

# 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*.<sup>\*</sup> 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  $\Gamma$  and  $C$  respectively. The operations of  $G$  will usually be denoted by small letters ( $s$ ,  $\sigma$  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  $g_1, g_2, \dots, g_n$  are any set of independent generating operations (I.G.O.) for  $G$ ,<sup>†</sup> then  $C$  is generated by  $c_{12} = g_1^{-1}g_2g_1g_2^{-1}, c_{13}, \dots, c_{1n}, c_{23}, \dots, c_{2n}, \dots, c_{n-1,n}$ .

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

(c) If  $\sigma_a$  and  $\sigma_b$  are of orders  $p^{m_a}$  and  $p^{m_b}$  respectively,  $m_a \geq m_b$ , then the order of  $\sigma_a \sigma_b$  divides  $p^{m_a}$ .<sup>‡</sup> 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  $p$ th powers in  $G$  is itself a  $p$ th power in  $G$ .<sup>§</sup>

DEFINITION. Any operation of a given prime-power group which is not a  $p$ th 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  $\sigma_1, \sigma_2, \dots, \sigma_i, \dots$ .

We denote any permutation  $s_i$  of  $G$  (in the regular representation derived from post-multiplication) by the symbol  $(\sigma_{\sigma_i})$ . We may think of  $s_i$  as a representation of  $\sigma_i$ . A representation, as a permutation on the  $p^m$  symbols  $\sigma_1, \sigma_2, \dots$ , of any inner isomorphism  $S_i$  of  $G$  is afforded by the symbol  $(\sigma_i^{-1} \sigma_{\sigma_i})$ .\* 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  $(\sigma')$ .

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  $(\sigma_{\sigma'} \sigma) (\sigma')$ , where  $(\sigma_{\sigma'})$  is any permutation in the conjoint of  $G$ , while  $(\sigma')$  is any permutation of  $I(G)$ .

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

Now  $J \equiv \{G, H\}$  is a metabelian group of order  $p^{m+\mu}$ . Its central is  $\Gamma$ , its commutator subgroup is  $C$ ; the central quotient-group  $J/\Gamma$  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  $G/\Gamma$ , 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  $\theta$  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  $\theta_x$  by the equation  $\theta_x s = sS^x$ . (Since  $H$  is abelian,  $s_1 \sim S_1^x, s_2 \sim S_2^x, \dots$  etc. defines an isomorphism of  $G$  with  $H$ .) Let  $p^\nu$  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  $\sigma_1$  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  $p'$  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  $\theta$ . We note that  $\Gamma$  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  $\theta$  as an operator of period  $p'$ .

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

That they constitute a group follows from the equation  $(\theta^x s_i)(\theta^y s_j) = c_{i_j^{-x} \theta^x} (s_i s_j) = \theta^x (c_{i_j^{-x} s_i s_j})$ . 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  $\sigma_1$ . 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  $\Gamma$  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  $(\sigma')$  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

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

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  $\sigma_1, \sigma_2, \dots, \sigma_i, \dots$ , while every permutation of  $H$  omits  $\sigma_1$ , it is obvious that every permutation of  $G$

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

3. These  $p^r$  conformal groups  $G_1, G_2, \dots, G_x, \dots, G_{p^r} = G$  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  $t_i = s_i S_i^x$  and  $t_j = s_j S_j^x$  be any two operations of  $G_x$ . Now  $t_i^{-1} t_j t_i = t_j c_{ij}^{2x+1}$ , where  $c_{ij} = s_i^{-1} s_j s_i s_i^{-1}$ .\* 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  $p$ th powers of the elements of  $C$ . By means of the relation  $y \equiv 2x+1 \pmod{p^r}$ , we may associate with each member of  $D$  a value of  $y$  as a subscript. The  $p^{r-1}(p-1)$  members of  $D$  for which  $y$  is prime to  $p$  constitute a subset which we call  $D_1$ ; the  $p^{r-2}(p-1)$  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  $D_{p^r}$  consists of a single group, namely that  $G_x$  for which  $2x+1$  is divisible by  $p^r$ . This group, which is abelian, we shall designate by the letter  $A$ . Its permutations  $t_1, t_2, \dots, t_i, \dots$  are connected with those of  $G$  by the equation  $t_i = \theta^a s_i$ , where  $a$  is the smallest positive root of  $2a+1 \equiv 0 \pmod{p^r}$ . That  $G_a$  is abelian is sufficiently important to state as a theorem.

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

The conjoint of each group in a given set  $D_{p^\alpha}, \alpha = 0, 1, \dots, \nu$ , 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  $p^r$  for the conjoint of  $G_x$ . (It is easy to prove that the conjoint of  $G_x$  is  $G_{p^r-x-1}$ .)

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

Let  $\lambda$  be an integer prime to  $p$ . If we replace each operation of  $G_x$  by its  $\lambda$ th 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  $s_i^{-1} S_i s_i = S_j c_{ij}$  and  $S_i^{-1} s_j S_i = s_j c_{ij}$ . Of course  $S_i^{-1} S_j S_i = S_j$ .

be the permutation on the symbols  $\sigma_1, \sigma_2, \dots$  derived from associating each operation of  $G$  with its  $\lambda$ th power. Since  $T_\lambda$  defines an automorphism of the abelian group  $\Gamma$ , in determining how  $T_\lambda$  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  $2z \equiv 1 \pmod{p^\nu}$  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  $1-\lambda+2x \equiv 2\lambda\xi \pmod{p^\nu}$ . Then  $s_i^\lambda S_i^{\lambda\xi}$  is an operation of  $G_\xi$ . If we write the congruence above in the form  $1+2x \equiv \lambda(1+2\xi) \pmod{p^\nu}$ , 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  $p'$ . We can, therefore, identify the permutation  $T_\lambda$  with that automorphism of  $A$  which transforms each operation of  $A$  into its  $\lambda$ th power.

If we restrict the values of  $\lambda$  to the  $p'^{-1}(p-1)$  positive integers which are less than  $p'$  and prime to  $p$ , then the permutations  $T_\lambda$  constitute a cyclic group of order  $p'^{-1}(p-1)$ . We may identify each  $T_\lambda$  with the linear substitution  $X_\lambda$  on the subscripts of  $G_1, G_2, \dots, G_x, \dots$ , where  $X_\lambda$  is  $x' \equiv a[1 - \lambda'(2x+1)] \pmod{p'}$ , while  $a$  and  $\lambda'$  are defined by the congruences  $2a+1 \equiv 0 \pmod{p'}$  and  $\lambda\lambda' \equiv 1 \pmod{p'}$ . Or we can represent  $T_\lambda$  as the linear substitution  $Y_\lambda: y' \equiv \lambda'y \pmod{p'}$ . The order of  $T_\lambda$  is obviously the period of  $\lambda$  with respect to  $p'$ . When  $\lambda$  is  $p'-1$ , then  $T_\lambda$  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  $s_1, s_2, \dots$  all begin with the same letter  $\sigma_1$ , 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  $\sigma_1$ . The subgroup of  $I(G)$  which gives the inner isomorphisms of  $G$  we shall denote by  $H$ . We let  $S_1, S_2, \dots$  denote the permutations of  $H$ , where  $S_i$  transforms  $G$  according to  $s_i$ . Furthermore,  $p'$  denotes the order of the element of highest order in  $H$ , while  $a$  is the least positive root of  $2a+1 \equiv 0 \pmod{p'}$ . 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  $\sigma_1$ . 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  $t_1, t_2, \dots$  denote the permutations of  $A$  and let  $R_1, R_2, \dots$  denote the permutations of a subgroup  $\bar{R}$  of  $I(A)$ . Let  $\gamma_{ij}$  denote the commutator  $R_i^{-1}t_jR_it_j^{-1}$ , and (c) let every product  $\gamma_{ij}\gamma_{ji}^{-1}$  be invariant under  $\bar{R}$ . If the correspondence  $\bar{\Gamma} \sim E, \dots, \bar{\Gamma}t_i \sim R_i, \dots$  defines an isomorphism  $\tau$  of  $A$  with  $\bar{R}$  for which (d)  $\bar{\Gamma}$  contains every  $\gamma_{ij}$ , then the  $p^m$  products*

$$(1) \quad \bar{\Gamma}E, \dots, \bar{\Gamma}t_iR_i, \dots$$

*constitute a metabelian subgroup  $\bar{G}$  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  $\bar{R}$  have only the identity in common. That these products constitute a metabelian group is a consequence of (c). From the existence of  $\tau$  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  $\bar{G}$  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  $\bar{R}$  of  $I(A)$ , it is clearly sufficient to show that  $\bar{G}$  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  $\bar{G}$  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  $\gamma_{ij}$  need not be separately invariant under  $\bar{G}$ . But it is obvious that every commutator  $R_k^{-1}\gamma_{ij}R_k\gamma_{ji}^{-1}$  must be invariant under  $\bar{G}$ , and hence under  $\bar{R}$ . That is, the class of  $\{A, \bar{R}\}$  cannot exceed 2.

This derivation of  $\bar{G}$  from  $A$  and  $\bar{R}$  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  $Q \sim E, \dots, \bar{Q}q_i \sim q'_i, \dots$ , where  $Q$  contains all commutators  $q_i^{-1}q_kq_iq_k^{-1}, q_k$  and  $q'_i$  being any two elements of  $Q$  and  $Q'$  respectively. Then the  $m$  products*

$$(1) \quad \bar{Q}E, \dots, \bar{Q}q_iq'_i, \dots$$

*constitute a group  $Q''$  of order  $m$ .*

From (c) it is clear that  $q_kq'_iq_jq'_i$  can be brought into the form  $q_{ij}q'_i q'_j q'_i$ , where  $q_{ij}$  is in  $\bar{Q}$ . 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  $q_i^{-1}q_j = q'_j q'_i^{-1} = E$ .

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  $\bar{G}$  is the same as in Theorem I of §4.

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

We regard the elements of  $\bar{G}$  as a certain  $p^m$  products  $t_i R_i$ ; (see Theorem I of §4). We write  $\bar{G}$  in cosets with respect to  $\bar{\Gamma}$ , where  $\bar{\Gamma}$  is the subgroup of  $\bar{G}$  (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  $\bar{G}$  is a regular group.*

As above, we regard the elements of  $G$  as the products  $t_i R_i$ . Since each permutation of  $I(A)$  omits  $\sigma_1$ , the initial letter in the permutations of  $A$ , we see that every permutation in  $\bar{G}$  permutes  $\sigma_1$ . If a certain permutation, say  $\bar{i}$ , of  $\bar{G}$  should omit the letter  $\sigma_k$ , then we could find a permutation  $t$  in  $A$  such that  $t^{-1} \bar{i} t$  would omit  $\sigma_1$ . 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  $\Gamma'$  and  $\Gamma''$  denote the centrals of  $G'$  and  $G''$  respectively. Obviously  $\Gamma'$  and  $\Gamma''$  are simply-isomorphic subgroups in  $A$ . We denote the permutations of  $G'$  by  $s'_1, s'_2, \dots$  and those of  $H'$  by  $S'_1, S'_2, \dots$ , 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  $t'_i = s'_i S'_i{}^a$  ( $t''_i = s''_i S''_i{}^a$ ). We write  $\bar{S}'_i$  for  $S'_i{}^{-a}$  and  $\bar{S}''_i$  for  $S''_i{}^{-a}$ . Then the permutations of  $G'$  and of  $G''$  are derivable from those of  $A$  by the equations

$$(1) \quad s'_i = t'_i \bar{S}'_i$$

and

$$(2) \quad s''_i = t''_i S''_i$$

respectively.

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

$$(3) \quad \Gamma' \sim \Gamma'', \dots, \Gamma' t'_i \bar{S}'_i \sim \Gamma'' t''_i \bar{S}''_i, \dots, \Gamma' t'_i \bar{S}'_i \sim \Gamma'' t''_i \bar{S}''_i, \dots.$$

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

$$(4) \quad \dots, \bar{S}'_i \sim \bar{S}''_i, \dots, \bar{S}'_i \sim \bar{S}''_i, \dots.$$

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  $\gamma_{ij}'$  must correspond to  $\gamma_{ij}''$  under (3), we get

$$(5) \quad (t'_i t'_j)(\bar{S}'_i \bar{S}'_j) \sim (t''_i t''_j)(\bar{S}''_i \bar{S}''_j).$$

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

$$(6) \quad \Gamma' \sim \Gamma'', \dots, \Gamma' t'_i \sim \Gamma'' t''_i, \dots, \Gamma' t'_i \sim \Gamma'' t''_i, \dots.$$

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

$$(7) \quad \Gamma' \sim \Gamma'', \dots, \Gamma' t'_i \bar{S}'_i \sim \Gamma'' t''_i \bar{\Pi}^{-1} \bar{S}'_i \bar{\Pi}, \dots.$$

Since  $\bar{\Pi}^{-1} \gamma_{ij}' \bar{\Pi}$  equals  $\gamma_{ij}''$ , it follows that  $\bar{\Pi}^{-1} \bar{S}'_i \bar{\Pi}$  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  $\bar{\Pi}^{-1} \bar{S}'_i \bar{\Pi}$  and  $G''$  coincides with  $\bar{\Pi}^{-1} G' \bar{\Pi}$ . 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  $\bar{R}$  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  $\bar{R}$  to the following additional restrictions: each  $\gamma_{ij}$  is invariant under  $\bar{R}$ ;  $\gamma_{ij} = \gamma_{ji}^{-1}$  (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  $\pi$  of order 3 which is commutative with  $A_1$  and  $A_3$  and transforms  $A_2$  into  $A_2A_1$ . We see that  $\pi$  permutes exactly 18 letters. Since  $\pi$  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  $\bar{G} = \{A_1, A_2, A_3\pi\}$ , 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:  $A, C, \Gamma, G/C, G/\Gamma$  (which is simply isomorphic with  $H$ ). From each of these groups there arises a set of arith-

metrical invariants of  $G$ . We enumerate the following:

- (1) the  $r$  invariants  $p^{\delta_1}, p^{\delta_2}, \dots, p^{\delta_r}$  of  $A$ ;
- (2) the  $l$  invariants  $p^{a_1}, \dots, p^{a_l}$  of  $C$ ;
- (3) the invariants  $p^r, p^r, p^{r_3}, \dots, p^{r_h}$  of  $G/\Gamma$ ;
- (4) the invariants of  $\Gamma$ ;
- (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  $\nu$ , while  $G/\Gamma$  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  $\mathcal{U}_\alpha$  the subgroup composed of the  $p^\alpha$ th powers of the elements of  $G$ . These groups  $\mathcal{U}_\alpha$  constitute a series of characteristic subgroups  $\mathcal{U}_1, \mathcal{U}_2, \dots, \mathcal{U}_{\delta_1} = E$  of  $G$ , each being contained in those which precede it.\* For  $C$  we define the series  $C_1, C_2, \dots, C_r = E$ , where  $C_\alpha$  is the subgroup composed of the  $p^\alpha$ th powers of the elements of  $C$ . Finally we have a third series  $\bar{C}_1, \bar{C}_2, \dots, \bar{C}_r = E$ , where  $\bar{C}_\alpha$  is the subgroup composed of those elements of  $C$  which are in  $\mathcal{U}_\alpha$ . Obviously  $\bar{C}_\alpha$  contains  $C_\alpha$ . 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  $C/\bar{C}_1$ ;
- (8) the number  $l_2$  of invariants of  $\bar{C}_1/C_1$ .†

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

For the case where  $C/\bar{C}_1$  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  $C \equiv \bar{C}_1$ . Such groups we shall call  $\omega$ -groups. An immediate illustration of their significance is provided by

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

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

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

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

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

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  $\phi$ -subgroup  $\Phi(G)$  of  $G$ . That (a)  $\Phi(G)$  is the cross-cut of all subgroups of index  $p$  in  $G$ , and that (b)  $G/\Phi$  is of order  $p^n$  and type  $1, 1, \dots, 1$ , are two familiar results in the theory of prime-power groups. From (b) it follows that  $\Phi(G)$  is generated by  $\mathfrak{U}_1(G)$  and  $C$ .

Now  $\Phi(A)$ , the  $\phi$ -subgroup of  $A$ , coincides with  $\mathfrak{U}_1(A)$ . Obviously  $\mathfrak{U}_1(A)$  is  $\theta^a\mathfrak{U}_1(G)$ . 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  $1, 1, \dots, 1$  to  $l_1$  factors.*

From Theorem II follows

**THEOREM III.** *For  $G$  to be an  $\omega$ -group it is necessary and sufficient that  $r$  equal  $n$ . If  $G$  is not an  $\omega$ -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  $g_1, \dots, g_n$  are a set of I.G.O. for  $G$ , then no product  $g_1^{x_1}g_2^{x_2} \dots g_n^{x_n}$  in which an exponent is prime to  $p$  can be in  $\Phi(G)$ . The second is

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

To prove this, we note that every operation  $\sigma$  in  $G$  can be expressed in the form  $g_y c$ , where  $g_y$  is  $g_1^{y_1}g_2^{y_2} \dots g_n^{y_n}$  and  $c$  is some element in  $C$ . Since  $C$  is in  $\mathfrak{U}_1(G)$ ,  $c$  can be expressed as  $(g_x c')^p$ . Then  $\sigma$  can be brought into the form  $g_y g_x^p c'^p = g_y c''$ . Since the order of  $c''$  is less than the order of  $c$ , we can eventually bring  $\sigma$  into the form  $g_x$  above.

BASES FOR  $G$

7. Any set of elements  $g_1, g_2, \dots$  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  $q_1, q_2, \dots$  of  $Q$  such that  $Q$  is the direct product of the cyclic subgroups  $\{q_1\}, \{q_2\}, \dots$ . To

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

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  $g_1, g_2, \dots, g_n$ . Let  $g_x$  be any product  $g_1^{x_1} g_2^{x_2} \dots g_n^{x_n}$  in which the  $g_i$  occur, without repetitions, in the normal order  $g_1, g_2, \dots$  etc.\*

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

(2) If  $g_x$  is in  $\Gamma$  only when each factor  $g_i^{x_i}$  is in  $\Gamma$ , then the  $g$ 's are said to constitute a  $\Gamma$ -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  $P_1, P_2, \dots, P_p$  is said to constitute a *uniqueness-basis* ( $U$ -basis) for  $G$  provided that each operation of  $G$  can be represented uniquely in the form  $P_1^{x_1} P_2^{x_2} \dots P_p^{x_p}$ , 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  $v_1^{x_1} v_2^{x_2} \dots$  is clearly in  $C$  only if each  $v_i^{x_i}, v_2^{x_2}$ , 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  $\Gamma$ -basis for  $G$  we first write  $G$  in cosets with respect to  $\Gamma$ ; then, from each of those cosets which correspond to the elements of a  $U$ -basis for  $G/\Gamma$ , we select an operation of  $G$ , obtaining thereby the  $h$  operations  $u_1, u_2, \dots, u_h$ .

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

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

\* Throughout this paper it is assumed that in any indicated product, such as  $A_1^{x_1} \dots A_r^{x_r}, P_1^{x_1} \dots P_r^{x_r}$  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  $G/\Gamma$  is of type  $\alpha, \alpha, \dots, \alpha$ . 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  $\Gamma$ -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.,  $\beta_1, \beta_2, \dots, \beta_n$  with the property that  $\beta_1^{\lambda_1} \beta_2^{\lambda_2} \dots \beta_n^{\lambda_n}$  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  $\beta_1$  be such an operation, and let  $\beta_2$  be an operation in  $G$  of lowest possible order such that  $\beta_1$  and  $\beta_2$  generate  $G$ . We shall now prove that  $\{\beta_1\}$  and  $\{\beta_2\}$  can have only the identity in common.

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

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

(Since  $p$  is an odd prime,  $(p^{e_1} + 1) / 2$  is an integer; since  $\beta_2^{p^{e_2}}$  is commutative with  $\beta_1$ , the order of the element in the brackets divides  $p^{e_1}$ .) Clearly  $\beta_1$  and  $\beta_2 \beta_1^{b p^{e_1}}$  generate  $G$ . But the order of this second operation is less than the order of  $\beta_2$ , 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  $\bar{s}_1, \bar{s}_2, \dots, \bar{s}_{n-1}, \bar{s}$  the first  $n - 1$  elements generate a metabelian (or abelian) subgroup  $\bar{H}$  of  $G$ . Since  $G$  is  $\{\bar{H}, \bar{s}\}$ , it is clear that  $\bar{H}$  has exactly  $n - 1$  I.G.O. Hence for  $\bar{H}$  we can find a  $B$ -basis, say  $\beta_1, \beta_2, \dots, \beta_{n-1}$ . We now show that  $\beta_1, \dots, \beta_{n-1}, \bar{s} = \beta_n$  must constitute a  $B$ -basis for  $G$ . Let us assume the contrary; that is, let  $\beta_1^{\lambda_1} \beta_2^{\lambda_2} \dots \beta_{n-1}^{\lambda_{n-1}} \beta_n^{\lambda_n} = E$ , where at least one of the  $\lambda$ 's is not divisible by the order of the  $\beta$  to which it belongs. Certainly one of these  $\lambda$ 's must be  $\lambda_n$ , since  $\beta_1, \dots, \beta_{n-1}$

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

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

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

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

Since  $(\beta)$  could not be the identity, we should have  $(\beta) = (c)^{-1} \neq E$ . Since  $(\beta)$  and  $(c)$  would be of the same order, at least two of the  $\lambda$ 's would necessarily be prime to  $p$ . But  $(\beta)$  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  $P_1, P_2, \dots, P_p$  to constitute a  $U$ -basis for  $G$ :

- (A)  $P_x = P_1^{x_1}P_2^{x_2} \dots P_p^{x_p}$  and  $P_y = P_1^{y_1} \dots P_p^{y_p}$  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  $P_1, P_2, \dots, P_p$  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  $S_i^{-\alpha}$ .

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

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

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

- (i) the product of the orders of  $A_1, A_2, \dots$  equals the order of  $A$ ;
- (ii) the product  $A_x = A_1^{x_1} A_2^{x_2} \dots$  can be the identity only when each factor  $A_1^{x_1}, A_2^{x_2}, \dots$  is the identity.

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

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  $P_x P_y^{-1} = E$ , and this latter equation may be brought into the form

$$(1) \quad P_x P_y^{-1} = P_1^{x_1 - y_1} \dots P_\rho^{x_\rho - y_\rho} \prod_{i < j} c_{ij}^{-v_i(x_j - y_j)} = E,^* \text{ where } c_{ij} = P_i^{-1} P_j P_i P_j^{-1}.$$

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

$$(2) \quad P_{y+z} P_y^{-1} = P_1^{z_1} P_2^{z_2} \dots P_\rho^{z_\rho} \prod c_{ij}^{-v_i z_j} = E.$$

Now the product

$$A_u = (P_1 S_1^\alpha)^{u_1} (P_2 S_2^\alpha)^{u_2} \dots (P_\rho S_\rho^\alpha)^{u_\rho}$$

can be reduced to the form

$$(3) \quad A_u = P_1^{u_1} \dots P_\rho^{u_\rho} \prod c_{ij}^{-a u_i u_j} \prod S_i^{a u_i}.$$

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

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  $a u_i$  and  $z_i$  equal to  $u_j$ , we see from (3) that  $A_u$  can be the identity only when the order of  $P_i S_i^\alpha$  divides  $u_i$ . This completes our proof.

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

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  $p^{a_1}, p^{a_2}, \dots, p^{a_r}$  of  $A$ .\**

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

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

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

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

The  $U$ -basis  $A_1, \dots, A_r$  is said to be a *primary  $U$ -basis for  $A$*  provided that for the associated automorphisms  $T_1, \dots, T_r$  (arising from the equation  $s_i = \theta^{-a_i} A_i = A_i T_i$ ) any product  $T_z = T_1^{z_1} T_2^{z_2} \dots T_r^{z_r}$  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  $A_1, \dots, A_r$  are any given  $U$ -basis for  $A$ , then the elements  $A_1T_1, \dots, A_rT_r$  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

$$(4) \quad (A_1T_1)^{z_1}(A_2T_2)^{z_2} \dots (A_rT_r)^{z_r} = (A_1T_1)^{v_1} \dots (A_rT_r)^{v_r}.$$

This equation we may bring into the form

$$(5) \quad A_{z-y} \gamma_{z-y} T_{z-y} = E,$$

where

$$A_{z-y} = \prod_{i=1}^r A_i^{z_i - v_i}, \quad \gamma_{z-y} = \prod_{i < j} \gamma_{ij}^{(z_i + v_j)(x_j - v_i)},$$

$\gamma_{ij}$  being

$$T_i A_j T_i^{-1} A_j^{-1}; \quad T_{z-y} = \prod_1^r T_i^{z_i - v_i}.$$

For convenience we shall write  $z_i$  in place of  $x_i - y_i$  and  $v_i$  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.

$$(6) \quad A_s \gamma_s = E.$$

If (6) is satisfied only by  $A_s = E$ , then the  $A_i T_i$  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  $\gamma_s^{-1}$ , where  $A_s$  is not the identity. Then  $A_s$  and  $\gamma_s$  must be of the same order.

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

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

$$(7) \quad A_s = \gamma_s^{-1}, A_s \neq E,$$

is an impossible one.

As an element of  $A$ , each  $\gamma_{ij}$  can be expressed in the form  $A_1^{b_1} A_2^{b_2} \dots A_r^{b_r}$ . If the exponent of every  $\gamma_{ij}$  in  $\gamma_s$  is divisible by  $p^\alpha$  (but not by  $p^{\alpha+1}$ ), then each exponent  $z_i$  in  $A_s$  must be divisible by  $p^\alpha$ . In this case there must exist an element  $\bar{A}_\alpha$  in  $A$ , whose order does not exceed  $p^\alpha$ , such that  $\bar{A}_\alpha A_{s'}$  equals  $\gamma_s^{-1}$ , where  $z_i$  is  $p^\alpha z'_i$ , while  $A_{s'}$  and  $\gamma_{s'}$  are derived from  $A_s$  and  $\gamma_s$  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  $\bar{A}_\alpha$ , since  $\bar{A}_\alpha$  is of lower order than  $A_{s'}$ . We shall, therefore, assume that in equation (7) the exponent of one of the  $\gamma_{ij}$ , say of  $\gamma_{ab}^{u_a u_b}$ , is prime to  $p$ . Then  $A_b^{u_b}$  must be a principal element of  $A$ . Since  $A_b^{u_b}$  occurs in  $\gamma_s^{-1}$ , some constituent of  $\gamma_s$ , say  $\gamma_{cd}^{u_c u_d}$ , must contain  $A_b^\lambda$ , where  $\lambda$  is some exponent prime to  $p$ . Obviously  $u_c z_d$  must be prime to  $p$ , and  $\gamma_{cd}$  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

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

But the assumption that  $A_1, \dots, A_r$  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  $A_1, \dots, A_r$ , 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  $A_1, \dots, A_r$  of  $A$ . The order of  $A_i$  is of course  $p^{\delta_i}$ ; we assume the inequalities  $\delta_1 \geq \delta_2 \geq \dots \geq \delta_r$ .

It is a well known fact that the  $r$  elements

$$(1) \quad A'_i = A_1^{a_{i1}} A_2^{a_{i2}} \dots A_r^{a_{ir}} \quad (i = 1, 2, \dots, r)$$

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  $p^{\delta_i - \delta_j}$  for  $i > j$ . We propose to determine the  $a_{ij}$  so that  $A'_1, \dots, A'_r$  will be a primary  $U$ -basis for  $A$ .

If the  $T_i$ 's satisfy no relation of the form

$$(2) \quad T_1^{\lambda_1} T_2^{\lambda_2} \dots T_r^{\lambda_r} = E$$

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

$$A'_\alpha = A_\alpha^{\lambda_\alpha} A_{\alpha+1}^{\lambda_\alpha+1} \dots A_r^{\lambda_\alpha}$$

Then for the permutation  $T'_\alpha$  of  $H$  which is associated with  $A'_\alpha$  we shall have the equation

$$(3) \quad T'_\alpha = T_1^{-\lambda_1} T_2^{-\lambda_2} \dots T_{\alpha-1}^{-\lambda_{\alpha-1}},$$

where  $\lambda_1, \dots, \lambda_{\alpha-1}$  are all divisible by  $p$ . From the remaining relations of type (2) we eliminate  $T_\alpha$  by means of the equation  $T_\alpha = T_1^{-\lambda_1} \lambda_\alpha^{-1} \dots T_r^{-\lambda_r} \lambda_\alpha^{-1}$ , arranging, of course, the elements in each new relation according to the sequence  $T_1, T_2, \dots, T_{\alpha-1}, T_{\alpha+1}, \dots$ . 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  $A'_1, \dots, A'_r$  for which a certain  $h$  of the  $T$ 's, say  $T_{e_1}', T_{e_2}', \dots, T_{e_n}'$ , constitute a set of I.G.O. for  $H$ , while each of the remaining  $T$ 's is of the form

$$T_{e_1}^{d_1 p} \dots T_{e_n}^{d_n p}$$

That  $A'_1, \dots, A'_r$  constitute a  $U$ -basis for  $A$  is obvious from the fact that  $|a_{ij}|$  equals  $\lambda_\alpha \lambda'_\alpha \dots$ , while  $\lambda_\alpha, \lambda'_\alpha, \dots$  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  $\omega$ -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  $\omega$ -group is clear from the following example.

Let  $G$  be the metabelian group defined by the relations

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

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  $\beta_1, \beta_2, \dots, \beta_n$  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  $\chi$ , which equals the sum of the orders of the elements in this  $B$ -basis. Those  $B$ -bases for which  $\chi$  is a minimum in  $G$  we shall call  $MB$ -bases.

Let the elements of any  $MB$ -basis be denoted by  $\beta_1, \beta_2, \dots, \beta_n$ , of orders  $p^{\eta_1}, \dots, p^{\eta_n}$  respectively, where  $\eta_1 \geq \eta_2 \geq \dots \geq \eta_n$ . We know that every operation of  $G$  can be represented in the form  $\beta'_x = \beta_x c$ , where  $\beta_x$  equals  $\beta_1^{x_1}\beta_2^{x_2} \dots \beta_n^{x_n}$ , while  $c$  is some element of  $C$ . Furthermore, we know that the order of  $\beta_x$  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  $\beta_x$  is a principal element of  $G$ , then the order of  $\beta'_x$  is the order of that one of its constituents  $\beta_1^{x_1}, \beta_2^{x_2}, \dots, \beta_n^{x_n}, c$  which is of highest order.*

The theorem is clearly true when  $\beta_x$  and  $c$  are of unequal orders. So we assume that  $\beta_x$  and  $c$  are both of order  $p^a$ , while  $\beta'_x$  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  $\beta'_y$  is of lower order than  $\beta_y$ , there is

none whose order is less than  $p^b$ .

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

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

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

Now we can find in  $G$  an operation  $\beta'_z = \beta_{zc'}$ , where  $\beta_z$  is a principal element  $\beta_1^{z_1} \beta_2^{z_2} \dots \beta_n^{z_n}$  in  $G$ , such that  $\beta'_z{}^{p^e}$  equals  $\beta_\lambda'$  (see (d) of §1). The order of  $\beta_z$  is clearly greater than  $p^e$ ; the order of  $\beta'_z$  is  $p^e$ , since  $\beta_\lambda'$  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  $\beta_x$ , where each exponent  $x_i$  is a least positive residue modulo  $p^{n_i}$ , then the  $x_i$ 's are uniquely determined.*

Suppose that  $s$  is given by  $\beta_x$  and also by  $\beta_y$ , where  $\beta_y$  is  $\beta_1^{y_1} \beta_2^{y_2} \dots \beta_n^{y_n}$ . 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  $\beta_{x-y}$  is  $\beta_1^{x_1 - y_1} \dots \beta_n^{x_n - y_n}$  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  $\beta_{x-y}$  must be the identity, since  $\beta_{x-y} = E$  requires  $x_i - y_i \equiv 0 \pmod{p^{n_i}}$ .

Suppose that  $\beta_{x-y}$  is not the identity. Then each exponent in  $\beta_{x-y}$  must be divisible by  $p$ ; otherwise,  $\beta_{x-y}$  could not be in the  $\phi$ -subgroup of  $G$ . Let  $p^\alpha$  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  $\beta'_z = \beta_{zc'} = \beta_1^{z_1} \beta_2^{z_2} \dots \beta_n^{z_n} c'$ , such that  $\beta_z$  is a principal element of  $G$ , and such that  $\beta'_z{}^{p^\alpha}$  is  $\beta_{x-y} c_{x-y}$ . Since the order of  $\beta_z$  exceeds  $p^\alpha$ , this leads to a contradiction of Theorem I. Hence  $\beta_{x-y}$  must be the identity.

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

To prove the "conversely" we need only to show that the elements  $P_1, P_2, \dots, P_r$  of a  $U$ -basis constitute a set of I.G.O. for  $G$ . The  $\phi$ -subgroup of an  $\omega$ -group is  $\mathfrak{U}_1(G)$ . Clearly a product  $P_1^{\lambda_1} P_2^{\lambda_2} \dots P_r^{\lambda_r}$  can be a  $p$ th power in  $G$  only when each  $\lambda$  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  $\bar{\beta}_s = \bar{\beta}_1^{x_1} \bar{\beta}_2^{x_2} \dots \bar{\beta}_n^{x_n}$ , where  $\bar{\beta}_1, \bar{\beta}_2, \dots, \bar{\beta}_n$  are a  $B$ -basis for  $G$ , we have only to show that  $s$  is uniquely represented by  $\bar{\beta}_s$ , whenever the exponents  $x_i$  are least positive residues.

In the proof of Theorem II above we use the assumption that  $\beta_1, \beta_2, \dots, \beta_n$  are an  $MB$ -basis in order to show that  $\beta_x = \beta_y$  requires  $\beta_{x-y} = E$ . But if  $G$  is an  $\omega$ -group, we can prove this without requiring that the  $\beta$ 's constitute an  $MB$ -basis. If  $\bar{\beta}_1, \bar{\beta}_2, \dots, \bar{\beta}_n$  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  $\omega$ -group every commutator can be expressed in the form  $\bar{\beta}_1^{d_1 p} \bar{\beta}_2^{d_2 p} \dots \bar{\beta}_n^{d_n p}$ . 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  $\omega$ -group, then in Theorem II we may replace our assumption that  $\beta_1, \beta_2, \dots, \beta_n$  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  $\bar{\beta}_1, \bar{\beta}_2, \dots, \bar{\beta}_n$  satisfy the requirements (A) and (C) of §9 and accordingly constitute a  $U$ -basis for  $G$ .

**THEOREM IV.** *If  $G$  is an  $\omega$ -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  $\omega$ -group, this follows directly from Theorem III. We let  $\beta_1, \beta_2, \dots, \beta_n$ , of orders  $p^{\eta_1}, p^{\eta_2}, \dots, p^{\eta_n}$  respectively, and  $\beta'_1, \beta'_2, \dots, \beta'_n$ , of orders  $p^{\eta'_1}, p^{\eta'_2}, \dots, p^{\eta'_n}$ , be any two  $MB$ -bases for  $G$ . We may assume the inequalities  $\eta_1 \geq \eta_2 \geq \dots \geq \eta_n$  and  $\eta'_1 \geq \eta'_2 \geq \dots \geq \eta'_n$ . Now  $\eta_1$  and  $\eta'_1$  must be equal. Let  $\eta'_\alpha$  be the first one of the  $\eta'$ 's which differs from its corresponding  $\eta$ , and let  $\eta'_\alpha$  be less than  $\eta_\alpha$ . Now the elements  $\beta'_1, \dots, \beta'_n$  can be expressed in terms of the  $\beta$ 's by means of the equations

$$(1) \quad \beta'_i = \beta_1^{a_{i1}} \beta_2^{a_{i2}} \dots \beta_n^{a_{in}} c_i \quad (i = 1, 2, \dots, n)$$

where  $c_1, \dots, c_n$  are elements of  $C$ . Since the  $\beta$ '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

$\beta_{\alpha'}$  is  $p^{\eta_{\alpha'}}$ , either (b)  $a_{\alpha 1}, a_{\alpha 2}, \dots, a_{\alpha \alpha}$  are divisible by  $p^{\eta_1 - \eta_{\alpha'}}, p^{\eta_2 - \eta_{\alpha'}}, \dots, p^{\eta_{\alpha} - \eta_{\alpha'}}$  respectively, or (c) the order of  $\beta_1^{a_{\alpha 1}} \beta_2^{a_{\alpha 2}} \dots \beta_n^{a_{\alpha n}}$  exceeds the order of  $\beta_{\alpha'}$ . 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,  $\eta_i'$  must equal  $\eta_i$ , for  $i=1, 2, \dots, n$ .

To our list of invariants in §6 we may add the invariants  $p^{\eta_1}, p^{\eta_2}, \dots, p^{\eta_n}$ . Obviously  $\eta_1$  equals  $\delta_1$ . That these invariants coincide with a certain  $n$  of the invariants  $p^{\delta_1}, p^{\delta_2}, \dots, p^{\delta_r}$  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  $\omega$ -groups the theorem is trivial. We therefore assume that  $G$  is not an  $\omega$ -group.

(i) We first show that  $A_1 = \theta^a \beta_1, A_2 = \theta^a \beta_2, \dots, A_n = \theta^a \beta_n$  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  $A_{n+1}, \dots, A_r$  such that  $A_1, \dots, A_r$  will constitute a  $U$ -basis for  $A$ .

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

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

$$(2) \quad A_1^{\lambda_1} A_2^{\lambda_2} \dots A_n^{\lambda_n} = E$$

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

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

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

Now  $\beta_1^{\lambda_1} \beta_2^{\lambda_2} \dots \beta_n^{\lambda_n}$  cannot be in  $\Phi(G)$  unless each  $\lambda_i$  is divisible by  $p$ . Consequently, every exponent  $a \lambda_i \lambda_j$  must be divisible by  $p^2$ . Evidently  $\beta_1^{\lambda_1} \dots \beta_n^{\lambda_n}$  must be the identity, if equation (3) is to hold. Since the  $\beta$ 's are an  $MB$ -basis, each  $\lambda_i$  must be divisible by  $p^{\eta_i}$ . Since the order of  $A_i$  is  $p^{\eta_i}$ , 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  $Q_1, Q_2, \dots, Q_{l_1}$ , of orders  $p^{t_1}, p^{t_2}, \dots, p^{t_{l_1}}$ , be any  $U$ -basis for  $A/A'$ .\* We wish to show that the coset of  $A$  which corresponds to  $Q_j, j=1, 2, \dots, l_1$ , 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  $\mathfrak{U}_1(A)$ . If  $c_j$  is of order  $p^{k_j}$ , then we denote it by the letter  $A_{n+j}$  and add it to the set  $A_1, \dots, A_n$ . If not, then there must exist an equation

$$(4) \quad c_j p^{k_j} = (A_1^{b_1} A_2^{b_2} \dots A_n^{b_n}) p^{\xi},$$

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

$$(5) \quad (\beta_1^{b_1} \beta_2^{b_2} \dots \beta_n^{b_n}) p^{\xi} = c' p^{\xi} c_j p^{-\zeta_j}.$$

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

**Proof of (iii).** Let  $T_1, T_2, \dots, T_r$  be the permutations of  $H$  which correspond by means of the equation  $s_i = \theta^{-a_i} t_i$  to  $A_1, \dots, A_r$  as determined in (i) and (ii) above. From the manner of selection for  $A_1, A_2, \dots, A_r$  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  $A_{n+1}^{x_{n+1}} A_{n+2}^{x_{n+2}} \dots A_r^{x_r}$  must be in  $\Phi(G)$ .

Now the equation

$$(6) \quad (A_1 T_1)^{x_1} \dots (A_r T_r)^{x_r} = (A_1 T_1)^{y_1} \dots (A_r T_r)^{y_r}$$

can be brought into the form

$$(7) \quad \beta_1^{x_1 - y_1} \dots \beta_n^{x_n - y_n} = \beta_\phi,$$

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

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

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  $p$ .<sup>\*</sup> Hence the proof of Theorem IV in §9 is applicable to the  $U$ -basis  $A_1, \dots, A_r$ , as determined in (i) and (ii) above. Having proved that

<sup>\*</sup> In the hypothesis of Theorem IV in §9 we demanded this property of every equation  $T_1^{x_1} \dots T_r^{x_r} = E$ . Obviously it is sufficient to require it only for that particular equation which arises from equation (5) of §9.

$A_1T_1, \dots, A_rT_r$ , 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.,  $p^{n_1}, p^{n_2}, \dots, p^{n_r}, p^{l_1}, \dots, p^{l_r}$ , do not, in this sequence, necessarily coincide with  $p^{\delta_1}, p^{\delta_2}, \dots, p^{\delta_r}$  respectively.

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

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

**THEOREM VIII.** *If  $P_{s_1}, P_{s_2}, \dots, P_{s_r}$  are the elements  $P_1, P_2, \dots, P_r$  above written in any arbitrary sequence, then each element of  $G$  can be expressed uniquely in the form  $P_{s_1}^{x_1}P_{s_2}^{x_2} \dots P_{s_r}^{x_r}$ , 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  $P_1, P_2, \dots, P_r$  be any  $U$ -basis for  $G$ . Any  $n$  elements  $P_{s_1}, P_{s_2}, \dots, P_{s_n}$  (of this  $U$ -basis) which generate  $G$  will constitute an  $MB$ -basis for  $G$ .*

Since  $P_1, \dots, P_r$  generate  $G$ , it is obvious that a certain  $n$  of them, say  $P_{s_1}, \dots, P_{s_n}$ , will constitute a set of I.G.O. for  $G$ . Let the orders of these be  $p^{n_1}, p^{n_2}, \dots, p^{n_n}$ ,  $\eta_1 \geq \eta_2 \geq \dots \geq \eta_n$ . Let  $\beta_1, \beta_2, \dots, \beta_n$ , of orders  $p^{\eta_1}, p^{\eta_2}, \dots, p^{\eta_n}$ ,  $\eta_1 \geq \eta_2 \geq \dots \geq \eta_n$ , be any  $MB$ -basis for  $G$ . Our theorem will follow if we can show that  $\eta'_i$  must equal  $\eta_i$ ,  $i=2, 3, \dots, n$ , since  $P_{s_1}, \dots, P_{s_n}$  constitute at least a  $B$ -basis.

Now each  $\beta_i$ ,  $i=1, 2, \dots, n$ , can be expressed in the form  $\beta_i = P_{s_1}^{a_{i1}}P_{s_2}^{a_{i2}} \dots P_{s_n}^{a_{in}}c_i$ , where  $c_i$  is some element of  $C$ . Suppose that  $\eta'_\alpha$  is the first of the  $\eta$ 's, in the sequence  $\eta'_2, \eta'_3, \dots, \eta'_n$ , which differs from its corresponding  $\eta$ . Since  $\eta'_\alpha$  cannot be less than  $\eta_\alpha$ , we take  $\eta'_\alpha > \eta_\alpha$ . Now  $|a_{i,j}|$  must be prime to  $p$  (see proof of Theorem V). Hence at least one of the exponents  $a_{i1}, a_{i2}, \dots, a_{in}$  in every  $\beta_i$  must be prime to  $p$ . So we take  $a_{i\alpha}$  prime to  $p$ . As an element of  $G$ ,  $c_i$  can be expressed uniquely in the form  $P_{s_1}^{x_1}P_{s_2}^{x_2} \dots P_{s_n}^{x_n}P_{s_{n+1}}^{x_{n+1}} \dots$  (see Theorem VIII). In this expression each  $x_j$ ,  $j=1, \dots, n$ , is divisible by  $p$ , since no product  $P_{s_1}^{y_1}P_{s_2}^{y_2} \dots P_{s_n}^{y_n}$  can be in  $C$  unless each  $y_j$  is divisible by  $p$ . We can therefore express  $\beta_i$  in the form

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

From this we see that the order of  $\beta_i$  is at least equal to the order of  $P_{s_\alpha}$ , which is  $\eta'_\alpha$  (see Theorem VII). Consequently, for  $i > j$ ,  $a_{i,j}$  must be divisible by  $p^{\eta'_i - \eta_j}$ . Taking  $i = \alpha$ , we see that  $a_{\alpha 1}, a_{\alpha 2}, \dots, a_{\alpha \alpha}$  must be divisible by

$p^{\eta_1 - \eta_\alpha}, p^{\eta_2' - \eta_\alpha}, \dots, p^{\eta_{\alpha'} - \eta_\alpha}$  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  $P_{s_1}, P_{s_2}, \dots, P_{s_n}$  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  $P_1, P_2, \dots, P_r$  of a given  $U$ -basis for  $G$ .

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

$$(1) \quad R[P_1^{x_1} \dots P_r^{x_r}]$$

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

$$(2) \quad P_{ij} = P_1^{b_{1ij}}P_2^{b_{2ij}} \dots P_r^{b_{rij}},$$

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  $P_k^{-1}P_\alpha^{b_{\alpha ij}}P_kP_\alpha^{-b_{\alpha ij}}$ ,  $i, j, k = 1, 2, \dots, r$ , 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  $P_{x'} = P_1^{x'_1}P_2^{x'_2} \dots P_r^{x'_r}$ . For instance, the first step in this reduction is to bring  $P_xP_y$  into the form

$$P_1^{x_1+y_1} \dots P_r^{x_r+y_r} \prod_{i < j} P_{ij}^{\lambda_{ij}}$$

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  $\delta_{ij} \leq \delta_i, \delta_{ij} \leq \delta_j$ , 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  $\lambda_i$  is formally divisible by  $p^{\delta_i}, i = 1, 2, \dots, r$ . 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  $x'_i = x_i + y_i + f_i(x_1, \dots, x_r, y_1, \dots, y_r)$ ,  $i = 1, 2, \dots, r$ , 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

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

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

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

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

If each component  $x_i$  in the vector  $v_x = (x_1, x_2, \dots, x_r)$  is a least positive residue modulo  $p^{\delta_i}$ , 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 con-formal 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  $\left(\begin{smallmatrix} v \\ v v_y \end{smallmatrix}\right)$  of the  $p^m$  vectors. So we may regard (3) as defining a representation of  $G$  as a regular permutation group  $G_r$ .

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

$$\left(\begin{smallmatrix} v \\ v v_y \end{smallmatrix}\right) \sim \tau_y^{-1}.$$

---

\* 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  $B_1, B_2, \dots, B_n$  be  $n$  operations which satisfy the following conditions and no others:*

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

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

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

where the  $x_i$  and the  $x_{jk}, j < k$ , are least positive residues modulus  $p^{\eta_i}$  and  $p^{\eta_{jk}}$  respectively.† The symbol  $v_x$  has  $n + n(n-1)/2$  components (each component for which  $\eta_{jk}$  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  $p^{2\eta_i + \eta_{jk}}$  distinct values. We propose to show that the symbols  $v_x$  constitute a group of this order, under the law of multiplication given by  $v_w = v_x v_y$ , where the components of  $v_w$  are defined by

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

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.,  $v_0 v_x = v_x v_0 = v_x$ . By computation, we find that the components of  $(v_x)^\lambda$  are given by

$$(6) \quad x'_i = R_{p^{\eta_i}}(\lambda x_i), \quad i = 1, \dots, n; \quad x'_{jk} = R_{p^{\eta_{jk}}}\left(\lambda x_{jk} + \frac{\lambda(\lambda - 1)}{2} x_j x_k\right).$$

\* 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  $\eta_{ij}$  equals  $\eta_{ji}$ . 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  $n_x x_i \equiv 0 \pmod{p^{n_i}}$ ;  $n_x x_{jk} \equiv 0 \pmod{p^{n_{jk}}}$ . 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  $v_x = v_x^{-1} v_y v_x v_y^{-1}$ . Its components are given by

$$(7) \quad z_i = 0, \quad i = 1, 2, \dots, n; \quad z_{jk} = R_{p^{n_{jk}}}(x_j y_k - x_k y_j).$$

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

It remains to associate the symbols  $B_i$  and  $B_{jk}$  with the symbols  $v_x$ . We define  $v_i, i = 1, 2, \dots, n$ , 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  $p^{n_i}$ , while the order of each  $v_{jk}$  is  $p^{n_{jk}}$ . 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  $n, \eta_i, \eta_{jk}$  are no longer arbitrary, but represent respectively the number of I.G.O., the order of  $\beta_i$ , the order of  $c_{jk} (= \beta_j^{-1} \beta_k \beta_j \beta_k^{-1})$ , where  $\beta_1, \beta_2, \dots, \beta_n$  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

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

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

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

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

We state without proof two results, whose verification presents no difficulty: (a) the number of formally distinct representations of a given element  $\sigma$  of  $G$  in the form  $\beta_x$  equals the number of formally distinct representations of the identity of  $G$ ; (b) the operation  $\psi$  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  $\prod B_{ij}^{x_{ij}}$  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  $\eta_{jk}$  is zero shall not occur in  $\prod B_{ij}^{x_{ij}}$ .



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

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  $p^{\delta_l}$  where  $j, k, l, u, v$  range independently from 1 to  $r$ . From the equality

(5')  $A_{jk} = A_{kj}^{-1}$

we obtain

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

As a special case of (5) we have

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

which may be derived immediately from the fact that

(6')  $T_j$  is commutative with  $A_i$ ,  $i = 1, 2, \dots, r$ .

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

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

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

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

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  $\theta$  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  $\theta^{-a} A_i = A_i T_i$  ( $i = 1, 2, \dots, r$ ) 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  $A_1, \dots, A_r$  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  $A_1, \dots, A_r$  by  $p^{b_1}, \dots, p^{b_r}$  respectively.

We now define  $T_j, j=1, \dots, r$ , to be the substitution  $A_1 \rightarrow A_1', \dots, A_r \rightarrow A_r'$ , 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  $p^{b_k - b_i}$ . 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  $T_1, \dots, T_r$  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  $T_1, T_2, \dots, T_r$  generate an abelian group, and  $A$  is isomorphic with this abelian group under the correspondence defined by

$$(9) \quad A_i \sim T_i \quad (i = 1, 2, \dots, r).$$

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

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

constitute a group  $\bar{G}$  of order  $p^{2b_i}$ . That this group is metabelian follows from (4') and the fact that the commutator subgroup of  $\bar{G}$  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  $p^{b_k}$ . These matrices, together with the orders of  $A_1, \dots, A_r$ , 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



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

BROWN UNIVERSITY,  
PROVIDENCE, R.I.