CONCERNING UNIQUENESS-BASES OF FINITE GROUPS WITH APPLICATIONS TO p-GROUPS OF CLASS 2*

BY

CHARLES HOPKINS†

A *uniqueness-basis* (U-basis) of a finite group G has been defined as "an ordered set of elements $Q_1, Q_2, \cdots, Q_\rho$ such that every element of G can be expressed uniquely in the form $Q_1^{x_1}Q_2^{x_2}\cdots Q_\rho^{x_\rho}$, where each x_i is a least positive residue modulo the order of Q_i."‡ In the case of the abelian groups the notion of U-basis is of undisputed importance: the theorem that every finite abelian group A has a U-basis may fairly be regarded as the cornerstone of the theory of abelian groups.

In the case of most non-abelian groups, however, the concept of U-basis is of doubtful advantage, especially in the general form above. Of greater usefulness, naturally, would be a "simplest type" of U-basis for the group under consideration. But the problem of constructing a definition of a "normal form" which shall be significant for reasonably general categories—the non-abelian p-groups, say—is an exceedingly difficult one. We offer a tentative definition in the case of the regular p-groups§ (§§2–3), which have, in common with the abelian p-groups, the property that the orders of the elements in every U-basis constitute a set of invariants of the group. In §4 we shall show how a "normal" U-basis may be used in constructing for every regular p-group G of class 2 a simply-isomorphic representation by l-matrices§ —matrices whose coordinates are residue classes modulo certain powers of p. These representations of G are of interest in that they usually involve a much smaller number of rows than do the matrix-representations whose coordinates are in a field. (The l-matrices are by no means novel; they have long been used for representing automorphisms of abelian p-groups.) In §5 we shall discuss the representation by l-matrices of the group of isomorphisms of G, and in §§6–7 we shall describe, very briefly, a representation of G as a multiplicative group in a finite ring.

1. In this section we shall state—for the most part without proof—several theorems which afford a set of criteria for the existence of a U-basis in a finite group G.

* Presented to the Society, September 5, 1936; received by the editors June 19, 1936.

† Corinna Borden Keen Research Fellow of Brown University.

‡ P. Hall, Proceedings of the London Mathematical Society, (2), vol. 36 (1934), p. 90.

§ Defined in §3.

THEOREM I. *For the ordered set of elements* $Q_1, Q_2, \cdots, Q_\rho$ *to constitute a U-basis for G it is necessary and sufficient that* (a) *each element of G be representable in the form* $Q_1^{x_1}Q_2^{x_2}\cdots Q_\rho^{x_\rho}$; (b) *the product of the orders of* $Q_1, Q_2, \cdots, Q_\rho$ *equal the order of G.**

Let $P_1, P_2, \cdots, P_n$ denote n operations of G whose orders are $g_1, g_2, \cdots, g_n$ respectively. Let P_x and P_y denote the products $P_1^{x_1}P_2^{x_2}\cdots P_n^{x_n}$ and $P_1^{y_1}P_2^{y_2}\cdots P_n^{y_n}$ respectively, $0 \leqq x_i < g_i$, $0 \leqq y_i < g_i$. We shall say that P_x and P_y are *formally distinct* if at least one x_k is not equal to y_k; we shall call them *effectively distinct* if they do not represent the same operation of G.

THEOREM II. *For the ordered set of elements* $P_1, P_2, \cdots, P_n$ *to constitute a U-basis for G it is necessary and sufficient that* (a) *the product* $g_1g_2\cdots g_n$ *equal the order of G*; (b) *any two formally distinct products* P_x *and* P_y *be effectively distinct.*

The following result is often useful:

THEOREM III. *If a finite group G, of order g, contains a set of subgroups* $G = G_1 \supset G_2 \supset \cdots \supset G_m$, *each* G_{i+1} *being a proper subgroup of index* g_i *in* G_i, *and if*

(a) G_m *contains a U-basis* $Q_1, Q_2, \cdots, Q_n$;

(b) $G_i - G_{i+1}$, $i = 1, 2, \cdots, m-1$, *contains an element* P_i *of order* g_i *such that* $P_i^{g_i}$ *is the lowest power of* P_i *which is in* G_{i+1}; *then the ordered set of elements* $P_1, P_2, \cdots, P_{m-1}, Q_1, \cdots, Q_n$ (*and* $Q_1, \cdots, Q_n, P_{m-1}, \cdots, P_2, P_1$ *as well*) *constitute a U-basis for G.*

By writing G_{m-1} in cosets with respect to G_m,

$$G_{m-1} = G_m + P_{m-1}G_m + \cdots + P_{m-1}^{g_{m-1}-1}G_m,$$

we see from Theorem I that $P_{m-1}, Q_1, \cdots, Q_n$ form a U-basis for G_{m-1}. The proof may be completed by induction.

THEOREM IV. *If a group G of order g contains two subgroups* H_1 *and* H_2, *of orders* h_1 *and* h_2 *respectively*; *and if*

(a) $h_1h_2 = g$;

(b) *the cross-cut* $H_1 \wedge H_2$ *is the identity*;

(c) H_1 *and* H_2 *contain the U-bases* $P_1, \cdots, P_\rho$ *and* $Q_1, \cdots, Q_\sigma$, *respectively*; *then the ordered set of elements* $P_1, \cdots, P_\rho, Q_1, \cdots, Q_\sigma$ (*or* $Q_1, \cdots, Q_\sigma, P_1, \cdots, P_\rho$) *constitute a U-basis for G.*

This theorem is easily proved by writing G in cosets with respect to H_1 (or H_2) and applying Theorem I.

* This rather obvious condition is mentioned by Hall for the case of a regular p-group; loc. cit., p. 95.

THEOREM V. *If G is the direct product of the subgroups $G_1, G_2, \cdots, G_m$, and if each subgroup G_i has the U-basis $Q_{i1}, \cdots, Q_{in_i}$, then a U-basis for G is given by the ordered set $Q_{11}, \cdots, Q_{1n_1}, Q_{21}, \cdots, Q_{2n_2}, \cdots$, etc.*

The wording of the theorem obviously implies that in this ordered arrangement the sets $(Q_{i1}, \cdots, Q_{in_i})$ may be permuted at will, provided that the sequence of the elements within the sets is undisturbed. For $m=2$ this theorem is a corollary of Theorem IV; by induction it can be proved for any m.

We conclude this section by giving several examples of groups which have uniqueness-bases.

A. *All dihedral groups.* For the dihedral group of order $2m$ (which is generated by two operations P and Q which satisfy the relations $P^2=Q^m=E$, $QP=PQ^{-1}$) the ordered set P, Q (and Q, P, as well) constitute a U-basis.

B. *Every symmetric group.* By Theorem III we may prove that the ordered set of cycles $a_1a_2, a_1a_2a_3, \cdots, a_1a_2 \cdots a_n$ constitute a U-basis for the symmetric group of degree n.

C. *Every alternating group $\mathcal{A}_n$.* The theorem is obvious for the alternating groups of degrees 2 and 3. We outline a proof by induction, assuming that the alternating group $\mathcal{A}_{n-1}$ of degree $n-1$ has a U-basis. There are three cases to consider: (a) when n is odd; (b) when n is divisible by 4; (c) when n is divisible by 2 and not by 4. In case (a) we know that $\mathcal{A}_n-\mathcal{A}_{n-1}$ contains the cycle $a_1a_2 \cdots a_n$. In case (b) it is easy to see that $\mathcal{A}_n$ contains the dihedral group of order n as a regular permutation group. In either case (a) or case (b), then, the proof may be completed by using Theorem IV. For case (c) we select from $\mathcal{A}_n$ the two permutations $s=(a_1a_n)(a_2a_3)$ and $t=(a_1a_2 \cdots a_{n/2})(a_{n/2+1} \cdots a_n)$. Now case (c) cannot arise for $n<6$, and it is easy to see that when $n \geqq 6$ all formally distinct products $t^x s^y$ are effectively distinct, $0 \leqq x < n/2$; $0 \leqq y \leqq 1$; except for $x=0$ and $y=0$ the product $t^x s^y$ will permute the letter a_n, and hence will not be a permutation in $\mathcal{A}_{n-1}$. One may now complete the proof by using Theorem II and the induction-hypothesis.

D. *The Sylow p-group $\sum_{p,n}$ of the general n-ary linear homogeneous group modulo p.* It is well known that $\sum_{p,n}$ can be represented by the group of matrices

$$(\alpha_{ij}) = \begin{pmatrix} 1 & a_{12} & \cdots & a_{1n} \\ 0 & 1 & \cdots & a_{2n} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ 0 & 0 & \cdots & 1 \end{pmatrix},$$

where the $n(n-1)/2$ coordinates a_{ij} above the main diagonal are arbitrary elements of the Galois field of p elements. If we put $a_{in}=0, i=1, 2, \cdots, n-1$,

we obtain a representation of $\sum_{p,n-1}$; this group has only the identity in common with the abelian group defined by $a_{ij}=0$, $j\neq n$. By using Theorem IV and induction over n we may show that a U-basis for the group (α_{ij}) is given by the ordered set

$$E+e_{12}, E+e_{13}, E+e_{23}, E+e_{14}, \cdots, E+e_{1n}, E+e_{2n}, \cdots, E+e_{n-1,n},$$

where E is the n-rowed identity matrix and the e_{ij} are the usual basis-units of the n-ary matrix ring.

In conclusion, we offer the quaternion group as the simplest example of a group which has no U-basis.

2. In this section we introduce the notion of a *normal* U-basis. A U-basis $Q_1, Q_2, \cdots, Q_\rho$ of a finite group G is said to be *normal* with respect to G (in short, a *normal* U-basis) if for $i<j$; $i=1, 2, \cdots, \rho$; $j=2, 3, \cdots, \rho$, the elements Q_α satisfy the $\rho(\rho-1)/2$ equations

$$Q_jQ_i = Q_iQ_j^{\beta_{jij}}Q_{j+1}^{\beta_{jij+1}}\cdots Q_\rho^{\beta_{ji\rho}}.* \tag{1}$$

As examples of groups having a normal U-basis we mention the dihedral groups and the groups $\sum_{p,n}$ above. Groups which contain a normal U-basis evidently constitute an exceptional category, as the restrictions imposed by the definition are relatively strong; for instance, each subgroup $\{Q_j, Q_{j+1}, \cdots, Q_\rho\}$ must be invariant in G, and G must be solvable.

An advantageous property of a normal U-basis is the following:

THEOREM I. *If a finite group G has a normal U-basis $Q_1, \cdots, Q_\rho$, the order of Q_i being g_i, then G is completely defined by the equations*

$$Q_i^{g_i} = E \tag{2}$$

and the permutability relations (1) *above.*

Let $P_1, P_2, \cdots, P_\rho$ be a set of operations; i.e., elements which generate some group, and suppose that these elements are defined by equations (1) and (2) (assuming, of course, that we replace Q_i by P_i). Let $\overline{G}$ denote the group generated by $P_1, \cdots, P_\rho$. Since $\overline{G}$ and G are homomorphic under the correspondence defined by $P_i\sim Q_i$,† our theorem will follow if we can show that G and $\overline{G}$ have the same order; that is, if we can show that every product $\Pi=P_\alpha^{\nu_\alpha}P_\beta^{\nu_\beta}\cdots P_\alpha^{z_\alpha}\cdots$ of powers of $P_1, P_2, \cdots, P_\rho$ can be brought into the normal form $P_x=P_1^{x_1}P_2^{x_2}\cdots P_\rho^{x_\rho}$ by a finite number of reductions, each

---

* These equations define the commutators $(Q_j, Q_i), i<j$. From Theorem I below and the equation $(Q_i, Q_j)=(Q_j, Q_i)^{-1}$ it follows that (Q_i, Q_j) must have the form $Q_j^{\xi_{iij}}\cdots Q_\rho^{\xi_{ji\rho}}$.

† Burnside, *Theory of Groups of Finite Order*, 2d ed., p. 374.

reduction consisting of an interchange of two adjacent P's, using (1), followed by a reduction of exponents by means of (2). This is obviously possible when Π contains only $P_{\rho-1}$ and P_ρ as factors. The proof may be completed by induction: it is not difficult to show that a product Π involving no subscripts less than k can be brought into the normal form by a finite number of reductions, provided that this is true for all products containing subscripts greater than k.

Later we shall need the following generalization of the term "normal U-basis." Let G be a finite group and let Ψ be a group in which each element is an operator of G; suppose, further, that Ψ contains operators* which effect each of the inner isomorphisms of G. A U-basis $P_1, P_2, \cdots, P_\rho$ of G is said to be *normal with respect to* Ψ provided that

$$P_i\psi = P_i^{\beta_{i\psi}} P_{i+1}^{\beta_{i+1\psi}} \cdots P_\rho^{\beta_{\rho\psi}}, \qquad i = 1, 2, \cdots, \rho, \tag{3}$$

where ψ is a variable operator in Ψ.

If for Ψ we take the group G itself, then this definition is equivalent to our earlier definition of a U-basis normal with respect to G. For in this case equations (3) contain the $\rho(\rho-1)/2$ equations

$$P_i^{-1} P_j P_i = P_j^{\beta_{ji}} \cdots P_\rho^{\beta_{j\rho}}, \qquad i < j. \tag{4}$$

THEOREM II. *If Ψ is of order p^l and if every element of G satisfies the equation $s^p = E$, then G contains a U-basis normal with respect to Ψ.*

By taking $\Psi \equiv G$ we have, as a corollary,

THEOREM III. *A finite p-group whose elements are of order p (identity excepted) contains a normal U-basis.*

In connection with Theorem III we observe that each exponent β_{ji} in (4) must be 1 modulo p; otherwise, the number of conjugates of P_j under P_i would contain a factor prime to p. Obviously Theorem III is not valid for p-groups in general.

Proof of Theorem II. We write s' for $s\psi$, where s and ψ are any elements of G and Ψ respectively. Let G_1 denote the subgroup of G which is generated by the totality of elements $c_1 = s^{-1}s'$. We define inductively the subgroup G_{i+1}. Suppose that G_i has already been defined, and suppose that c_i represents any element of G_i. Let c_i' and c_{i+1} denote $c_i\psi$ and $c_i^{-1}c_i'$ respectively, where ψ is any operator of Ψ. Then G_{i+1} is defined as the group generated by the totality of elements c_{i+1}.

* For a treatment of groups with operators see van der Waerden, *Moderne Algebra*, vol. I, p. 132. As concerns its effect on G, each operator ψ is equivalent to an operation T in the holomorph of G ($P_i\psi$ and $T^{-1}P_iT$ are the same element of G). It is hardly necessary to point out that Ψ need not be simply isomorphic with a subgroup of the holomorph of G.

Since each ψ effects a p-automorphism of G, we know that there is associated with a fixed operator ψ_λ a series of subgroups $G \supset G' \supset G'' \supset \cdots \supset E$, each of index p in the preceding one, such that $s^{(\alpha)}\psi$, $s^{(\alpha)}$ being any element of $G^{(\alpha)}$, is equal to $s^{(\alpha)}$ multiplied by an element from $G^{(\alpha+1)}$.* From this we see at once that G_{i+1} is a proper subgroup of G_i, $i=1, 2, \cdots$; consequently, the series $G=G_0 \supset G_1 \supset G_2 \supset \cdots$ must terminate in the identity E. Suppose that $G_f \equiv E$, but $G_{f-1} \not\equiv E$. We shall say that G is of class f with respect to Ψ. (By hypothesis, Ψ contains operators which bring about each of the inner isomorphisms of G. Hence G_1 contains the commutator subgroup of G. And if Ψ is G itself, then our definition of class coincides with the usual one.)

Now the group G_{f-1} of order p^{n_f-1}, say, is abelian and of type $1, 1, \cdots, 1$. For G_{f-1} we can construct a U-basis $P_{f-1,1}, P_{f-1,2}, \cdots$, and this U-basis will be normal with respect to Ψ, since every element of G_{f-1} satisfies the equation $c\psi = c$.†

If G is of class 1 with respect to Ψ, then our construction is at an end. Otherwise, we proceed by induction over G_i. Suppose that for G_{k+1} we have already constructed a U-basis normal with respect to Ψ. Now each quotient-group G_i/G_{i+1}, of order p^{n_i}, is abelian and of type $1, 1, \cdots, 1$. Hence we may construct for G_k/G_{k+1} a U-basis $u_1, u_2, \cdots, u_{n_k}$. From each of those cosets of G_k (with respect to G_{k+1}) which correspond to $u_1, u_2, \cdots$ we select an element as a representative, obtaining thereby n_k elements $P_{k\lambda}$, $\lambda = 1, 2, \cdots, n_k$. The ordered set $P_{k1}, \cdots, P_{kn_k}$ followed by the elements of the U-basis for G_{k+1} (in the proper sequence) will constitute a U-basis for G_k which is normal with respect to Ψ. This assertion can readily be proved by using Theorem I of §1, together with the fact that the order of G_k is P^{r_k}, where r_k equals $\sum_{\alpha=k}^{f-1} n_\alpha$.

The construction which we have just given leads to a U-basis containing exactly m elements, where p^m is the order of G. It may be pointed out that every U-basis of G, normal or not, must contain exactly m elements. This follows from two considerations: every finite group whose elements are of order p, identity excepted, is a regular p-group;‡ the number of elements in a U-basis for a regular p-group is an invariant of the group.

3. In the introduction we mentioned an important category of p-groups, which resemble the abelian p-groups in that any two U-bases have the same number of elements of a given order. These are the regular p-groups, which have been defined in the following way:§ the p-group G will be called *regular*

* Miller, Blichfeldt, and Dickson, *Finite Groups*, p. 136.

† The proof of Theorem II depends mainly upon familiar properties of abelian groups A of order p^m and type $1, 1, \cdots, 1$: A has a U-basis, and the number of elements in every U-basis is exactly m.

‡ Hall, loc. cit., p. 74.

§ Hall, loc. cit., p. 73.

if, given any positive integer α and a pair of elements P and Q of G, it is always possible to find elements $S_3, S_4, \cdots, S_\rho$ all belonging to the commutator subgroup of $\{P, Q\}$ and satisfying the equation $(PQ)^{p^\alpha} = P^{p^\alpha} Q^{p^\alpha} S_3^{p^\alpha} S_4^{p^\alpha} \cdots S_\rho^{p^\alpha}$.

For an understanding of what follows, one must keep well in mind certain definitive properties of a regular p-group:

(a) The p^αth powers of the elements of G constitute a characteristic subgroup $\mathfrak{V}_\alpha(G)$.

(b) Those elements in G whose orders divide p^β constitute a characteristic subgroup $\Omega_\beta(G)$.

(c) The group G is conformal with an abelian group A.

(d) The orders of the elements in any U-basis of G are the same as the invariants $p^{\epsilon_1}, p^{\epsilon_2}, \cdots, p^{\epsilon_r}$ of A. (These orders have been called the *type-invariants* of G.)

(e) If Q_x is an element $Q_1^{x_1} Q_2^{x_2} \cdots Q_r^{x_r}$, written in the normal form with respect to the U-basis $Q_1, Q_2, \cdots, Q_r$, then the order of Q_x is equal to the order of its constituent $Q_\lambda^{x_\lambda}$, of highest order.

(f) If P and Q are any two elements of G, then the order of every element in the commutator subgroup of $\{P, Q\}$ divides the order of P (and of Q) relative to the central of G.

From (a) and (b) it is clear that G contains two series of characteristic subgroups: $G = \mathfrak{V}_0 \supset \mathfrak{V}_1 \supset \cdots \supset \mathfrak{V}_\delta = E$; $E = \Omega_0 \subset \Omega_1 \subset \cdots \subset \Omega_\delta = E$, where p^δ is the order of an element of highest order in G. From (c) it follows that δ is equal to the largest one of the ϵ's in (d).

(g) The order p^{ω_α} of $\Omega_\alpha / \Omega_{\alpha-1}$ equals the order of $\mathfrak{V}_{\alpha-1}/\mathfrak{V}_\alpha$, $\alpha = 1, 2, \cdots, \delta$. In particular, $G/\mathfrak{V}_1$ is of order ω_1. The ω's satisfy the inequalities $\omega_1 \geqq \omega_2 \geqq \cdots \geqq \omega_\delta$. Furthermore, ω_1 equals r, the number of type-invariants of G.

(h) For the ϵ's and ω's we have the relation $\sum_{i=1}^{r} \epsilon_i = \sum_{j=1}^{r} \omega_j = m$, where p^m is the order of G (and of A).

(i) $\mathfrak{V}_\alpha(G)$ and $\Omega_\beta(G)$ are conformal with $\mathfrak{V}_\alpha(A)$ and $\Omega_\beta(A)$ respectively, $\alpha, \beta = 0, 1, \cdots, \delta$.

Let $V_i(G)$ denote the cross-cut $\mathfrak{V}_1(G) \wedge \Omega_i(G)$, $i = 0, 1, \cdots, \delta$, and let $W_i(G)$ denote the group $\{V_i(G), \Omega_{i-1}(G)\}$.

(j) The groups $V_i(G)$, $W_i(G)$, $\Omega_i(G)/V_i(G)$, and $\Omega_i(G)/W_i(G)$ are conformal respectively with the groups which are obtained by replacing G with A.

(k) If the exponents of the invariants of A, arranged in descending order of magnitude, are given by $\delta_1 \geqq \delta_2 \geqq \cdots \geqq \delta_r$, and if in this arrangement the δ's constitute s sets, the jth set consisting of h_j equal δ's having the common

value e_i, then the order of $\Omega e_j(A)/We_j(A)$ is p^{h_j}. Obviously $m=\sum_{i=1}^{r}\delta_i$ $=\sum_{j=1}^{s}h_je_j$.

Items (a) through (i) are given explicitly in the paper of Hall to which reference has already been made (see pp. 73–81); item (j) is contained implicitly in Hall's results; item (k) is a familiar result from the theory of abelian p-groups.

DEFINITION. *A U-basis $P_1, P_2, \cdots, P_r$ for a regular p-group G, the order of P_i being p^{δ_i}, is said to be ω-normal provided that*

(1) $\delta_1 \geqq \delta_2 \geqq \cdots \geqq \delta_r$;

(2) *when (P_j, P_i),* $i<j$, is expressed in the normal form*

$$(P_j, P_i) = P_1^{\alpha_{ji1}} P_2^{\alpha_{ji2}} \cdots P_r^{\alpha_{jir}}, \qquad i = 1, 2, \cdots, r; j = 2, 3, \cdots, r,$$

each α_{jik} is divisible by p for $k \leqq j$.

We state without proof two implications of this definition:

(3) for $k<j$, $\alpha_{jik} \equiv 0 \bmod p^{\delta_k-\delta_i}$ (see (e) and (f));

(4) if the normal form of (P_i, P_j), $i<j$, is given by $P_1^{\alpha_{ij1}} \cdots P_r^{\alpha_{ijr}}$, then the highest power of p that divides α_{iik} also divides α_{jik}, and conversely. Moreover, (2) is clearly a consequence of (1) when no two of the δ's are equal.

For the abelian group A conformal with G any U-basis for which (1) is satisfied may be regarded as a "normal form," since all such U-bases are equivalent under the holomorph of A. In defining a normal form for a U-basis of G we must obviously demand more, and (2) seems to be the most natural additional requirement which can be satisfied in the case of every regular p-group. The qualifying phrase "ω-normal" is suggested by the fact that $P_1, P_2, \cdots, P_r$, regarded as representatives of a U-basis for $G/\mathfrak{V}_1$, constitute a *normal* U-basis for this quotient group; i.e.,

$$P_jP_i \equiv P_iP_jP_{j+1}^{\alpha_{iij+1}} \cdots P_r^{\alpha_{jir}} \bmod \mathfrak{V}_1.$$

As an attempt at defining a normal form for a U-basis, our definition above is obviously of no value unless we can prove the following theorem:

Every regular p-group G contains an ω-normal U-basis.

First, we explain a method for constructing a set of elements which satisfy requirements (1) and (2) above. To avoid repeated explanations, the symbols G, $\Omega(\ )$, m, h_j, e_j, etc., will have the same significance as in (a) through (k) above.

---

* This is the familiar notation for the commutator $P_j^{-1}P_i^{-1}P_jP_i$.

Let $\Omega_a(G)$ be the first term in the series $E=\Omega_0 \subset \Omega_1 \subset \cdots \subset \Omega_s=G$ for which W_a is a proper subgroup of Ω_a; i.e.,

$$W_j \equiv \Omega_j, \quad j = 0, 1, \cdots, a-1; \qquad W_a \subset \Omega_a. \tag{5}$$

From (j) and (k) we see that the order of Ω_a/W_a is exactly p^{h_a}. Furthermore, every element of this quotient-group is of order p, except for the identity. Since Ω_a and W_a are characteristic subgroups of G, and since each element of G effects an automorphism of Ω_a/W_a, we can construct for this quotient-group a U-basis, $u_1, u_2, \cdots, u_{h_a}$, say, which is normal with respect to G (see Theorem II of §2). From the coset of Ω_a which corresponds to u_j we select any element Q_j as a representative, obtaining thereby the h_a elements $Q_1, Q_2, \cdots, Q_{h_a}$.

(6) Each $Q_j, j=1, 2, \cdots, h_a$, is of order p^a.

Otherwise, contrary to (5), we could find a $k<a$ for which $W_k \not\equiv \Omega_k$.

It is easy to see that every element of Ω_a can be expressed in the form $Q_1^{x_1}Q_2^{x_2}\cdots Q_{h_a}^{x_{h_a}}w_{a,x}$, where $w_{a,x}$ is an element in W_a. And since the Q_j's are representatives of a U-basis for Ω_a/W_a which is normal with respect to G, it is clear that for a variable element X in G we have the congruences

$$X^{-1}Q_jX \equiv Q_jQ_{j+1}^{\xi_{j+1}}\cdots Q_{h_a}^{\xi_{h_a}} \bmod W_a, \qquad j = 1, 2, \cdots, h_a. \tag{7}$$

From (i), (j), and (k) we also have the equality

$$a = e_a. \tag{8}$$

If Ω_a is G itself, then our construction is at an end. If not, let Ω_b be the first term in the series $\Omega_{a+1}, \Omega_{a+2}, \cdots$ for which

$$W_b \subset \Omega_b; \; W_{a+l} \equiv \Omega_{a+l}, \qquad l = 0, 1, \cdots, b-a-1. \tag{9}$$

As above, we construct for Ω_b/W_b, which is necessarily of order $p^{h_{a-1}}$, a U-basis normal with respect to G, and from each coset of Ω_b which corresponds to one of these basis-elements we choose an element, obtaining the h_{a-1} elements $R_1, R_2, \cdots, R_{h_{a-1}}$.

(10) Each of the R's is of order p^b.

Suppose that one of them, R_λ, say, were of order less than p^b. Then R_λ would necessarily occur among the elements of a certain set $\Omega_k - W_k$ where $k<b$. From (5) and (9) we know that a is the only value of $k<b$ for which $W_k \subset \Omega_k$. And certainly R_λ cannot be an element in $\{\mathfrak{v}_1, \Omega_a\}$, since Ω_a is contained in W_b. As in (8) above, we have the equality $b=e_{a-1}$.

From the manner of their construction it follows that the R's satisfy congruences of the type

$$(11) \qquad X^{-1}R_iX = R_iR_{i+1}^{\xi_{i+1}} \cdots R_{h_{s-1}}^{\xi_{h_{s-1}}} \bmod W_b, \qquad i = 1, 2, \cdots, h_{s-1},$$

when X is any element of G.

Since W_b is a subgroup of $\{\mathfrak{V}_1, \Omega_a\}$, we may replace (11) by

$$(12) \qquad X^{-1}R_iX \equiv R_iR_{i+1}^{\xi_{i+1}} \cdots R_{h_{s-1}}^{\xi_{h_{s-1}}}Q_1^{\eta_1} \cdots Q_{h_s}^{\eta_{h_s}} \bmod \mathfrak{V}_1.$$

If Ω_b is not equal to G, then we continue the construction; and at this point it is reasonably clear how the construction advances. The final (the sth) stage will consist of selecting h_1 elements $P_1, P_2, \cdots, P_h$ of $\Omega_\delta \geqq G$ which correspond to a U-basis of G/W_s, this U-basis being, of course, normal with respect to G. Thus we obtain an ordered set of $r = \sum_{i=1}^{s} h_i$ elements

$$(13) \qquad P_{11}, P_{12}, \cdots, P_{1h_1}, P_{21}, \cdots, P_{s-11}, \cdots, P_{s1}, \cdots, P_{sh_s},$$

where $P_{s-1\,i}$ and P_{sj} denote the elements R_i and Q_j above.

For our purpose the significant properties of these elements are the two following: $\delta_1 \geqq \delta_2 \geqq \cdots \geqq \delta_r$, and

$$(14) \qquad X^{-1}P_jX \equiv P_jP_{j+1}^{\xi_{j+1}} \cdots P_r^{\xi_r} \bmod \mathfrak{V}_1(G), \qquad j = 1, 2, \cdots, r.$$

(For the sake of a simpler notation we have replaced P_{11} by P_1, P_{12} by P_2, $\cdots$, P_{sh_s} by P_r.) It is clear, therefore, that if the elements $P_1, P_2, \cdots, P_r$ form a U-basis for G, then this U-basis will be ω-normal.

To prove that $P_1, P_2, \cdots, P_r$ constitute a U-basis, it is sufficient to show that they form a canonical basis for G, since it is known that every canonical basis of a regular p-group is necessarily a U-basis.*

A canonical-basis of a regular p-group has been defined* as a set of $\omega(=\omega_1)$ elements $Q_1, Q_2, \cdots, Q_\omega$ (ω being the order of $G/\mathfrak{V}_1(G)$) which satisfy the following conditions:

(α) there exists a set of ω subgroups $G = K_1 \supset K_2 \supset \cdots \supset K_\omega \supset K_{\omega+1} = \mathfrak{V}_1$, each being invariant in G and a proper subgroup of the preceding, such that each of the ω sets $K_i - K_{i+1}$ contains exactly one of the Q_i's;

(β) the product of the orders of the Q_i's is as small as possible, consistent with (α).

It is known that

(γ) the product of the orders of the elements in and canonical basis must equal the order of G.†

To show that the elements $P_1, \cdots, P_r$ above form a canonical-basis, it is therefore sufficient to show that they satisfy requirements (α) and (γ).

* Hall, loc. cit., p. 91.

† Hall, loc. cit., p. 92.

Now (γ) is satisfied, since the elements (13) constitute s sets, the jth set containing h_j elements each of order p^{e_j} [see (k) and (8) above].

To prove that (α) is also satisfied, we observe from (14) that the group $F_i=\{P_i, P_{i+1}, \cdots, P_r, \mathfrak{V}_1\}$ is an invariant subgroup of G; moreover F_i is a proper subgroup of index p in F_{i-1}, and r is equal to ω. Hence the series $G=F_1 \supset F_2 \supset \cdots \supset F_r \supset \mathfrak{V}_1$ has the properties of the K-series in (α); and since F_i-F_{i+1} contains P_i and no other one of the P's, it follows that requirement (α) is satisfied by the r elements $P_1, P_2, \cdots, P_r$.

Whenever an ω-normal U-basis is normal with respect to G, that is, whenever the congruences $(P_j,P_i)\equiv P_{i+1}^{\beta_{ji i+1}} \cdots P_r^{\beta_{jir}} \bmod \mathfrak{V}_1$, $i<j$, can be replaced by equalities

$$(P_j,P_i)=P_{i+1}^{\lambda_{ji i+1}} \cdots P_r^{\lambda_{jir}}, \tag{15}$$

then, from Theorem I of §2, we know that G is completely defined by the orders $p^{\delta_1}, \cdots, p^{\delta_r}$ and the exponents in (15). The existence of a G-normal U-basis is clearly exceptional and it is an open question whether the data provided by an ω-normal U-basis, namely, the orders of the elements and the $r(r-1)/2$ equations (2), are always sufficient to define the regular p-group from which they are derived.

A Note on l-Matrices.* Let (ξ_{ij}) be an r-rowed square matrix whose coordinates are arbitrary rational integers, and let $\delta_1, \delta_2, \cdots, \delta_r$ be a sequence of fixed positive integers satisfying the inequalities $\delta_1 \geqq \delta_2 \geqq \cdots \geqq \delta_r$. The l-matrix (x_{ij}) we shall define as the matrix formed by replacing each ξ_{ij} by the set of integers having the form $\xi_{ij} \pm \lambda_{ij} p^{\delta_j}$; that is, (x_{ij}) is the matrix whose jth column is composed of residue classes $[\xi_{ij}]$ modulo p^{δ_j}. The class $[\xi_{ij}]$ is characterized by the least positive residue of ξ_{ij} modulo p^{δ_j}; accordingly, we shall usually assume that the coordinate x_{ij} in the l-matrix (x_{ij}) is a least positive residue rather than a class $[\xi_{ij}]$. Two l-matrices are naturally to be regarded as distinct unless their corresponding coordinates are identical. The totality of distinct l-matrices constitute a set, which we shall designate by the expression $L_p(\delta_1, \delta_2, \cdots, \delta_r)$. The sum of two l-matrices (x_{ij}) and (y_{ij}) we shall define as the l-matrix (z_{ij}) for which z_{ij} is the least positive residue of $x_{ij}+y_{ij}$ modulo $p^{\delta_j}, j=1, 2, \cdots, r$; the product $(x_{ij})(y_{ij})$ is the l-matrix (w_{ij}) in which w_{ij} is the least positive residue of $\sum_{\alpha=1}^{r} x_{i\alpha} y_{\alpha j}$ modulo p^{δ_j}. Those l-matrices for which the conditions

(α) $x_{ij} \equiv 0 \bmod p^{\delta_j-\delta_i}, i>j,$

and

(β) $|x_{ij}| \not\equiv 0 \bmod p$

* These l-matrices were first defined, in a slightly different form, by A. Ranum, these Transactions, vol. 8 (1907), pp. 71–91.

hold constitute under multiplication a group, which we shall refer to as "the group of l-matrices."* This group, which we shall denote by the expression $GL_p(\delta_1, \delta_2, \cdots, \delta_r)$, is simply isomorphic with the group of isomorphisms of the abelian p-group of type $\delta_1, \delta_2, \cdots, \delta_r$.*

Multiplication is not, in general, associative for any three matrices of the set $L_p(\delta_1, \cdots, \delta_r)$. For l-matrices (x_{ij}) which satisfy (α), however, multiplication is associative and distributive, and these l-matrices constitute a ring. Thus any expression $(a(x_{ij})+b(y_{ij})+\cdots)^n(c(u_{ij})+d(v_{ij})+\cdots)^m\cdots$, where a, b, m, n are positive integers, defines a unique l-matrix, and this consideration is the justification for our later notation. In particular, the l-matrix defined by the expression $a(x_{ij})$, where (x_{ij}) satisfies condition (α), may be regardod as $(x_{ij})+(x_{ij})+\cdots+(x_{ij})$, where there are a terms, as $(\alpha_{ij})(x_{ij})$, or as $(x_{ij})(\alpha_{ij})$, where (α_{ij}) is the l-matrix whose diagonal elements are the least positive residues of a modulis p^{δ_1}, p^{δ_2}, $\cdots$, etc., the remaining elements being zeros.

4. This section is concerned with applying the data furnished by an ω-normal U-basis to the problem of constructing a one-to-one representation by l-matrices† for a special category of regular p-groups; that is, the regular p-groups of class 2.‡ The theory of representations of a group of order g by means of matrices with coefficients in a field of characteristic prime to g has been rather thoroughly exploited. Little is known, however, about representations of p-groups by matrices with coefficients in a field of characteristic p; and it is fair to say that the problem of representing a *given* p-group by l-matrices has received almost no attention.§

Since the group $GL_p(\delta_1, \cdots, \delta_r)$—the group of l-matrices—is simply isomorphic with the group of automorphisms of the abelian p-group of type $\delta_1, \delta_2, \cdots, \delta_r$, we can easily construct a representation of a p-group G_p if we can find an abelian p-group A_p which is transformed into itself by G_p. Thus we can always construct a multiply-isomorphic representation by l-matrices for any p-group G_p, whether regular or not, since G_p always contains invariant abelian subgroups. The real difficulty arises when we demand a 1–1 representation of G_p (that is, a representation which is simply isomorphic with G_p).

* Ranum, pp. 84–85.

† These l-matrices are defined in §3.

‡ Groups of class 2 (metabelian groups, in the terminology of American mathematicians) were originally defined as groups having abelian central quotient-groups (W. B. Fite, Proceedings of the American Association for the Advancement of Science, vol. 49 (1901), p. 41). They have also been defined as groups having abelian commutator subgroups. The two definitions are obviously equivalent.

§ The reciprocal problem, namely, the investigation of the subgroups of the group $GL_p(\delta_1,\delta_2, \cdots, \delta_r)$ has been widely discussed.

It is precisely these 1–1 representations which are of most interest, and in the case of regular p-groups of class 2 a method for constructing them may be developed from the theory of regular permutation groups.

Let G be a regular p-group of class 2 and of order p^m, $p>2$,* which is represented as a regular† permutation group on its p^m elements. Let $K(G)$ denote the holomorph of G, and let H denote that representation in $K(G)$ of the group of inner isomorphisms of G whose permutations omit the symbol for the identity of G. Let $s_1, s_2, \cdots, s_{p^m}$ denote the permutations of G, and let S_i denote that permutation of H which transforms G according to s_i. Since G is of class 2, its commutator subgroup $C(G)$ is contained in its central $\Gamma(G)$; furthermore, H is abelian, since it is simply isomorphic with G/Γ. From this we see that G is multiply isomorphic with H under the correspondence defined by $s_i \sim S_i^\lambda$, $i=1, 2, \cdots, p^m$, where λ is any fixed integer.

At this point we introduce several useful formulas, which one may readily verify:

(1) $(s_i, s_j) = (s_i^{-1}, s_j^{-1}) = (s_j^{-1}, s_i) = (s_j, s_i^{-1}) = (s_j, s_i)^{-1}$,

(2) $(s_i^x, s_j^y) = (s_i, s_j)^{xy}$,

(3) $(s_i, s_j) = (S_i, s_j) = (s_i, S_j)$; $(S_i, S_j) = E$.

Let p^μ be the order of the element of highest order in H. Since p is an odd prime $(p^\mu-1)/2$ is a positive integer; and we denote this integer by the letter a.

We shall need the following results:‡

(4) The p^m products $S_i^a s_i$ constitute a regular permutation group G_a which is abelian and conformal with G.

(5) The cross-cut $G \wedge G_a$ is the permutation group Γ.

(6) The group G_a is transformed into itself by G, and conversely.

Let $K(G_a)$ denote the holomorph of G_a, written as a permutation group on the letters of G, and let $I(G_a)$ be that representation in $K(G_a)$ of the group of isomorphisms of G_a which omits the symbol for the identity of G. Correspondingly, we define $I(G)$ as that representation in $K(G)$ of the group of isomorphisms of G which omits the symbol for the identity of G.

(7) The permutation group $I(G)$ is a subgroup of $I(G_a)$.

(8) Between the permutations $t_1, t_2, \cdots$ of G_a and those of G there is a

* The assumption $p>2$ is pertinent, since a group of order 2^m is regular only when it is abelian.

† The simultaneous occurrence of "regular" in two distinct and unrelated meanings is unfortunate; both usages, however, are already established in the literature. To avoid confusing repetitions of the adjective "regular", we agree that throughout the remainder of this section the symbol G shall be used precisely in the sense above.

‡ These Transactions, vol. 37 (1935), pp. 163-171. This paper will be referred to as H.

1–1 correspondence, which is defined by the equations $t_i = S_i^a s_i$ and $s_i = S_i^{-a} t_i$.

When, in the future, we speak of an element of G (or of G_a) as the "corresponding element" of an element in G_a (or in G), we shall have in mind the correspondence defined by the equations in (8).

Let $P_1, P_2, \cdots, P_r$, of orders $p^{\delta_1}, p^{\delta_2}, \cdots, p^{\delta_r}$, be the permutations of an ω-normal U-basis for G; i.e., a set of permutations satisfying the conditions

$$P_i^{p^{\delta_i}} = E, \qquad \delta_1 \geqq \delta_2 \geqq \cdots \geqq \delta_r; \tag{9}$$

$$(P_j, P_i) = P_1^{\alpha_{ji1}} P_2^{\alpha_{ji2}} \cdots P_r^{\alpha_{jir}}, \quad i < j;\ i = 1, 2, \cdots, r;\ j = 2, 3, \cdots, r; \tag{10}$$

$$\alpha_{jik} \equiv 0 \bmod p, \text{ for } k \leqq j.$$

Let $\bar{S}_i$, $i = 1, 2, \cdots, r$ denote the permutation of H which transforms G according to P_i.

Of fundamental importance for our method of attack is the following result:*

(11) The permutations $A_1 = \bar{S}_1^a P_1$, $A_2 = \bar{S}_2^a P_2, \cdots, A_r = \bar{S}_r^a P_r$, which are necessarily of orders $p^{\delta_1}, p^{\delta_2}, \cdots, p^{\delta_r}$ respectively, constitute a U-basis for G_a.

In what follows we shall usually write T_i for $\bar{S}^{-a}$. From the equation

$$P_i = T_i A_i \tag{12}$$

it follows that each basis-element P_i may be regarded as a product of a basis-element of G_a by an automorphism of G_a, and this is a point of view which we shall constantly emphasize.

From (1), (2), and (3) it is easy to establish the following formulas:

$$(A_j, T_i) = (A_j, P_i) = (\bar{S}_j^a P_j, P_i) = (P_j, P_i)^{a+1}; \tag{13}$$

$$(A_i, T_j) = (A_j, T_i)^{-1}; (A_i, T_i) = E. \tag{14}$$

Now each T_i, $i = 1, 2, \cdots, r$, is a permutation in the group of isomorphisms of G_a (see (7) above). Regarded as an automorphism of G_a, each T_i is equivalent to a change of basis for G_a, defined by r equations of the form

$$\begin{cases} A_1 \to A_1' = A_1^{1+\gamma_{1i1}} A_2^{\gamma_{1i2}} \cdots A_r^{\gamma_{1ir}} \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ A_r \to A_r' = A_1^{\gamma_{ri1}} A_2^{\gamma_{ri2}} \cdots A_r^{1+\gamma_{rir}}, \end{cases} \tag{15}$$

where γ_{jik} is a least positive residue modulo p^{δ_k}.

If we denote the matrix of the exponents in (15) by $E_r + M_i$, E_r being the identity matrix of $GL_p(\delta_1, \delta_2, \cdots, \delta_r)$, then the r matrices $E_r + M_i$ generate

* H, p. 177.

a 1–1 representation of H (and consequently a p^γ-1 representation of G, where p^γ is the order of the central $\Gamma(G)$). We know that each γ_{jik} in (15) is uniquely determined by the permutations T_i and $A_1, A_2, \cdots, A_r$. What is of equal interest, perhaps, is the fact that the γ_{jik} are uniquely determined by equations (9) and (10) together with the equations

$$(16) \qquad (P_j, P_i)P_k = P_k(P_j, P_i), \qquad i, j, k = 1, 2, \cdots, r,$$

for the reason that any r operations which satisfy (9), (10), and (16) generate a group which is simply isomorphic with G.*

We indicate a method for computing the γ_{jik} from the data in (9), (10), and (16). If $T_k^x = E$, $k=1, 2, \cdots, r$, where x ranges over all the exponents α_{jik} in (10), that is, if each constituent $P_k^{\alpha_{jik}}$ of (P_j, P_i) is in Γ, then it follows from (12) and (13) that γ_{jik} is equal to the least positive residue of $(a+1)\alpha_{jik}$ modulo p^{δ_k}. In general, however, it is impossible to find for G an ω-normal U-basis for which this favorable situation arises. The following procedure is always valid. In (13) we replace each P_k by T_kA_k, obtaining thereby a first approximation for (A_j, T_i) in terms of the basis elements of G_a:

$$(17) \quad (A_j, T_i) = (P_1^{\alpha_{ji1}} \cdots P_r^{\alpha_{jir}})^{a+1}$$
$$= (T_1^{\alpha_{ji1}} A_1^{\alpha_{ji1}} T_2^{\alpha_{ji2}} A_2^{\alpha_{ji2}} \cdots T_r^{\alpha_{jir}} A_r^{\alpha_{jir}})^{a+1} = T_\alpha^{a+1} A_\alpha^{a+1} c_\alpha^{a+1},$$

where

$$T_\alpha = T_1^{\alpha_{ji1}} \cdots T_r^{\alpha_{jir}}; \; A_\alpha = A_1^{\alpha_{ji1}} \cdots A_r^{\alpha_{jir}}; \; c_\alpha = \prod_{k,l} (A_k, T_l)^{\alpha_{jik}\alpha_{jil}},$$
$$k < l; \; k = 1, 2, \cdots, r; \; l = 2, 3, \cdots, r.$$

Since (P_j, P_i) is in the central of G, we know that T_α must be the identity of H. We observe, in addition, that for $k \leqq j$ the order of $(A_k, T_l)^{\alpha_{jik}\alpha_{jil}}$ is less than the order of (A_k, T_l), since α_{jik} is divisible by p for $k \leqq j$; and for $k > j$, the first constituent of $(A_k, T_l) = P_1^{\alpha_{kl1}} \cdots P_r^{\alpha_{klr}}$ whose exponent is prime to p must have a subscript greater than l. Hence a finite number of reductions of the type (17) will suffice to bring (A_j, T_i) into the form $A_1^{\gamma_{ji1}} \cdots A_r^{\gamma_{jir}}$.

We have outlined a method for constructing, from the data of an ω-normal U-basis, a representation of G by a subgroup of the group $GL_p(\delta_1, \delta_2, \cdots, \delta_r)$ of r-rowed l-matrices. Presently we shall extend this p^γ-1 representation of G to a 1–1 representation by imbedding each matrix $E_r + M_i$ in an $(r+1)$-

* The proof of this assertion is similar to the proof of Theorem I in §2. In interchanging the P's we make use of the formula $P_\beta^y P_\alpha^x = P_\alpha^x P_\beta^y (P_\beta, P_\alpha)^{xy}$, $\beta > \alpha$, which can be derived from (16); a basis for induction is provided by the fact that the exponent of each constituent P_λ in the normal form of (P_β, P_α) is divisible by p for $\lambda \leqq \beta$.

rowed l-matrix. First, however, we list several interesting properties of the matrices M_i:

(18) The highest power of p which divides γ_{jik} divides α_{jik}, and conversely.

(19) Every element in and below the main diagonal of each M_i is divisible by p.

(20) For $j>k$, γ_{jik} is divisible by $p^{\delta_k-\delta_j}$.

The truth of (18) follows from the details of (17) and from the fact that this reduction is reversible; i.e., we may reduce $(A_1^{\gamma_{j1}}\cdots A_r^{\gamma_{jr}})^{-a-1}$ to the form $P_1^{\alpha_{j1}}\cdots P_r^{\alpha_{jr}}$ if we replace A_k by $T_k^{-1}P_k$. Obviously (19) and (20) follow directly from (18), or we may derive (20) from the fact that the order of (A_k, T_i) must divide the order of A_k.

Since $(A_i, T_j)=(A_j, T_i)^{-1}$, we have the relation

$$\gamma_{ijk} = p^{\delta_k} - \gamma_{ijk}. \tag{21}$$

For $i=j$, this gives

$$\gamma_{jjk} = 0, \tag{22}$$

where this zero is the residue 0 modulo p^{δ_k}.

Let M_0 denote the r-rowed l-matrix in which each element in the jth column is the residue 0 modulo $p^{\delta_j}, j=1, 2, \cdots, r$. Let R_{li} denote the r-rowed l-matrix whose lth row is $\gamma_{li1}, \gamma_{li2}, \cdots, \gamma_{lir}$ and whose remaining rows contain only zeros. Now the least positive residues of the lth row in the product $R_{li}M_j$ are the exponents of the commutator $((A_l, T_i), T_j)$ (written, of course, in the normal form $A_1^{\lambda_1}A_2^{\lambda_2}\cdots A_r^{\lambda_r}$). Since this commutator is the identity of G_a, we see that $R_{li}M_j$ must equal M_0. But $M_i=R_{1i}+R_{2i}+\cdots+R_{ri}$.* This establishes an important property of the matrices M_i, namely,

$$M_iM_j \equiv M_0, \qquad i, j = 1, 2, \cdots, r.\dagger \tag{23}$$

For $i=j$, this gives

$$M_i^2 \equiv M_0. \tag{24}$$

Let H_M denote the group generated by the matrices $E_r+M_i, i=1, 2, \cdots, r$. As we have seen above, H_M is a 1–1 representation of H and a p^γ-1 representation of G. The element of H_M which corresponds to the "general" element $P_1^{x_1}P_2^{x_2}\cdots P_r^{x_r}$ of G is the l-matrix derived from $(E_r+M_1)^{x_1}(E_r+M_2)^{x_2}\cdots$

* See note on l-matrices in §3. The matrices M_i, R_{ji} are elements of a ring.

† We wish to emphasize the fact that M_iM_j is to be regarded not as the product of M_i and M_j in the ordinary sense, but as the l-matrix defined by this product.

$(E_r+M_r)^{x_r}$; and from (23) we see that this product can be represented in the simple form*

$$(25) \qquad (E_r + M_1)^{x_1} \cdots (E_r + M_r)^{x_r} \equiv E_r + \sum_{k=1}^{r} x_k M_k.$$

We shall now construct a 1–1 representation of G as a subgroup of the group $GL_p(\delta_0, \delta_1, \delta_2, \cdots, \delta_r)$, where δ_0 is any fixed integer not less than δ_1. First, we define M_i' as the $(r+1)$-rowed l-matrix

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 \\ 0 & \gamma_{1i1} & \gamma_{1i2} & \cdots & \gamma_{1ir} \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ 0 & \gamma_{ri1} & \gamma_{ri2} & \cdots & \gamma_{rir} \end{pmatrix}, \qquad i = 1, 2, \cdots, r,$$

where the elements in the first column are the residues 0 modulo p^{δ_0}. In order to avoid altering much of our earlier notation, we shall number the rows (and columns) in M_i' (and in the other $(r+1)$-rowed matrices which we shall presently define) by the sequence $0, 1, 2, \cdots, r$. Let E' be the identity matrix† of $GL_p(\delta_0, \delta_1, \cdots, \delta_r)$. It is at once evident that the matrices $E'+M_i'$ generate a group G_M which is simply isomorphic with H_M.

We denote by L_i' the $(r+1)$-rowed l-matrix which has in row 0 and column i the residue 1 modulo p^{δ_i} and zeros elsewhere. We shall denote the sum $M_i'+L_i'$ by the symbol N_i'.

The main result of this section is the following:

THEOREM I. *The r matrices $E'+N_i'$ generate a group G_N which is simply isomorphic with G under the correspondence defined by $P_i \sim E'+N_i'$, $i=1, 2, \cdots, r$.*

In proving this theorem we shall make use of the following known result: If $B_1, B_2, \cdots, B_r$, of orders $p^{\delta_1}, p^{\delta_2}, \cdots, p^{\delta_r}$ respectively, constitute a U-basis for an abelian group of order p^m, and if $\Theta_1, \Theta_2, \cdots, \Theta_r$ are a set of automorphisms of this group, each being defined by the r equations

$$(\alpha) \qquad (B_j, \Theta_i) = B_1^{\gamma_{ji1}} \cdots B_r^{\gamma_{jir}},$$

where the δ's and the γ_{jik} are the same as in (9) and (15) above, then the p^m products $\Theta_i B_i$, $i=1, 2, \cdots, r$, generate a group which is simply isomorphic with G under the correspondence $P_i \sim \Theta_i B_i$.‡

* That is, both sides of this equation define the same l-matrix of H_M.

† At this point we shall drop the subscripts from the identity matrices.

‡ This result is contained implicitly in the paper on metabelian groups which has been quoted above (see H, p. 193). It is proved there that the p^m products $\Theta_1^{x_1} \cdots \Theta_r^{x_r} B_1^{x_1} \cdots B_r^{x_r}$, $0 \leqq x_i < p^{\delta_i}$, constitute a group simply isomorphic with G; and it is easy to see that one may bring into this form any product $(\Theta_\alpha B_\alpha)^{y_\alpha} \cdots (\Theta_\beta B_\beta)^{y_\beta} \cdots$.

To prove Theorem I it is therefore sufficient to show that

(i) $E'+N_i'$ equals U_iV_i, where U_i and V_i denote $E'+M_i'$ and $E'+L_i'$, respectively;

(ii) $V_1, V_2, \cdots, V_r$ are of orders $p^{\delta_1}, p^{\delta_2}, \cdots, p^{\delta_r}$ respectively, generate an abelian group, and constitute a U-basis for this group;

(iii) the U_i and V_j satisfy the equations

$$(\beta) \qquad (V_j, U_i) = V_1^{\gamma_{ji1}} \cdots V_r^{\gamma_{jir}}, \qquad i < j;\ i = 1, \cdots, r;\ j = 2, \cdots, r.$$

First, we write several useful formulas, which can be verified from the rules for multiplying l-matrices:*

$$(26) \qquad \begin{aligned} &L_iL_j \equiv M_{0j}M_iM_j \equiv M_0 \quad ((23) \text{ above}); \quad M_iL_j \equiv M_0; \\ &L_jM_i \equiv \gamma_{ji1}L_1 + \cdots + \gamma_{jir}L_r, \qquad i, j = 1, 2, \cdots, r. \end{aligned}$$

$$(27) \qquad \begin{aligned} &U_i^{x_i} = (E + M_i)^{x_i} \equiv E + x_iM_i; \quad V_j^{y_j} = (E + L_j)^{y_j} \equiv E + y_jL_j; \\ &U_1^{x_1} \cdots U_r^{x_r} \equiv E + \sum_{k=1}^{r} x_kM_k; \qquad V_1^{y_1} \cdots V_r^{y_r} \equiv E + \sum_{k=1}^{r} y_kL_k. \end{aligned}$$

To prove (i) we have

$$U_iV_i = (E + M_i)(E + L_i) \equiv E + M_i + L_i + M_iL_i \equiv E + M_i + L_i = E + N_i.$$

(By definition, $N_i = L_i + M_i$; from (26), $M_iL_i \equiv M_0$.)

We now prove (ii). The equation $V_i^{y_i} = E$ requires $E + y_iL_i \equiv E$. Since p^{δ_i} is the smallest value of y_i for which $y_iL_i \equiv M_0$, it follows that the order of V_i is exactly p^{δ_i}. The permutability of V_i and V_j follows from (26). For $V_1, V_2, \cdots, V_r$ to constitute a U-basis for the abelian group which they generate, it is sufficient that the equation $V_1^{y_1} \cdots V_r^{y_r} = E$ be satisfied only by $y_i \equiv 0 \bmod p^{\delta_i}$. That this is the case follows directly from (27) and the linear independence of the L's.

Finally we prove (iii). From (26) and (27) we derive the equalities†

$$\begin{aligned} (V_j, U_i) = V_j^{-1}U_i^{-1}V_jU_i &\equiv (E - L_j)(E - M_i)(E + L_j)(E + M_i) \\ &\equiv (E - L_j - M_i + L_jM_i)(E + L_j + M_i + L_jM_i) \\ &\equiv E + \sum_{k=1}^{r} \gamma_{jik}L_k \\ &\equiv \prod_{k=1}^{r} (E + L_k)^{\gamma_{jik}} = V_1^{\gamma_{ji1}}V_2^{\gamma_{ji2}} \cdots V_r^{\gamma_{jir}}. \end{aligned}$$

* We shall drop all primes, since from this point on we shall deal exclusively with $(r+1)$-rowed matrices. Note that M_0 is now the $(r+1)$-rowed null-matrix of the set $L_p(\delta_0, \delta_1, \cdots, \delta_r)$.

† It is understood, of course, that the notation $E - L_j$ is merely a convenient substitute for $E + (p^{\delta_j} - 1)L_j$.

This completes the determination of our 1–1 representation of G by means of l-matrices. As we have seen, this particular representation G_N is completely defined by the orders of the basis elements $P_1, P_2, \cdots, P_r$ of G, the exponents α_{jik} in the $r(r-1)/2$ equations (10), and the permutability relation $(P_i, P_j)P_k = P_k(P_i, P_j)$. In respect to the totality of possible representations of G by l-matrices $L_p(\delta_1, \delta_2, \cdots, \delta_r)$, the representation G_N may be regarded as a normal form, in that for every matrix in G_N the elements in and below the main diagonal are congruent modulo p to 1 and 0 respectively.

We observe that the matrices $E+\sum_{k=1}^{r} x_k L_k$, $0 \leqq x_k < p^{\delta_k}$, define a 1–1 representation of the abelian group G_a, and the corresponding elements of G_N are the l-matrices derived from the products $(E+\sum_{k=1}^{r} x_k M_k)(E+\sum_{k=1}^{r} x_k L_k) \equiv E+\sum_{k=1}^{r} x_k N_k$ (see (8) and (25) above). Thus we obtain all the elements of G_N from a "general" matrix, whose coordinates are linear functions of r parameters, by specializing these parameters and taking least positive residues. We shall see, later, that the N's combine under multiplication according to the linear formula $N_i N_j \equiv \sum_{k=1}^{r} \gamma_{ijk} N_k$.

5. The notation which we shall use in this section is that of the preceding. Our objective is to characterize those matrices of the group $GL_p(\delta_1, \delta_2, \cdots, \delta_r)$ which represent automorphisms* of G. We know, of course, that the group of isomorphisms of G_a is simply isomorphic with $GL_p(\delta_1, \delta_2, \cdots, \delta_r)$; and from (7) of §4 it follows that $I(G)$ is simply isomorphic with a certain subgroup of $GL_p(\delta_1, \cdots, \delta_r)$. Now every matrix $X = (x_{ij})$ in $GL_p(\delta_1, \cdots, \delta_r)$ is characterized by two conditions on the coordinates x_{ij}, namely,

$$x_{ij} \equiv 0 \bmod p^{\delta_j - \delta_i} \text{ for } i > j; \tag{1}$$

$$|x_{ij}| \not\equiv 0 \bmod p. \tag{2}$$

Our problem, therefore, is to determine the additional restrictions which must be imposed on the coordinates x_{ij} in order that x shall define an automorphism of G. It is possible to determine these additional conditions as congruences involving the α_{jik} by regarding X as the coefficient-matrix in the correspondence

$$\begin{cases} P_1 \sim P_1^{x_{11}} \cdots P_r^{x_{1r}} \\ \cdots\cdots\cdots\cdots \\ P_r \sim P_1^{x_{r1}} \cdots P_r^{x_{rr}}. \end{cases}$$

It is much easier, however, to determine them in terms of the γ_{jik}, and this is

* Throughout this article the term "automorphism" of G denotes a 1-1 isomorphism of G with itself.

the procedure which we shall adopt. First, we regard X as the coefficient-matrix of the "general" automorphism of G_a, defined by the correspondence

$$(3) \qquad \begin{cases} A_1 \sim B_1 = A_1^{x_{11}} \cdots A_r^{x_{1r}} \\ \cdots\cdots\cdots\cdots \\ A_r \sim B_r = A_1^{x_{r1}} \cdots A_r^{x_{rr}}, \end{cases}$$

the x_{ij} being least positive residues.

Let π_x denote that permutation of $I(G_a)$ which is defined by X. Now π_x transforms G either into itself or a conjugate permutation group in $K(G_a)$; furthermore, G is generated by the r permutations $P_i = T_i$, $i = 1, \cdots, r$ (see (11) and (12) of §4). Hence, for X to define an automorphism of G it is necessary and sufficient that $\pi_x^{-1} T_i A_i \pi_x$, $x = 1, 2, \cdots, r$, be a permutation of G. Now the permutation of G which corresponds to the permutation $A_x = A_1^{z_1} \cdots A_r^{z_r}$ of G_a is the product $T_x A_x$, where T_x is $T_1^{z_1} \cdots T_r^{z_r}$ (see (8) of §4). Consequently, for X to define an automorphism of G it is necessary and sufficient that

$$(4) \qquad \pi_x^{-1} T_i \pi_x \text{ be equal to } T_1^{x_{i1}} \cdots T_r^{x_{ir}}, \qquad i = 1, 2, \cdots, r.$$

The sufficiency of this condition is obvious. That it is necessary, as well, follows from the fact that if we multiply a given permutation $A_z = A_1^{z_1} \cdots A_r^{z_r}$, $0 \leqq z_i < p^{\delta_i}$, on the left by all the permutations of H, then only one of these products will be a permutation in G; that is, the multiplying permutation T_x is unique, although its representation in the form $T_1^{z_1} \cdots T_r^{z_r}$, $0 \leqq z_i < p^{\delta_i}$, is never unique.

We seek a more explicit form for condition (5). As in the preceding section, each T_i is equivalent to a substitution

$$(5) \qquad \begin{cases} A_1 \to A_1' = A_1^{1+\gamma_{1i1}} \cdots A_r^{\gamma_{1ir}} \\ \cdots\cdots\cdots\cdots \\ A_r \to A_r' = A_1^{\gamma_{ri1}} \cdots A_r^{\gamma_{rir}}, \end{cases}$$

whose matrix we have already denoted by $E + M_i$. Similarly, the product $T_1^{x_{i1}} \cdots T_r^{x_{ir}}$ is equivalent to a substitution on the A's whose matrix is given by $E + \sum_{k=1}^{r} x_{ik} M_k$ (see (25) of §4). And the matrix of that substitution (on the A's) which is equivalent to the permutation $\pi_x^{-1} T_i \pi_x$ is clearly equal to $X^{-1}(E + M_i)X$. Hence (5) is equivalent to the equations

$$(6) \qquad E + \sum_{k=1}^{r} x_{ik} M_k \equiv X^{-1}(E + M_i)X, \qquad i = 1, \cdots, r;$$

and these, in turn, are equivalent to the set

$$\sum_{k=1}^{r} x_{ik}M_k \equiv X^{-1}M_iX. \tag{7}$$

The main result of this section may be expressed by the theorem:

The group of isomorphisms of G is simply isomorphic with the group generated by those l-matrices $L_p(\delta_1, \cdots, \delta_r)$ for which the following conditions are satisfied:

(a) $$x_{ij} \equiv 0 \bmod p^{\delta_j-\delta_i} \quad \textit{for} \quad i > j;$$

(b) $$|x_{ij}| \not\equiv 0 \bmod p;$$

(c) $$\sum_{k=1}^{r} x_{ik}M_k \equiv X^{-1}M_iX, \qquad i = 1, 2, \cdots, r.$$

In conclusion, we state a useful relation, namely,

$$\sum_{k=1}^{r} \gamma_{ijk}M_k \equiv M_0, \qquad i = 1, 2, \cdots, r, \tag{8}$$

which can be derived by substituting $E+M_i$ for X in (7) above.

6. In this section we shall investigate the abstract structure of the representation G_N, and we shall see that the matrices $E, N_1, \cdots, N_r$ may be regarded as basis-units in a certain finite ring.

We have already pointed out that the general element of G_N is obtained by reducing the matrix $J_x=E+\sum_{k=1}^{r}x_kN_k$, where each x_k ranges from 0 to $p^{\delta_k}-1$. Since the product $J_z=J_xJ_y$ must occur in the form $J_z=E+\sum z_kN_k$, each of the r^2 products N_iN_j must obviously be equivalent to a linear function of the matrices $E, N_1, \cdots, N_r$. This linear relation is given by the formula

$$N_iN_j \equiv \sum_{k=1}^{r} \gamma_{ijk}N_k. \tag{1}$$

In deriving this formula we replace N_i by L_i+M_i.* From (26) of §4 and (8) of §5 we have the chain of equations

$$N_iN_j = (L_i + M_i)(L_j + M_j) \equiv L_iM_j \equiv \sum_{k=1}^{r} \gamma_{ijk}L_k \equiv \sum_{k} \gamma_{ijk}L_k + \sum_{k} \gamma_{ijk}M_k$$

$$\equiv \sum_{k} \gamma_{ijk}(L_k + M_k) \equiv \sum_{k=1}^{r} \gamma_{ijk}N_k.$$

* Observe that M_i is the $(r+1)$-rowed matrix M_i' of §4. It is evident that (8) above is valid if we replace M_i by M_i'.

Since $\gamma_{jik} \equiv -\gamma_{ijk} \bmod p^{\delta_k}$ and $\gamma_{iik} \equiv 0 \bmod p^{\delta_k}$ (see (21) and (22) of §4), we have for the N's the further relations

$$N_iN_j \equiv -N_jN_i \tag{2}$$

(the interpretation of this congruence is obvious);

$$N_i^2 \equiv N_0, \tag{3}$$

where N_0 is the $(r+1)$-rowed null matrix.

From (1) and (2) it is easy to show that the product of any three of the N's is the null matrix; that is,

$$N_iN_jN_k \equiv N_0, \qquad i, j, k = 1, 2, \cdots, r. \tag{4}$$

At this point it is fairly evident that with the group G_N there is associated a finite ring having as basis-units the matrices $E, N_1, \cdots, N_r$. We wish to show that this ring can be constructed without assuming the existence of G_N.

We start with a system $\mathfrak{S}$ of double composition in which all the ring postulates are satisfied except (possibly) associativity of multiplication. We designate a set of $r+1$ linearly independent basis-units for $\mathfrak{S}$ by $v_e, v_1, \cdots, v_r$, and we assume that every element of $\mathfrak{S}$ can be represented uniquely in the form $v_x = x_0v_e + \sum_{i=1}^{r} x_iv_i$, where the x_i are arbitrary rational integers.

We assume that multiplication for the basis-units (and accordingly for every element of $\mathfrak{S}$) is defined by the equations

$$\left\{\begin{array}{ll} v_e^2 = v_e, & \\ v_ev_i = v_iv_e = v_i, & i = 1, 2, \cdots, r, \\ v_iv_j = \sum_{k=1}^{r} \gamma_{ijk}v_k, * & \end{array}\right. \tag{5}$$

where the γ_{ijk} have the same values as in (1) above. We recall that each γ_{ijk} is a positive integer less than p^{δ_k}, and that these r^3 integers satisfy

$$\gamma_{ijk} \equiv -\gamma_{jik} \bmod p^{\delta_k} \qquad [\S4, (21)] \tag{6}$$

$$\left.\begin{array}{ll} \gamma_{ijk} \equiv 0 & \bmod p^{\delta_k - \delta_i} \text{ for } i > k \\ \gamma_{ijk} \equiv 0 & \bmod p^{\delta_k - \delta_j} \text{ for } j > k \end{array}\right\} \quad [\S4, (20) \text{ and } (21)] \tag{7}$$

$$\sum_{\alpha=1}^{r} \gamma_{ija}\gamma_{akl} \equiv 0 \bmod p^{\delta_l} \qquad [\S4, (23)] \tag{8}$$

$$\sum_{\alpha=1}^{r} \gamma_{jka}\gamma_{ial} \equiv 0 \bmod p^{\delta_l} \qquad [\S5, (8)]. \tag{9}$$

* It is known, of course, that the various assumptions above are always consistent. In fact, a system of the type $\mathfrak{S}$ exists if we replace the γ_{ijk} in (5) by r^3 arbitrary integers; and if multiplication is associative (which is generally not the case), then this system is a ring of rank $r+1$, having the ring of integers as its coefficient-domain.

Now those elements v_x for which x_k is divisible by p^{δ_k}, $k=0, 1, \cdots, r$,* constitute under addition a modulus $\mathfrak{M}$. We wish to show that the elements of this modulus constitute an invariant ideal in $\mathfrak{S}$. Since they form a modulus, it is sufficient to show that $v_x\alpha_y$ and $\alpha_y v_x$ are each of the form $\lambda_0 p^{\delta_0} v_e + \sum_{i=1}^{r} \lambda_i p^{\delta_i} v_i$, where v_x and α_y are any elements of $\mathfrak{S}$ and $\mathfrak{M}$ respectively.

From (5) we have†

$$\left(\sum_{i=1}^{r} x_i v_i\right)\left(\sum_{j=1}^{r} y_j p^{\delta_j} v_j\right) = \sum_{k=1}^{r}\left[\sum_{i=1}^{r} x_i\left(\sum_{j=1}^{r} y_j p^{\delta_j}\gamma_{ijk}\right)\right] v_k.$$

Since $\delta_1 \geqq \delta_2 \geqq \cdots \geqq \delta_r$, it is obvious that when k is at least equal to both i and j, then the coefficient of v_k is divisible by p^{δ_k}. From (7), however, we know that γ_{ijk} has the form $\gamma'_{ijk}p^{\delta_k-\delta_i}$ (or $\gamma''_{ijk}p^{\delta_k-\delta_j}$) for $k<i$ (for $k<j$). In every case then, the coefficient of v_k is divisible by p^{δ_k}, $k=0, 1, \cdots, r$. Similarly, we may show that $\alpha_y v_x$ is an element of $\mathfrak{M}$. We denote this invariant ideal by the letter $\mathfrak{z}$.

From a familiar result in the theory of ideals we know that the residue classes of $\mathfrak{S}$ with respect to $\mathfrak{z}$ form a system $\overline{\mathfrak{S}}$ which is homomorphic with $\mathfrak{S}$. If we denote by $u_e, u_1, \cdots, u_r$ the elements of $\overline{\mathfrak{S}}$ to which $v_e, v_1, \cdots, v_r$ correspond respectively in this homomorphism, then it is easy to see that the u's constitute a basis for $\overline{\mathfrak{S}}$, and that every element of $\overline{\mathfrak{S}}$ can be represented in the form $u_x = [x_0]u_e + \sum_{i=1}^{r}[x_i]u_i$, where $[x_i]$ is the symbol for the class of integers congruent to x_i modulo p^{δ_i}. In view of the homomorphism above, we know that the sum u_x+u_y is represented by $[x_0+y_0]u_0+\sum_i[x_i+y_i]u_i$, while the multiplication table for the u's is given by

$$\begin{aligned} u_e^2 &= u_e, \\ u_e u_i &= u_i u_e = u_i, \qquad i = 1, 2, \cdots, r, \\ u_i u_j &= \sum_{k=1}^{r} \gamma_{ijk} u_k. \end{aligned} \tag{10}$$

The condition for associativity of multiplication in $\overline{\mathfrak{S}}$ is given by

$$\left[\sum_{\alpha=1}^{r} [\gamma_{ij\alpha}]_\alpha [\gamma_{\alpha k l}]_l\right]_l = \left[\sum_{\alpha=1}^{r} [\gamma_{jk\alpha}]_\alpha [\gamma_{i\alpha l}]_l\right]_l.\ddagger$$

But from (8) and (9) we know that both sides of this equation are equal to the residue class 0 modulo p^{δ_l}. Hence $\overline{\mathfrak{S}}$ is a ring, since it is homomorphic

* These p^{δ_k} are the type-invariants of G [see §4].

† Obviously $v_x \cdot y_0 p^{\delta_0} v_e$ is in $\mathfrak{M}$.

‡ The symbol $[\xi]_\lambda$ denotes the class of integers having the form $\xi \pm np^{\delta_\lambda}$. We need consider only elements in $\overline{\mathfrak{S}}$ of the form $\sum_{i=1}^{r}[x_i]u_i$, since $(u_e u_x)u_y$ is obviously equal to $u_e(u_x u_y)$.

with a system $\mathfrak{S}$ which satisfies every ring postulate except associativity of multiplication.

From (6), which implies that $[\gamma_{ijk}]_k = [-\gamma_{jik}]_k$, we may easily show that those elements in $\overline{\mathfrak{S}}$ which have the form $u_x' = \sum_{i=1}^{r} [x_i]u_i$ constitute a nilpotent* ring $\mathfrak{R}$ of index 3 in which the square of every element is the zero element. It is clear that $\mathfrak{R}$ is an invariant subring of $\overline{\mathfrak{S}}$; furthermore, the elements of $\mathfrak{R}$ constitute under addition an abelian group A_R which is simply isomorphic with G_a of §4. One may also show that the elements of $\overline{\mathfrak{S}}$ having the form $u_x'' = [1]u_e + u_x'$ constitute under multiplication a group G_R of order p^m and class 2. That they form a group is obvious, since $u_x''u_y''$ can be brought into the form $[1]u_e + u_z'$, while every u_x'' has an inverse, namely, $[1]u_e + \sum_{i=1}^{r}[-x_i]u_i$. The commutator (u_i'', u_j''), where $u_i'' = u_e + u_i$, is $u_e + \sum_{\alpha=1}^{r} 2\gamma_{ij\alpha}u_\alpha$, and by using (8) and (9) one readily computes for $(u_i'', u_j'')u_k''$ and $u_k''(u_i'', u_j'')$ the common value $u_e + u_k + \sum_{\alpha=1}^{r} 2\gamma_{ij\alpha}u_\alpha$. Since G_R is generated by the u_k'''s, its commutator subgroup must be contained in its central; hence G_R is of class 2.

Since $\overline{\mathfrak{S}}$ contains a principal unit u_e, we can construct a 1–1 matrix-representation of $\overline{\mathfrak{S}}$ by the familiar process of post-multiplication. We denote the products $u_e(u_e+u_i)$, $u_1(u_e+u_i)$, $\cdots$, $u_r(u_e+u_i)$ by $\bar{u}_e$, $\bar{u}_1$, $\cdots$, $\bar{u}_r$ respectively. Then the matrix-representation of the element u_e+u_i is the coefficient-matrix of the linear transformation

$$\begin{cases} \bar{u}_e = u_e + u_i \\ \bar{u}_1 = (1+\gamma_{1i1})u_1 + \cdots + \gamma_{1ir}u_r \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ \bar{u}_r = \gamma_{ri1}u_1 + \cdots + (1+\gamma_{rir})u_r. \end{cases}$$

And this matrix is exactly the l-matrix $E+N_i$ of G_N. Since G_R is generated by the r elements u_e+u_i, $i=1, 2, \cdots, r$, it follows that the group $G_R(\ )$ is simply isomorphic with G_N, and consequently with G (of §4).

This representation of G as a multiplicative group of elements in a finite ring which are congruent to the principal unit modulo a nil ring has conspicuous advantages for the study of the structure of G.† For instance, if $\mathfrak{R}'$ is an invariant subring of $\mathfrak{R}$, then the elements of G_R which have the form

* A nilpotent ring of index k is a ring in which the product of any k elements is 0; a nil ring is one in which some power of every element is 0. A nil ring containing a finite basis is necessarily nilpotent.

† This method of "Strahlbildung" has been used to advantage by K. Shoda (Mathematische Annalen, vol. 100 (1928), pp. 674–686) for determining two important series of characteristic subgroups of $GL_p(\delta_1, \delta_2, \cdots, \delta_r)$.

$[1]u_e+\rho$, ρ in $\mathfrak{R}'$, constitute an invariant subgroup of G_R. Thus the subgroup $\mathfrak{V}_\alpha(G_R)$ corresponds to the subring $\sum_{i=1}^{r}[x_i p^\alpha]u_i$ of $\mathfrak{R}$.

From the representation G_R we can derive a second set of conditions on the coordinates of those matrices in $L_p(\delta_1, \delta_2, \cdots, \delta_r)$ which define automorphisms of G. Now any automorphism of the additive group in $\mathfrak{R}$ is defined by a linear transformation

$$\Theta: \begin{cases} u_1' = y_{11}u_1 + \cdots + y_{1r}u_r \\ \cdots\cdots\cdots\cdots \\ u_r' = y_{r1}u_1 + \cdots + y_{rr}u_r, \end{cases}$$

in which the y_{ij} are least positive residues satisfying the conditions

$$|y_{ij}| \not\equiv 0 \bmod p;\ y_{ij} \equiv 0 \bmod \phi^{\delta_j-\delta_i} \text{ for } i > j. \tag{11}$$

But Θ defines a correspondence of the elements of G_R, and for this correspondence to define an automorphism of G_R, it is clearly necessary and sufficient that the multiplication table of the u_i''s be the same as that of the u_i's. By substituting the u_i''s in equations (10) and taking account of the relations $u_i^2 \equiv 0$ and $u_j u_i \equiv -u_i u_j$ we find that Θ will define an automorphism of G_R if, and only if, the y's satisfy the $r^2(r-1)/2$ congruences

$$\sum_{\mu,\nu} D_{ij-\mu\nu}\gamma_{\mu\nu k} \equiv \sum_{\alpha=1}^{r} \gamma_{ij\alpha}y_{\alpha k} \bmod p^{\delta_k},$$

where $k = 1, \cdots, r$; $i < j$; $i = 1, \cdots, r$; $j = 2, \cdots, r$; $\mu < \nu$; $\mu = 1, \cdots, r$; $\nu = 2, \cdots, r$, and where $D_{ij-\mu\nu}$ denotes the determinant

$$\begin{vmatrix} y_{i\mu} & y_{i\nu} \\ y_{j\mu} & y_{j\nu} \end{vmatrix}.$$

As one would expect, these congruences are equivalent to the matrix-equations (7) in §5.

The representation G_R above was derived (although indirectly) from a particular ω-normal U-basis of G, and our method is probably the simplest one for obtaining a ring-representation for G. But the existence of a U-basis is by no means necessary* for the existence of a representation of a finite p-group $\overline{G}$ as the multiplicative group of those elements in a ring which are congruent to the principal unit modulo a subring whose elements are expressible uniquely in the form $\sum_{i=1}^{r}\xi_i w_i$, the ξ_i being least positive residues

* The quaternion group, which has no U-basis, is the multiplicative group of elements $\rho+\xi_1 u_1 + \xi_2 u_2 + \xi_3 u_3$, $i=0, 1$, in the ring of 16 elements whose multiplication is defined by the equations $e^2=e$; $eu_i = u_i e = u_i$; $u_1^2 = u_2^2 = u_2u_1 = u_3$; $u_1u_3 = u_3u_1 = u_1u_2 = u_2u_3 = u_3u_2 = u_3^2 = 0$.

modulo certain powers of p. Nor is it necessary, when $\overline{G}$ is the group G above, that $\bar{r}$, the number of linearly independent basis units of $\overline{\mathfrak{R}}$, be equal to r, the number of type-invariants of G. For $\bar{r} \neq r$, however, the ring $\overline{\mathfrak{R}}$ must contain elements whose square is not zero, and although it is always nilpotent, it need not be of index 3.

In conclusion, we point out that if the group G is a direct product of groups $G' \times G'' \times \cdots$, then for each factor $G^{(i)}$ we can find an ω-normal U-basis, and by the method given in §§4 and 6 we can construct for each factor a ring-representation $G_{R^{(i)}}$. Then for G itself we obtain a ring-representation if we replace $\mathfrak{R}$ in §6 by the direct sum of the rings $\mathfrak{R}' + \mathfrak{R}'' + \cdots$. And from this representation we obtain, by post-multiplication, a representation of G as the direct sum of matrix-representations $G_{N'} + G_{N''} + \cdots$.

7. In the preceding section we proved that every metabelian group of prime-power order can be exhibited as a multiplicative group in a finite ring. And since every metabelian group is the direct product of its Sylow subgroups, one may construct for any metabelian group $\overline{G}$ of odd order a representation of this sort in which the ring $\mathfrak{R}$ is replaced by the direct sum of nil rings $\mathfrak{R}_{p_1}, \mathfrak{R}_{p_2}, \cdots$, each $\mathfrak{R}_{p_\lambda}$ corresponding to a Sylow subgroup of $\overline{G}$. We wish to show that there is, in a crude sense, a reciprocal relationship between nil rings and metabelian groups.

If S is a ring which contains a principal unit e and a subring Σ such that
(a) *the square of every element in Σ is the zero element, and*
(b) *the number of elements in Σ is an odd integer n,*
then those elements in S which are of the form $e+\sigma$, σ in Σ, constitute under multiplication a group of order n whose class does not exceed 2.

It is easy to show that the elements $e+\sigma$ constitute under multiplication a group F_Σ of order n, having e as the identical operation. We therefore give only the proof that F_Σ is either abelian or metabelian.

Let α and β denote any two elements of Σ. From (a) we have

$$\sigma^2 = 0, \text{ where } \sigma \text{ is any element of } \Sigma. \tag{1}$$

By substituting $\alpha+\beta$ for σ in this equation, we obtain

$$\alpha\beta + \beta\alpha = 0. \tag{2}$$

Two cases arise:

Case A. $\alpha\beta = \beta\alpha$ for every pair of elements in Σ;

Case B. Σ contains two elements σ_α and σ_β such that $\sigma_\alpha\sigma_\beta \neq \sigma_\beta\sigma_\alpha$.

In Case A equation (2) reduces to $2\alpha\beta = 0$. Since Σ contains a finite number of elements, with each element σ_i there is associated a smallest positive

integer m_i such that $m_i\sigma_i=0$. Now the elements of Σ constitute under addition an abelian group of order n, and since m_i is clearly the order of σ_i with respect to this group, we see that m_i, being a divisor of n, is necessarily odd. Hence the equation $2\alpha\beta=0$ is possible only if $\alpha\beta=0$. In Case A, therefore, any two elements $e+\alpha$ and $e+\beta$ are commutative, and F_Σ is of class 1.

For Case B we first prove that the product of any three elements of Σ is zero. By using (2) and the associativity postulate, we obtain the equations

$$(3)\qquad \begin{aligned}(\sigma_\alpha\sigma_\beta)\sigma_\gamma &= \sigma_\alpha(\sigma_\beta\sigma_\gamma) = -(\sigma_\beta\sigma_\gamma)\sigma_\alpha = -\sigma_\beta(\sigma_\gamma\sigma_\alpha) = (\sigma_\gamma\sigma_\alpha)\sigma_\beta \\ &= \sigma_\gamma(\sigma_\alpha\sigma_\beta) = -(\sigma_\alpha\sigma_\beta)\sigma_\gamma.\end{aligned}$$

That is, $2\sigma_\alpha\sigma_\beta\sigma_\gamma=0$; and as in Case A, we infer that $\sigma_\alpha\sigma_\beta\sigma_\gamma$ is zero. To prove that F_Σ is of class 2 it is sufficient to show that the commutator $(e+\sigma_\alpha, e+\sigma_\beta)$ of any two elements in F_Σ is commutative with any third element $e+\sigma_\gamma$. From (1) we find that the inverse of $e+\sigma_\alpha$ is $e-\sigma_\alpha$. By making use of (3), it is a simple matter to show that the commutator $(e+\sigma_\alpha, e+\sigma_\beta)$ is given by $e+\sigma_\alpha\sigma_\beta-\sigma_\beta\sigma_\alpha$ and is commutative with $e+\sigma_\gamma$.

Finally, we observe that the theorem above is valid if we replace (a) by the assumption that Σ is nilpotent and of index 3; that is, the product of any three elements in Σ is the zero-element. (In this case, the commutator $(e+\sigma_\alpha, e+\sigma_\beta)$ equals $e+\sigma_\alpha\sigma_\beta-\sigma_\beta\sigma_\alpha-\sigma_\alpha^2-\sigma_\beta^2$.)

BROWN UNIVERSITY,
PROVIDENCE, R. I.