_1^{\lambda_1} \cdots \beta_{\alpha-1}^{\lambda_{\alpha-1}} \beta_x'^{\lambda_\alpha} \cdots \beta_n^{\lambda_n}$, requires that each λ be divisible by the order of the element to which it belongs. If λ_α is divisible by p^b, then there is nothing to prove. So we assume that p^d, the highest power of p which divides λ_α, is less than p^b.

In β_λ we replace β_x' by $\beta_x c$ and bring the result into the form $\beta_\lambda' = \beta_1^{\lambda_1+\lambda_\alpha x_1} \beta_\alpha^{\lambda_\alpha x_\alpha} \cdots \beta_n^{\lambda_n+\lambda_\alpha x_n} c^{\lambda_\alpha} \bar{c}$, where $\bar{c}$ is a product of commutators, each of whose exponents is divisible by λ_α. Let p^e be the highest power of p that divides every exponent in β_λ'. Clearly e is not greater than d.

Now we can find in G an operation $\beta_z' = \beta_z c'$, where β_z is a principal element $\beta_1^{z_1}\beta_2^{z_2} \cdots \beta_n^{z_n}$ in G, such that $\beta_z'^{p^e}$ equals β_λ' (see (d) of §1). The order of β_z is clearly greater than p^e; the order of β_z' is p^e, since β_λ' is the identity. This, however, involves a contradiction of assumption (a), since e is less than b. We conclude, therefore, that d must equal b. This completes the demonstration of Theorem I.

THEOREM II. *If an operation s of G can be represented in the form β_x, where each exponent x_i is a least positive residue modulo p^{η_i}, then the x_i's are uniquely determined.*

Suppose that s is given by β_x and also by β_y, where β_y is $\beta_1^{y_1}\beta_2^{y_2} \cdots \beta_n^{y_n}$. Then $\beta_x = \beta_y$ leads to $\beta_x \beta_y^{-1} = E$. This latter equation can be reduced to the form $\beta_{x-y} c_{x-y} = E$, where β_{x-y} is $\beta_1^{x_1-y_1} \cdots \beta_n^{x_n-y_n}$ and c_{x-y} is $\prod_{i<j} c_{ij}^{-y_i(x_j-y_j)}$, c_{ij} being $\beta_i^{-1}\beta_j\beta_i\beta_j^{-1}$. Our theorem will follow if we can show that β_{x-y} must be the identity, since $\beta_{x-y} = E$ requires $x_i - y_i \equiv 0 \pmod{p^{\eta_i}}$.

Suppose that β_{x-y} is not the identity. Then each exponent in β_{x-y} must be divisible by p; otherwise, β_{x-y} could not be in the ϕ-subgroup of G. Let p^α be the highest power of p that divides every $x_i - y_i$. Since every exponent in c_{x-y} contains one of the $x_i - y_i$, we can find in G an operation $\beta_z' = \beta_z c' = \beta_1^{z_1}\beta_2^{z_2} \cdots \beta_n^{z_n} c'$, such that β_z is a principal element of G, and such that $\lambda_z'^{p^\alpha}$ is $\beta_{x-y} c_{x-y}$. Since the order of β_z exceeds p^α, this leads to a contradiction of Theorem I. Hence β_{x-y} must be the identity.

THEOREM III. *If G is an ω-group, then every B-basis is a U-basis, and conversely.*

To prove the "conversely" we need only to show that the elements $P_1, P_2, \cdots, P_r$ of a U-basis constitute a set of I.G.O. for G. The ϕ-subgroup of an ω-group is $\mathfrak{V}_1(G)$ Clearly a product $P_1^{\lambda_1}P_2^{\lambda_2}\cdots P_r^{\lambda_r}$ can be a pth power in G only when each λ is divisible by p.

To prove the first part of our theorem we make use of Theorem IV of §6. Knowing that we can express every operation s of G in the form $\bar{\beta}_x=\bar{\beta}_1^{x_1}\bar{\beta}_2^{x_2}\cdots\bar{\beta}_n^{x_n}$, where $\bar{\beta}_1, \bar{\beta}_2, \cdots, \bar{\beta}_n$ are a B-basis for G, we have only to show that s is uniquely represented by $\bar{\beta}_x$, whenever the exponents x_i are least positive residues.

In the proof of Theorem II above we use the assumption that $\beta_1, \beta_2, \cdots, \beta_n$ are an MB-basis in order to show that $\beta_x=\beta_y$ requires $\beta_{x-y}=E$. But if G is an ω-group, we can prove this without requiring that the β's constitute an MB-basis. If $\bar{\beta}_1, \bar{\beta}_2, \cdots, \bar{\beta}_n$ are simply a B-basis, then $\bar{\beta}_{x-y}=E$ will hold only when each x_i-y_i is divisible by the order of the $\bar{\beta}_i$ to which it belongs. In the case of an ω-group every commutator can be expressed in the form $\bar{\beta}_1^{d_1p}\bar{\beta}_2^{d_2p}\cdots\bar{\beta}_n^{d_np}$. From this we see that $\bar{\beta}_{x-y}$ and $\bar{c}_{x-y}$ (in Theorem II) can never be of the same order unless each is the identity. That is, if G is an ω-group, then in Theorem II we may replace our assumption that $\beta_1, \beta_2, \cdots, \beta_n$ are an MB-basis by the weaker assumption that they are a B-basis.

From this modified form of Theorem II we see that the elements $\bar{\beta}_1, \bar{\beta}_2, \cdots, \bar{\beta}_n$ satisfy the requirements (A) and (C) of §9 and accordingly constitute a U-basis for G.

THEOREM IV. *If G is an ω-group, then every B-basis is an MB-basis.*

This follows directly from Theorem III, since the orders of the elements of a U-basis are an invariant of G.

THEOREM V. *The orders of the elements in any MB-basis for G are an invariant of G.*

When G is an ω-group, this follows directly from Theorem III. We let $\beta_1, \beta_2, \cdots, \beta_n$, of orders $p^{\eta_1}, p^{\eta_2}, \cdots, p^{\eta_n}$ respectively, and $\beta_1', \beta_2', \cdots, \beta_n'$, of orders $p^{\eta_1'}, p^{\eta_2'}, \cdots, p^{\eta_n'}$, be any two MB-bases for G. We may assume the inequalities $\eta_1 \geqq \eta_2 \geqq \cdots \geqq \eta_n$ and $\eta_1' \geqq \eta_2' \geqq \cdots \geqq \eta_n'$. Now η_1 and η_1' must be equal. Let η_α' be the first one of the η''s which differs from its corresponding η, and let η_α' be less than η_α. Now the elements $\beta_1', \cdots, \beta_n'$ can be expressed in terms of the β's by means of the equations

$$\beta_i' = \beta_1^{a_{i1}}\beta_2^{a_{i2}}\cdots\beta_n^{a_{in}}c_i \qquad (i = 1, 2, \cdots, n) \tag{1}$$

where $c_1, \cdots, c_n$ are elements of C. Since the β''s are a set of I.G.O. for G, it is obvious that the determinant $|a_{ij}|$ must be prime to p. Since the order of

β_α' is $p^{\eta_\alpha'}$, either (b) $a_{\alpha 1}, a_{\alpha 2}, \cdots, a_{\alpha\alpha}$ are divisible by $p^{\eta_1-\eta_\alpha'}, p^{\eta_2-\eta_\alpha'}, \cdots, p^{\eta_\alpha-\eta_\alpha'}$ respectively, or (c) the order of $\beta_1^{a_{\alpha 1}}\beta_2^{a_{\alpha 2}}\cdots\beta_n^{a_{\alpha n}}$ exceeds the order of β_α'. In case (b), the determinant $|a_{ij}|$ would be divisible by p, while in case (c), we should have a contradiction of Theorem I. Consequently, η_i' must equal η_i, for $i=1, 2, \cdots, n$.

To our list of invariants in §6 we may add the invariants $p^{\eta_1}, p^{\eta_2}, \cdots, p^{\eta_n}$. Obviously η_1 equals δ_1. That these invariants coincide with a certain n of the invariants $p^{\delta_1}, p^{\delta_2}, \cdots, p^{\delta_r}$ is a consequence of the following result.

THEOREM VI. *By the addition of a certain $r-n$ terms every MB-basis can be extended to a U-basis for G.*

For ω-groups the theorem is trivial. We therefore assume that G is not an ω-group.

(i) We first show that $A_1=\theta^a\beta_1$, $A_2=\theta^a\beta_2, \cdots, A_n=\theta^a\beta_n$ constitute a U-basis for the subgroup A' of A which they generate.

(ii) Next we show that we can select from A a certain $r-n$ elements $A_{n+1}, \cdots, A_r$ such that $A_1, \cdots, A_r$ will constitute a U-basis for A.

(iii) Finally, we prove that $\theta^{-a}A_1, \cdots, \theta^{-a}A_r$ constitute a U-basis for G.

Proof of (i). We have only to show that the equation

$$A_1^{\lambda_1}A_2^{\lambda_2}\cdots A_n^{\lambda_n} = E \tag{2}$$

holds only for λ_i divisible by p^{η_i}. Now $\theta^a\beta_i$ equals $\beta_iS_i^a$, where S_i transforms G according to β_i. In (2) we replace each A_i by $\beta_iS_i^a$ and bring the result into the form

$$\beta_1^{\lambda_1}\beta_2^{\lambda_2}\cdots\beta_n^{\lambda_n}\prod_{i<j}c_{ij}^{-a\lambda_i\lambda_j} = E, \tag{3}$$

where c_{ij} is $S_i^{-1}\beta_jS_i\beta_j^{-1}$.

Now $\beta_1^{\lambda_1}\beta_2^{\lambda_2}\cdots\beta_n^{\lambda_n}$ cannot be in $\Phi(G)$ unless each λ_i is divisible by p. Consequently, every exponent $a\lambda_i\lambda_j$ must be divisible by p^2. Evidently $\beta_1^{\lambda_1}\cdots\beta_n^{\lambda_n}$ must be the identity, if equation (3) is to hold. Since the β's are an MB-basis, each λ_i must be divisible by p^{η_i}. Since the order of A_i is p^{η_i}, we see that A' is the direct product of $\{A_1\}$, $\{A_2\}$, etc.

Proof of (ii). We write A in cosets with respect to A'. Let $Q_1, Q_2, \cdots, Q_{l_1}$, of orders $p^{t_1}, p^{t_2}, \cdots, p^{t_{l_1}}$, be any U-basis for A/A'.* We wish to show that the coset of A which corresponds to $Q_j, j=1, 2, \cdots, l_1$, contains an operation of order p^{t_j}.

* One sees that A/A' and $C/\bar{C}_1$ have the same number of invariants. Furthermore, l_1 equals $r-n$ (see §6).

Now this coset contains an element c_j of C which is a principal element of C and is not in $\mathfrak{V}_1(A)$. If c_j is of order p^{ζ_j}, then we denote it by the letter A_{n+j} and add it to the set $A_1, \cdots, A_n$. If not, then there must exist an equation

$$c_j^{p^{\zeta_j}} = (A_1^{b_1}A_2^{b_2}\cdots A_n^{b_n})^{p^\xi}, \tag{4}$$

where the element in the parenthesis is a principal element of A'. We propose to show that ξ must exceed ζ_j. We replace, in (4), each A_i by $\beta_i S_i^a$. We may then bring (4) into the form

$$(\beta_1^{b_1}\beta_2^{b_2}\cdots\beta_n^{b_n})^{p^\xi} = \bar{c}^{p^\xi} c_j^{p^{\zeta_j}}. \tag{5}$$

(It is clear that $(S_1^{ab_1}\cdots S_n^{ab_n})^{p^\xi}$ must be the identity.) If ξ is not greater than ζ_j, we can determine an element c' in C such that $\beta_1^{b_1}\cdots\beta_n^{b_n}\bar{c}^{-1}c'c_j^{-p^{\zeta_j-\xi}}$ will be of order p^ξ. Since $\beta_1^{b_1}\beta_2^{b_2}\cdots\beta_n^{b_n}$ is a principal element of G whose order exceeds p^ξ, we have a contradiction of Theorem I. For the element A_{n+j} we may therefore take $c_j(A_1^{b_1}A_2^{b_2}\cdots A_n^{b_n})^{-p^{\xi-\zeta_j}}$. Obviously the r elements $A_1, \cdots, A_n, A_{n+1}, \cdots, A_{n+l_1=r}$ constitute a U-basis for A.

Proof of (iii). Let $T_1, T_2, \cdots, T_r$ be the permutations of H which correspond by means of the equation $s_i = \theta^{-a}t_i$ to $A_1, \cdots, A_r$ as determined in (i) and (ii) above. From the manner of selection for $A_1, A_2, \cdots, A_r$ it is clear that no T_{n+j} can be a principal element of H (observe the inequality $\xi > \zeta_j$ above). Again, every product $A_{n+1}^{x_{n+1}}A_{n+2}^{x_{n+2}}\cdots A^{x_r}$ must be in $\Phi(G)$.

Now the equation

$$(A_1T_1)^{x_1}\cdots(A_rT_r)^{x_r} = (A_1T_1)^{y_1}\cdots(A_rT_r)^{y_r} \tag{6}$$

can be brought into the form

$$\beta_1^{x_1-y_1}\cdots\beta_n^{x_n-y_n} = \beta_\phi, \tag{7}$$

where β_ϕ is in $\Phi(G)$. We know that (7) can exist only if each $x_i - y_i$, $i = 1, \cdots, n$, is divisible by p. We also know that (6) requires that the T's satisfy the equation

$$T_1^{x_1-y_1}\cdots T_n^{x_n-y_n}T_{n+1}^{x_{n+1}-y_{n+1}}\cdots T_r^{x_r-y_r} = E. \tag{8}$$

Consequently, in the particular equation (8) which arises from a given equation (6) the exponent of every T which is a principal element in H must be divisible by p.* Hence the proof of Theorem IV in §9 is applicable to the U-basis $A_1, \cdots, A_r$, as determined in (i) and (ii) above. Having proved that

* In the hypothesis of Theorem IV in §9 we demanded this property of *every* equation $T_1^{s_1}\cdots T_r^{s_r} = E$. Obviously it is sufficient to require it only for that *particular* equation which arises from equation (5) of §9.

$A_1T_1, \cdots, A_rT_r$ constitute a U-basis for G, our demonstration of Theorem VI is at an end. It is, of course, obvious that the orders of the A_iT_i, viz., $p^{\eta_1}, p^{\eta_2}, \cdots, p^{\eta_n}, p^{\delta_1}, \cdots, p^{\delta_h}$, do not, in this sequence, necessarily coincide with $p^{\delta_1}, p^{\delta_2}, \cdots, p^{\delta_r}$ respectively.

We now mention two theorems, which are rather obvious consequences of the definition of a U-basis.

THEOREM VII. *If $P_1, P_2, \cdots, P_r$ are any U-basis for G, then the order of $P_x = P_1^{x_1}P_2^{x_2} \cdots P_r^{x_r}$ is the order of its constituent $P_i^{x_i}$ of highest order.*

THEOREM VIII. *If $P_{s_1}, P_{s_2}, \cdots, P_{s_r}$ are the elements $P_1, P_2, \cdots, P_r$ above written in any arbitrary sequence, then each element of G can be expressed uniquely in the form $P_{s_1}^{x_1}P_{s_2}^{x_2} \cdots P_{s_r}^{x_r}$, where each exponent is a least positive residue modulo the order of the element to which it belongs.*

The proofs are easily supplied.

We now prove the complement to Theorem VI.

THEOREM IX. *Let $P_1, P_2, \cdots, P_r$ be any U-basis for G. Any n elements $P_{s_1}, P_{s_2}, \cdots, P_{s_n}$ (of this U-basis) which generate G will constitute an MB-basis for G.*

Since $P_1, \cdots, P_r$ generate G, it is obvious that a certain n of them, say $P_{s_1}, \cdots, P_{s_n}$, will constitute a set of I.G.O. for G. Let the orders of these be $p^{\eta_1}, p^{\eta_2'}, \cdots, p^{\eta_n'}$, $\eta_1 \geqq \eta_2' \geqq \cdots \geqq \eta_n'$. Let $\beta_1, \beta_2, \cdots, \beta_n$, of orders $p^{\eta_1}, p^{\eta_2}, \cdots, p^{\eta_n}$, $\eta_1 \geqq \eta_2 \geqq \cdots \geqq \eta_n$, be any MB-basis for G. Our theorem will follow if we can show that η_i' must equal η_i, $i=2, 3, \cdots, n$, since $P_{s_1}, \cdots, P_{s_n}$ constitute at least a B-basis.

Now each β_i, $i=1, 2, \cdots, n$, can be expressed in the form $\beta_i = P_{s_1}^{a_{i1}}P_{s_2}^{a_{i2}} \cdots P_{s_n}^{a_{in}}c_i$, where c_i is some element of C. Suppose that η_α' is the first of the η''s, in the sequence $\eta_2', \eta_3', \cdots, \eta_n'$, which differs from its corresponding η. Since η_α' cannot be less than η_α, we take $\eta_\alpha' > \eta_\alpha$. Now $|a_{ij}|$ must be prime to p (see proof of Theorem V). Hence at least one of the exponents $a_{i1}, a_{i2}, \cdots, a_{in}$ in every β_i must be prime to p. So we take $a_{i\lambda}$ prime to p. As an element of G, c_i can be expressed uniquely in the form $P_{s_1}^{x_1}P_{s_2}^{x_2} \cdots P_{s_n}^{x_n}P_{s_{n+1}}^{x_{n+1}} \cdots$ (see Theorem VIII). In this expression each x_j, $j=1, \cdots, n$, is divisible by p, since no product $P_{s_1}^{y_1}P_{s_2}^{y_2} \cdots P_{s_n}^{y_n}$ can be in C unless each y_i is divisible by p. We can therefore express β_i in the form

$$\beta_i = P_{s_1}^{a_{i1}+b_{i1}p} \cdots P_{s_\lambda}^{a_{i\lambda}+b_{i\lambda}p} \cdots P_{s_n}^{a_{in}+b_{in}p}P_{s_{n+1}}^{b_{i,n+1}} \cdots .$$

From this we see that the order of β_i is at least equal to the order of P_{s_λ}, which is η_λ' (see Theorem VII). Consequently, for $i>j$, a_{ij} must be divisible by $p^{\eta_j'-\eta_i}$. Taking $i=\alpha$, we see that $a_{\alpha 1}, a_{\alpha 2}, \cdots, a_{\alpha\alpha}$ must be divisible by

$p^{\eta_1-\eta_\alpha}$, $p^{\eta_2'-\eta_\alpha}$, $\cdots$, $p^{\eta_{\alpha'}-\eta_\alpha}$ respectively. But for $\eta_\alpha' > \eta_\alpha$, this would lead to $|a_{ij}| \equiv 0 \pmod{p}$. Hence the assumption $\eta_\alpha' > \eta_\alpha$ is impossible, and the elements $P_{s_1}, P_{s_2}, \cdots, P_{s_n}$ must constitute an MB-basis for G.

Defining relations for G

12. In this section we shall develop a compact set of abstract defining relations for G which arise from the elements $P_1, P_2, \cdots, P_r$ of a given U-basis for G.

As before, we denote the orders of $P_1, P_2, \cdots$ by $p^{\delta_1}, p^{\delta_2}, \cdots$. We define the symbol $R_{p^\epsilon}(q)$ to be the least positive residue of q modulo p^ϵ. Again, by the symbol $R[P_1^{x_1} \cdots P_r^{x_r}]$—in short, $R[P_x]$—we mean the result obtained by replacing each exponent x_i by its least positive residue modulo p^{δ_i}. That is,

$$R[P_1^{x_1} \cdots P_r^{x_r}] \tag{1}$$

is the product of r terms $P_i^{R_i}$, where $R_i = R_{p^{\delta_i}}(x_i)$. Let P_{ij} be defined by the equation $P_{ij} = P_i^{-1}P_jP_iP_j^{-1}$, and let $p^{\delta_{ij}}$ denote the order of P_{ij}. We know that each P_{ij} can be represented uniquely in the form

$$P_{ij} = P_1^{b_{1ij}}P_2^{b_{2ij}} \cdots P_r^{b_{rij}}, \tag{2}$$

where the exponents are least positive residues. Although every P_{ij} is invariant in G, the constituents $P_\alpha^{b_{\alpha ij}}$ need not be separately invariant under G. We know, however, that the order of $P_k^{-1}P_\alpha^{b_{\alpha ij}}P_kP_\alpha^{-b_{\alpha ij}}$, $i, j, k = 1, 2, \cdots, r$, is less than the order of P_{ij}. From this fact we see that by using equations (2) we can ultimately bring any product P_xP_y (where the x's and y's are arbitrary integers) into the form $P_{x'} = P_1^{x_1'}P_2^{x_2'} \cdots P_r^{x_r'}$. For instance, the first step in this reduction is to bring P_xP_y into the form

$$P_1^{x_1+y_1} \cdots P_r^{x_r+y_r} \prod_{i<j} P_{ij}^{x_jy_i}.$$

Now P_x and P_y are operations of G, whether or not we regard the x's and y's as least positive residues. But if we wish to obtain a unique representation for each operation of G, we must obviously replace P_x by $R[P_x]$. In view of the inequalities $\delta_{ij} \leqq \delta_i$, $\delta_{ij} \leqq \delta_j$, it is clearly a matter of indifference, in bringing P_xP_y into the form $R[P_{x'}]$, whether we reduce exponents after each step (after adding together x_1 and y_1, for instance) or whether we make only a single reduction,—on the exponents of $P_{x'}$. Let us adopt this latter point of view with the proviso that in the course of bringing P_xP_y into the form $P_{x'}$ we drop out all elements $P_i^{\lambda_i}$ for which the exponent λ_i is formally divisible by p^{δ_i}, $i = 1, 2, \cdots, r$. This, of course, amounts to treating the x's and y's as unknowns during the process of constructing $P_{x'}$. We see,

therefore, that the exponents of $P_{x'}$ can be given in terms of the x's and y's by the equations $x_i' = x_i + y_i + f_i(x_1, \cdots, x_r, y_1, \cdots, y_r)$, $i = 1, 2, \cdots, r$, where f_i is either identically zero or a rational integral function of the x's and y's, each term of which is at least of the first degree in both x and y. In view of the congruence $x^{p^{\delta_i - 1}(p-1)} \equiv 1 \pmod{p^{\delta_i}}$, we may assume that the exponent of each x or y in f_i does not exceed $p^{\delta_i - 1}(p-1)$. Let us write P_w for $R[P_{x'}]$. Then the exponents of P_w are given by the equations

$$w_i = R_{p^{\delta_i}}(x_i + y_i + f_i) \qquad (i = 1, 2, \cdots, r).^* \tag{3}$$

Now each of the p^m operations $R[P_x]$ of G is completely characterized by the exponents

$$R_{p^{\delta_j}}(x_j) \qquad (j = 1, 2, \cdots, r).$$

Consequently, G is completely defined by the r numbers $p^{\delta_1}, p^{\delta_2}, \cdots, p^{\delta_r}$ and the equations (3) above. One readily sees that the form of the functions f_i depends, in general, upon the particular U-basis $P_1, P_2, \cdots, P_r$ which we select.

If each component x_i in the vector $v_x = (x_1, x_2, \cdots, x_r)$ is a least positive residue modulo p^{δ_i}, then v_x has p^m distinct values. Now equations (3) associate with any two vectors v_x and v_y a unique product $v_w = v_x v_y$. It is clear that under the law of multiplication defined by (3) those p^m vectors constitute a representation of G. Under the multiplication defined by

$$w_i = R_{p^{\delta_i}}(x_i + y_i)$$

they constitute a representation of A. The "divergence" of G from its conformal abelian group is measured, so to speak, by the r functions f_i.

It is worthwhile to mention two other representations of G which arise from equations (3). If in (3) we hold the y's fixed and let the x's range over all permissible values (i.e., least positive residues), then there is defined a regular permutation $\begin{pmatrix} v \\ vv_y \end{pmatrix}$ of the p^m vectors. So we may regard (3) as defining a representation of G as a regular permutation group G_π.

If in (3) we regard the x's as unknowns and the y's as residues, then for a given set of values $y_1, \cdots, y_r$ there is defined a transformation τ_y, which is not necessarily linear. That is, (3) gives rise to a representation of G as a congruence group G_τ. It is a simple task to verify the fact that G_π and G_τ are simply isomorphic under the correspondence

$$\begin{pmatrix} v \\ vv_y \end{pmatrix} \sim \tau_y^{-1}.$$

* The x's and y's in equations (3) are to be regarded as unknowns; this point of view is essential for certain interpretations of (3) which we shall mention later. Of course in the computation above we are concerned only with values of the x's and y's which are least positive residues.

13. In §12 we indicated a means for constructing a set of defining relations for G, starting from a given U-basis for G. In §13 we set ourselves a similar task, with reference to the operations of a given MB-basis. First, however, we shall prove the following "existence" theorem.

THEOREM I. *Let $B_1, B_2, \cdots, B_n$ be n operations which satisfy the following conditions and no others:*

(1) *the order of B_i is p^{η_i}, $i=1, 2, \cdots, n$;*
(2) *the order of B_{ij} is $p^{\eta_{ij}}$, where B_{ij} is $B_i^{-1}B_jB_iB_j^{-1}$;*
(3) $\eta_{ij} \leqq \eta_i$, $\eta_{ij} \leqq \eta_j$;
(4) $B_iB_{jk}=B_{jk}B_i$, $i, j, k=1, 2, \cdots, n$; *the symbols* n, η_i, η_{jk} are arbitrary, but fixed, positive integers. Then $B_1, B_2, \cdots, B_n$ will generate a metabelian (or abelian) group F, whose order is $p^{\Sigma\eta_i+\eta_{jk}}$.*

It is, of course, permissible to assume $\eta_i>0$. If F exists, then the B_i plus those B_{jk} which are not the identity will surely constitute a U-basis for F. This suggests the introduction of the vector

$$v_x = (x_1, x_2, \cdots, x_n, x_{12}, x_{13}, \cdots, x_{1n}, x_{23}, \cdots, x_{2n}, \cdots, x_{n-1,n}),$$

where the x_i and the x_{jk}, $j<k$, are least positive residues modulis p^{η_i} and $p^{\eta_{jk}}$ respectively.† The symbol v_x has $n+n(n-1)/2$ components (each component for which η_{jk} is zero is represented by a zero); two symbols are to be regarded as distinct unless their components are identical. We readily see that v_x has $p^{\Sigma\eta_i+\eta_{jk}}$ distinct values. We propose to show that the symbols v_x constitute a group of this order, under the law of multiplication given by $v_w=v_xv_y$, where the components of v_w are defined by

$$(5)\qquad \begin{aligned} w_i &= R_{p^{\eta_i}}(x_i + y_i) && (i = 1, 2, \cdots, n);\\ w_{jk} &= R_{p^{\eta_{jk}}}(x_{jk} + y_{jk} + x_ky_j) && (j = 1, \cdots, n;\ k = 2, \cdots, n;\ j < k). \end{aligned}$$

We outline a method for proving that the four group-postulates are satisfied. Obviously (5) associates with any two symbols v_x and v_y a unique product v_w; from (3) it is easy to show that multiplication is associative. The element v_0, for which every component is a zero, has the characteristic property of an identity: i.e., $v_0v_x=v_xv_0=v_x$. By computation, we find that the components of $(v_x)^\lambda$ are given by

$$(6)\qquad x_i' = R_{p^{\eta_i}}(\lambda x_i),\ i = 1, \cdots, n;\quad x_{jk}' = R_{p^{\eta_{jk}}}\left(\lambda x_{jk} + \frac{\lambda(\lambda-1)}{2}\, x_jx_k\right).$$

* We justify this choice of symbols on the grounds that the B_i's will ultimately be identified with the elements of an MB-basis for a given G.

† From (2) and (4) it follows that B_{ij} must equal B_{ji}^{-1}; consequently η_{ij} equals η_{ji}. For x_{jk}, accordingly, we are justified in assuming $j<k$.

From (6) we see that $(v_x)^{n_x}$ equals v_0, where n_x is the smallest positive integer satisfying the simultaneous congruences $n_x x_i \equiv 0 \pmod{p^{\eta_i}}$; $n_x x_{jk} \equiv 0 \pmod{p^{\eta_{jk}}}$. The results of this paragraph show that the symbols v_x constitute a group.

To show that this group is metabelian (or abelian) we construct $v_z = v_x^{-1} v_y v_x v_y^{-1}$. Its components are given by

$$z_i = 0,\ i = 1, 2, \cdots, n;\quad z_{jk} = R_p^{\eta_{jk}}(x_j y_k - x_k y_j). \tag{7}$$

By referring to (5) we readily see that the commutator v_z is commutative with every v_x.

It remains to associate the symbols B_i and B_{jk} with the symbols v_x. We define v_i, $i=1, 2, \cdots, n$, to be that vector for which the component x_i is 1 while the remaining components are zeros. We define v_{jk} as that vector for which the component x_{jk} is 1 while the remaining components are zeros. From (6) it follows that the order of each v_i is p^{η_i}, while the order of each v_{jk} is $p^{\eta_{jk}}$. From (7) we observe that v_{jk} and $v_j^{-1} v_k v_j v_k^{-1}$ are the same. As symbols, therefore, v_i and B_i are interchangeable; the same is true of v_{jk} and B_{jk}. This completes the proof of Theorem I.

Let us now assume that the numbers n, η_i, η_{jk} are no longer arbitrary, but represent respectively the number of I.G.O., the order of β_i, the order of $c_{jk}(=\beta_j^{-1}\beta_k\beta_j\beta_k^{-1})$, where $\beta_1, \beta_2, \cdots, \beta_n$ are the elements of a given MB-basis for a given metabelian group G. We construct the group F, as in Theorem I above. Each of its operations is given uniquely by the symbol

$$B_x = B_1^{x_1} B_2^{x_2} \cdots B_n^{x_n} \prod_{i<j} B_{ij}^{x_{ij}},$$

where the exponents are least positive residues.* Let ψ be defined as the operation of replacing in B_x each B_i by β_i and each B_{jk} by c_{jk}. That is, $\psi(B_x) = \beta_x$, where β_x is

$$\beta_1^{x_1} \cdots \beta_n^{x_n} \prod_{j<k} c_{ij}^{x_{ij}}.$$

We know that every operation of G is representable (although not necessarily uniquely) in the form β_x.

We state without proof two results, whose verification presents no difficulty: (a) the number of formally distinct representations of a given element σ of G in the form β_x equals the number of formally distinct representations of the identity of G; (b) the operation ψ defines an isomorphism of F with G. Let F_1 denote that subgroup of F which corresponds to the identity of G in

* We agree always to write the factors of $\Pi B_{ij}^{x_{ij}}$ in the same order, although the particular order which we adopt is clearly a matter of indifference; we furthermore agree that those B_{jk} for which η_{jk} is zero shall not occur in $\Pi B_{ij}^{x_{ij}}$.

this isomorphism. Of course, G is simply isomorphic with F/F_1.

Let $N_1, N_2, \cdots, N_{n_1}$ denote an MB-basis for F_1. Of course, each N_i is representable uniquely in the form

$$N_i = B_1^{\xi_{i1}} \cdots B_n^{\xi_{in}} \prod_{j<k} B_{jk}^{\xi_{ijk}} \qquad (i = 1, \cdots, n_1). \tag{8}$$

By applying the operation ψ to every element of F_1 we obviously get all the formally distinct representations $\beta_x(E)$ of the identity of G. We readily see that every relation $\beta_x = E$ in G can be derived from the n_1 relations

$$\beta_1^{\xi_{i1}} \cdots \beta_n^{\xi_{in}} \prod_{j<k} c_{jk}^{\xi_{ijk}} = E \qquad (i = 1, \cdots, n_1). \tag{9}$$ *

Now the data given by (1), $\cdots$, (4), (9) were determined from the elements of a particular MB-basis for G. With these data at hand we are able to identify any product of powers of the *symbols* β_i and c_{jk} with a definite element of G. In this sense, therefore, we may regard (1), $\cdots$, (4) and (9) as constituting a set of abstract defining relations for G.

14. In this section we shall outline a third method for defining G, which amounts to a specialization of the procedure developed in §§3–4. The notation which we shall employ is the same as that given in §4 and in §9, assuming, of course, that G is represented as a regular permutation group.

Let $A_1, \cdots, A_r$, of orders $p^{\delta_1}, \cdots, p^{\delta_r}$, be the elements of any U-basis for A, and let A_{jk} be defined by the equation $A_{jk} = T_j^{-1} A_k T_j A_k^{-1}$, $j, k = 1, 2, \cdots, r$. As an element in A, A_{jk} may be represented in the form

$$A_{jk} = A_1^{a_{k1}^j} A_2^{a_{k2}^j} \cdots A_r^{a_k^j} \tag{1}$$

(the letter j in a_{k1}^j is a superscript, not an exponent). Since each operation T_j replaces A_k by $A_k A_{jk}$, we may represent T_j by the substitution

$$\begin{aligned} A_1 \to A_1' &= A_1^{a_{11}^j+1} A_2^{a_{12}^j} \cdots A_r^{a_{1r}^j}, \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ A_r \to A_r' &= A_1^{a_{r1}^j} A_2^{a_{r2}^j} \cdots A_r^{a_{rr}^j+1}. \end{aligned} \tag{2}$$

The matrix of the exponents in (2) we shall call M_j.

We know that the operation θ^{-a} (see §3) when applied in turn to each element of A yields all the operations of G. In particular,

$$\theta^{-a} A_1^{x_1} A_2^{x_2} \cdots A_r^{x_r} \text{ is } (A_1^{x_1} \cdots A_r^{x_r})(T_1^{x_1} \cdots T_r^{x_r}).$$

* In connection with the various representations $\beta_x(E)$ of the identity of G, which we may denote by $\beta_y' c_y''$, where

$$\beta_y' = \beta_1^{y_1} \cdots \beta_n^{y_n} \text{ and } c_y'' = \Pi c_{jk}^{y_{jk}},$$

it is of some interest to note that the order of β_y' cannot exceed the order of c_y''. If $\beta_y' c_y''$ is one of the n_1 elements $\psi(N_i)$, $i = 1, 2, \cdots, n_1$, then either β_y' is the identity or β_y' and c_y'' are of the same order.

Since each T_j is completely characterized by its matrix M_j, it follows that G is defined by the orders of $A_1, A_2, \cdots, A_r$, the exponents in the r matrices $M_1, M_2, \cdots, M_r$, and the operation θ^{-a}.*

From the known properties of G we may state certain necessary conditions which the elements of M_j must fulfill. Since

(3′) the order of T_j divides the order of A_j,

(3) each a_{ik}^{j} is divisible by $p^{\delta_k-\delta_i}$ for $i>k$;

since

(4′) every A_{jk} is commutative with every T_i,

(4) $\sum a_{jk}^{u}a_{kl}^{v}$ must be a multiple of p^{δ_l} where j, k, l, u, v range independently from 1 to r. From the equality

(5′) $A_{jk}=A_{kj}^{-1}$

we obtain

(5) $a_{ul}^{v}+a_{vl}^{u}\equiv 0 \pmod{p^{\delta_l}}$, $u, v, l=1, 2, \cdots, r$.

As a special case of (5) we have

(6) $a_{ij}^{i}\equiv 0 \pmod{p^{\delta_i}}$, $i, j=1, \cdots, r$,

which may be derived immediately from the fact that

(6′) T_i is commutative with A_i, $i=1, 2, \cdots, r$.

From the conclusions of the paragraph above we derive two additional results:

(7) the matrix of the exponents in T_j^{x} is given by

$$(M_j)^x=\begin{pmatrix} a_{11}^{i}x+1 & a_{12}^{i}x\cdots & a_{1r}^{i}x \\ \cdots\cdots\cdots\cdots & & \\ a_{r1}^{i}x & a_{r2}^{i}x\cdots & a_{rr}^{i}x+1 \end{pmatrix};$$

(8) the matrix for $T_1^{x_1}T_2^{x_2}\cdots T_r^{x_r}$ is given by

$$\begin{pmatrix} \sum_{k=1}^{r} a_{11}^{k}x_k+1\cdots & \sum_{k=1}^{r} a_{1r}^{k}x_k \\ \cdots\cdots\cdots\cdots & \\ \sum_{k=1}^{r} a_{r1}^{k}x_k & \cdots \sum_{k=1}^{r} a_{rr}^{k}x_k+1 \end{pmatrix}.$$

The foregoing results, as well as the symbols involved, are based on the assumption that we are given a regular permutation group G. The operations θ and T_j, as originally defined, have a meaning only when every permutation

* For this method of defining G it is clearly a matter of indifference whether or not the elements
$$\theta^{-a}A_i=A_iT_i \qquad (i=1, 2, \cdots, r)$$
constitute a U-basis for G.

of G is regarded as known. We wish to reinterpret the operations T_j quite apart from the assumed existence of G, under the sole assumption that $A_1, \cdots, A_r$ are a U-basis for a given abstract abelian group A. (We do not think of A as having any particular concrete representation.) As above, we shall denote the orders of $A_1, \cdots, A_r$ by $p^{\delta_1}, \cdots, p^{\delta_r}$ respectively.

We now define T_j, $j=1, \cdots, r$, to be the substitution $A_1 \rightarrow A_1', \cdots, A_r \rightarrow A_r'$, which is given by (2) above. For this substitution to define an automorphism of A, it is necessary and sufficient that the r^2 elements a_{ik}^j be integers which satisfy the following two conditions: (a) the determinant $|M_j|$ of M_j is prime to p; (b) for $i>k$, a_{ik}^j is divisible by $p^{\delta_k-\delta_i}$. Let us assume that the elements of M_j have any integral values which satisfy (3), (4), and (5) above. Since (3) and (b) are identical, in order to show that T_j now defines an automorphism of A, it is sufficient to prove that $|M_j|$ is prime to p. This we can derive as a consequence of (4). Or, from (7), which was derived from (4), we see that some power of M_j is the identity matrix, whence $|M_j|$ must surely be prime to p. As a consequence of these restrictions which we have imposed on the elements of M_j, it follows that the operations $T_1, \cdots, T_r$ may be interpreted as automorphisms of A.

In the course of verifying that (3) follows from (3'), (4) from (4'), (5) from (5') it becomes evident that these three statements are reversible, in the sense that (3'), (4'), (5') as a whole follow from (3), (4), (5). Therefore, the r automorphisms $T_1, T_2, \cdots, T_r$ generate an abelian group, and A is isomorphic with this abelian group under the correspondence defined by

$$A_i \sim T_i \qquad (i = 1, 2, \cdots, r). \tag{9}$$

By applying the theorem in the second footnote to §4, we conclude that the products $A_x T_x$, where

$$A_x \text{ is } A_1^{x_1} A_2^{x_2} \cdots A_r^{x_r} \text{ and } T_x \text{ is } T_1^{x_1} T_2^{x_2} \cdots T_r^{x_r},$$

constitute a group $\overline{G}$ of order $p^{\Sigma\delta_i}$. That this group is metabelian follows from (4') and the fact that the commutator subgroup of $\overline{G}$ is generated by the A_{jk}. That G is conformal with A follows from (3'), (6'), and (8).

We append a rough summary of this section. In the first part we showed that for a given G and a given U-basis for A there is determined a set of elements for each of the r matrices M_j, the elements being uniquely determined if we require that each a_{ik}^j be a least positive residue modulo p^{δ_k}. These matrices, together with the orders of $A_1, \cdots, A_r$, define G, since each element of G can be given in the form $A_x T_x$. We enumerated certain necessary conditions which the elements of these matrices must satisfy. In the second part of this section we proved that these "necessary conditions" are

"sufficient," in the sense that any choice of elements for M_j which is consistent with these conditions will give rise to an automorphism T_j of A, while the totality of distinct products $A_x T_x$ will constitute a metabelian group conformal with A. This latter part of §14 represents a refinement of the procedure given in §4. The problem of constructing all metabelian groups which are conformal with a given abelian group A is therefore reduced to the problem of determining all possible sets of elements a_{ik}^{j} which satisfy conditions (3), (4), and (5) above.*

15. In this section we shall outline a method for constructing a representation of G as a linear congruence group. No proofs will be given, since the demonstrations in every instance follow obvious and familiar lines. We assume that G is given as a regular permutation group, and we assume that $A_1, \cdots, A_r$ are any primary U-basis for A. Then the elements in the r matrices M_j (see §14) are determined; with no loss of generality, we may assume that each a_{ik}^{j} is a least positive residue modulo p^{δ_k}.

Now the permutation A_1 may be represented by the symbol

$$\begin{pmatrix} A_1^{z_1} & A_2^{z_2} \cdots A_r^{z_r} \\ A_1^{z_1+1} & A_2^{z_2} \cdots A_r^{z_r} \end{pmatrix}.$$

Since T_1 is commutative with A_1, we may designate T_1 by the symbol

$$\begin{pmatrix} A_1^{z_1} & A_2^{z_2} \cdots A_r^{z_r} \\ A_1^{z_1} & A_2'^{z_2} \cdots A_r'^{z_r} \end{pmatrix},$$

where $A_2', \cdots, A_r'$ are defined by (2) of §14. The product $A_1 T_1$ is given by

$$\begin{pmatrix} A_1^{z_1} & A_2^{z_2} \cdots A_r^{z_r} \\ A_1^{z_1+1} & A_2'^{z_2} \cdots A_r'^{z_r} \end{pmatrix}. \tag{1}$$

In (1) we replace $A_2', \cdots, A_r'$ by their equivalents from (2) of §14 and bring the result into the form

$$\begin{pmatrix} A_1^{z_1} & A_2^{z_2} \cdots A_r^{z_r} \\ A_1^{z_1'} & A_2^{z_2'} \cdots A_r^{z_r'} \end{pmatrix}. \tag{2}$$

Now the permutation $A_1 T_1$ is completely characterized by the exponents in (2) above. Hence $A_1 T_1$ is defined by the linear substitution

$$Z_1: \quad \begin{aligned} z_1' &\equiv z_1 + a_{21}^{1} z_2 + a_{31}^{1} z_3 + \cdots + a_{r1}^{1} z_r + 1 && (\mathrm{mod}\ p^{\delta_1}), \\ z_2' &\equiv (a_{22}^{1} + 1) z_2 + a_{32}^{1} z_3 + \cdots + a_{r2}^{1} z_r && (\mathrm{mod}\ p^{\delta_2}), \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ z_r' &\equiv a_{2r}^{1} z_2 + a_{3r}^{1} z_3 + \cdots + (a_{rr}^{1} + 1) z_r && (\mathrm{mod}\ p^{\delta_r}). \end{aligned} \tag{3}$$

* We naturally restrict our choice of the a_{ik}^{j} to those which are least positive residues modulo p^{δ_k}.

By an analogous procedure we may construct the linear substitutions $Z_2, \cdots, Z_r$ which define $A_2T_2, \cdots, A_rT_r$ respectively. Since $A_1T_1, \cdots, A_rT_r$ generate G (see Theorem IV of §9), $Z_1, Z_2, \cdots, Z_r$ will generate a representation of G as a linear congruence group.

BROWN UNIVERSITY,
PROVIDENCE, R.I.