THE GROUP OF CLASSES OF CONGRUENT MATRICES WITH APPLICATION TO THE GROUP OF ISOMORPHISMS OF ANY ABELIAN GROUP*

BY

ARTHUR RANUM

Introduction.

AN ordinary linear congruence group, or JORDAN† group, may be considered as a group of matrices whose elements (coefficients) are all residues of the same modulus m, or in other words as a group of classes of congruent matrices, mod m. Among the writers on these groups, besides JORDAN, are CAUCHY, MATHIEU, MOORE, DICKSON (for the case where m is prime) and GIERSTER (for the case where m is composite).

The subject of the first part of this paper is a generalization of the JORDAN group, and is obtained by using different moduli for the different elements of the matrices, so that each element is a residue of its own particular modulus. In this way a more general "group of classes of congruent matrices" is obtained, which includes the JORDAN group as a special case. For the sake of brevity it will sometimes be designated by the shorter title "linear congruence group," although its operators are matrices and not linear substitutions.

The second part is devoted to the application of these more general linear congruence groups to the group of isomorphisms of any abelian group. For the purpose of this application it will be shown that there is no loss of generality in restricting the moduli to being powers of the same prime p. Therefore that case alone will be considered in the first part.

Since every group of finite order can be represented as a group of matrices, the problem of finding the minimum degree of its representation is of considerable interest. In a large number of cases the degree can be made lower by means of these general groups than is possible by means of JORDAN groups alone. In other words, many of these groups cannot be represented as subgroups of JORDAN groups of the same degree; they are new groups of that degree.

* Received for publication August 6, 1906. Presented to the Society at the New Haven summer meeting September 3, 1906.

† JORDAN, *Traité des Substitutions*, 1870, pp. 91–110.

PART I.

THE GROUP OF CLASSES OF CONGRUENT MATRICES.

Classes of congruent matrices.

1. Let (l_{ij}) represent an n-ary matrix, or square array, of n^2 integers l_{ij} $(i, j = 1, 2, \cdots, n)$, l_{ij} being the element in the ith row and jth column. We introduce once for all a fixed matrix

$$(p^{a_{ij}})$$

whose elements $p^{a_{ij}}$ are powers of the same prime p with exponents $a_{ij} \geqq 0$, and call two matrices (l_{ij}), (m_{ij}) congruent with respect to the matrix $(p^{a_{ij}})$ as a modulus, in notation

$$(l_{ij}) \equiv (m_{ij}) \mod (p^{a_{ij}}),$$

in case

$$l_{ij} \equiv m_{ij} \mod p^{a_{ij}} \qquad (i, j = 1, 2, \cdots, n).$$

The elements $p^{a_{ij}}$ of the modular matrix $(p^{a_{ij}})$ are referred to as the moduli.

All matrices congruent to (l_{ij}) will be said to belong to the *class* * $((l_{ij}))$. In this way all matrices are distributed among a finite number of mutually exclusive classes.

Composition of classes.

2. Taking the usual law of composition or multiplication of matrices, viz.,

$$(1) \qquad (l_{ij})(l'_{ij}) = (l''_{ij}),\ l''_{ik} = \sum_{j=1}^{n} l_{ij} l'_{jk} \qquad (i, k = 1, \cdots, n),$$

we proceed to prove

THEOREM 1. *If (l_{ij}) and (l'_{ij}) are given matrices and if the matrices (m_{ij}) and (m'_{ij}) range over the classes $((l_{ij}))$ and $((l'_{ij}))$ respectively, the product $(m_{ij})(m'_{ij}) = (m''_{ij})$ will always belong to the class $((l''_{ij}))$, if, and only if, the conditions*

$$(2) \qquad p^{a_{ij}+a_{jk}} \equiv 0, \quad l_{ij} p^{a_{jk}} \equiv 0, \quad p^{a_{ij}} l'_{jk} \equiv 0, \quad \text{mod } p^{a_{ik}} \quad (i, j, k = 1, \cdots, n),$$

are satisfied.

When the conditions (2) are satisfied, there is defined a *unique law of composition of the classes* $((l_{ij}))$ and $((l'_{ij}))$, in virtue of which their product, in this order, is $((l''_{ij}))$.

* The explicit use of classes of matrices was suggested to me by Professor DICKSON.

3. Proof. The general values of the elements of (m_{ij}) and (m'_{ij}) are

$$m_{ij} = l_{ij} + h_{ij} p^{a_{ij}}, \qquad m'_{ij} = l'_{ij} + h'_{ij} p^{a_{ij}},$$

where h_{ij} and h'_{ij} are any integers. Therefore (m''_{ij}) will always belong to the class $((l''_{ij}))$, if and only if it is possible, whatever be the values of h_{ij} and h'_{ij}, to find values of the integers h''_{ij} $(i, j = 1, \cdots, n)$ to satisfy the equations

$$l''_{ik} + h''_{ik} p^{a_{ik}} = \sum_j (l_{ij} + h_{ij} p^{a_{ij}})(l'_{jk} + h'_{jk} p^{a_{jk}}) \quad (i, k = 1, \cdots, n).$$

All summations, unless otherwise specified, have the range $1, \cdots, n$.

By expansion and the subtraction of (1), these become

$$\sum_j h'_{jk} l_{ij} p^{a_{jk}} + \sum_j h_{ij} l'_{jk} p^{a_{ij}} + \sum_j h_{ij} h'_{jk} p^{a_{ij}+a_{jk}} = h''_{ik} p^{a_{ik}} \quad (i, k = 1, \cdots, n),$$

which are to be identities in the indeterminates h_{ij} and h'_{jk} and are therefore equivalent to the series of congruences (2).

4. Corollary. *The modular matrix* $(p^{a_{ij}})$ *admits the possibility of the composition of certain classes, if, and only if,*

$$a_{ij} + a_{jk} \geqq a_{ik} \qquad (i, j, k = 1, \cdots, n). \tag{3}$$

Sets of classes.

5. Conditions (2) show that unless all the moduli are alike, the composition of classes cannot apply to every * pair of classes. But it will be seen that if the moduli satisfy (3), a certain limited *set* of classes can be found, to which composition applies.

Suppose that $((l^{(s)}_{ij}))$ $(s = 1, 2, \cdots, N)$ are the classes of any such set S, not necessarily the largest set and not necessarily forming a group. Let $p^{\beta_{ij}}$ $(\beta_{ij} \geqq 0)$ be the highest power of p dividing $l^{(1)}_{ij}, \cdots, l^{(N)}_{ij}$, and put

$$l^{(s)}_{ij} = p^{\beta_{ij}} \lambda^{(s)}_{ij} \qquad (i, j = 1, \cdots, n;\ s = 1, \cdots, N), \tag{4}$$

where the factors $\lambda^{(s)}_{ij}$ $(s = 1, \cdots, N)$ cannot all be divisible by p. Since $l^{(s)}_{ij}$ is a residue of $p^{a_{ij}}$, $\lambda^{(s)}_{ij}$ is obviously a residue of $p^{a_{ij}-\beta_{ij}}$. Call $p^{\beta_{ij}}$ a *p-factor*, β_{ij} a *p-exponent*, $\lambda^{(s)}_{ij}$ a λ-*factor*, and $p^{a_{ij}-\beta_{ij}}$ a λ-*modulus*, of the set S.

6. Theorem 2. *If the moduli* $p^{a_{ij}}$ *satisfy* (3), *the classes of a set* S *are subject to the law of composition, if, and only if, its p-factors* $p^{\beta_{ij}}$ *satisfy the conditions*

$$\beta_{ij} \geqq \begin{cases} a_{ik} - a_{jk}, \\ a_{kj} - a_{ki} \end{cases} \qquad (i, j, k = 1, \cdots, n). \tag{5}$$

* E. g., if $a_{ik} > a_{jk}$, l_{ij} must be a multiple of $p^{a_{ik}-a_{jk}}$.

The conditions (5) for i, j fixed will be designated as $(5)_{ij}$.

Proof. By means of (4) we see that conditions (2), applied to every two equal or distinct classes in S, take the form of the congruences

$$\left.\begin{aligned} p^{a_{ij}+a_{jk}} &\equiv 0 \\ \lambda_{ij}^{(s)} p^{\beta_{ij}+a_{jk}} &\equiv 0 \\ \lambda_{jk}^{(s)} p^{a_{ij}+\beta_{jk}} &\equiv 0 \end{aligned}\right\}, \text{ mod } p^{a_{ik}} \qquad \begin{pmatrix} i, j, k=1, \cdots, n \\ s=1, \cdots, N \end{pmatrix},$$

which are equivalent to the inequalities

$$\begin{aligned} a_{ij} + a_{jk} &\geqq a_{ik}, \\ \beta_{ij} + a_{jk} &\geqq a_{ik}, \qquad (i, j, k=1, \cdots, n). \\ a_{ij} + \beta_{jk} &\geqq a_{ik}, \end{aligned}$$

If in the third inequality k is replaced by j, j by i, and i by k, it becomes $a_{ki} + \beta_{ij} \geqq a_{kj}$, which, with the second inequality, gives the required conditions.

Sets closed under composition.

7. Let S_β be the set obtained by giving to $\lambda_{ij}^{(s)}$ in (4) all integral values, mod $p^{a_{ij}-\beta_{ij}}$.

THEOREM 3. *The set S_β of classes, whose p-exponents β_{ij} satisfy* (5), *is closed under composition, if, and only if, they also satisfy the conditions*

$$\beta_{ij} + \beta_{jk} \geqq \beta_{ik} \qquad (i, j, k=1, \cdots, n). \tag{6}$$

Proof. If S_β is closed under composition, then the product

$$((l_{ij}^{(s)}))((l_{ij}^{(t)})) = ((l_{ij}^{(u)}))$$

is in S_β, when its factors are. If in the equations

$$l_{ik}^{(u)} = \sum_j l_{ij}^{(s)} l_{jk}^{(t)} \qquad \begin{pmatrix} i, k=1, \cdots, n \\ s, t=1, \cdots, N \end{pmatrix}$$

the p-factors are introduced by means of (4), they become

$$p^{\beta_{ik}} \lambda_{ik}^{(u)} = \sum_j p^{\beta_{ij}+\beta_{jk}} \lambda_{ik}^{(s)} \lambda_{ik}^{(t)} \quad (i, k=1, \cdots, n;\ s, t=1, \cdots, N),$$

which must be satisfied for integral values of $\lambda_{ik}^{(u)}$. This can happen only if (6) is satisfied. Conversely, if (6) is satisfied, S_β is closed.

The largest set S_α closed under composition.

8. Denote by α_{ij} the *smallest* value of β_{ij} which satisfies (5), i. e. for $i, j = 1, \cdots, n$,

$(7)_{ij}$ α_{ij} = the *greatest* of the $2n+1$ quantities $0, a_{ik}-a_{jk}, a_{kj}-a_{ki}$ $(k=1, \cdots, n)$. Then the set S_a of all classes $((l_{ij}^{(s)}))$, in which

$$0 \leqq l_{ij}^{(s)} < p^{a_{ij}}, \qquad l_{ij}^{(s)} \equiv 0, \mod p^{a_{ij}} \qquad (i, j=1, \cdots, n), \tag{8}$$

is the totality of all the classes to which composition applies, for given moduli $p^{a_{ij}}$ satisfying (3).

By comparing (7) and (3), we see that

$$\alpha_{ij} \leqq a_{ij} \qquad (i, j-1, \cdots, n). \tag{9}$$

THEOREM 4. *The set S_a is closed under composition.*

Proof: From $(7)_{ij}$ and $(7)_{ik}$ we have for $r = 1, \cdots, n$,

$$\alpha_{ij} \geqq a_{ir} - a_{jr}, \qquad \alpha_{jk} \geqq a_{jr} - a_{kr},$$

so that

$$\alpha_{ij} + \alpha_{jk} \geqq a_{ir} - a_{kr}.$$

Similarly

$$\alpha_{ij} + \alpha_{jk} \geqq a_{rk} - a_{ri},$$

and obviously

$$\alpha_{ij} + \alpha_{jk} \geqq 0.$$

Hence, by $(7)_{ik}$,

$$\alpha_{ij} + \alpha_{jk} \geqq \alpha_{ik}, \tag{10}$$

that is, the p-exponents of S_a satisfy (6).

The chief group.

9. The classes of S_a clearly do not form a group.* We shall prove however

THEOREM 5. *If the moduli satisfy* (3) *and the p-exponents are defined by* (7), *the totality G_a of classes of matrices $((l_{ij}^{(s)}))$ $(s = 1, \cdots, N_c)$, of elements $l_{ij}^{(s)}$ satisfying* (8) *with determinants $\Delta = |l_{ij}|$ prime to p,*

$$(\Delta, p) = 1, \tag{11}$$

form a group† G_a of order N_a.

As G_a is the largest group satisfying (11), we shall call it the *chief group of classes of congruent matrices modulo $(p^{a_{ij}})$, or the chief linear congruence group modulo $(p^{a_{ij}})$.*

* E. g., although $((l_{ij}))$, where $l_{ij}=0$ $(i, j=1, \cdots, n)$, is a class of S_a, it cannot belong to a group of order >1.

† We might also select classes, for which Δ is *divisible by* p, to form a group. E. g., with moduli all 3, the classes $L=\left(\left(\begin{smallmatrix}1&1\\1&1\end{smallmatrix}\right)\right)$ and $L^2=\left(\left(\begin{smallmatrix}2&2\\2&2\end{smallmatrix}\right)\right)=I$ form a group of order 2.

10. Proof.* (*a*) G_a is closed under composition. For, S_a is closed, and if the determinants of two matrices are prime to p, the determinant of their product is prime to p.

(*b*) The identity class I for all groups satisfying (11) is clearly $((\delta_{ij}))$, where

$$\delta_{ij} = \begin{cases} 1, & \text{if } i = j, \\ 0, & \text{if } i \neq j. \end{cases}$$

This class occurs in G_a, because by (7) we see that $\alpha_{ii} = 0$ $(i = 1, \cdots, n)$, i. e., every p factor in the axis is 1.

(*c*) Finally if $((l_{ij}))$ is any class of G_a, its inverse $((l'_{ij}))$ exists and is in G_a. For, let m_{ij} be the cofactor of l_{ij} in the expansion of $\Delta = |l_{ij}|$. Then, in view of (8), setting $l_{ij} = p^{\alpha_{ij}}\lambda_{ij}$, we write the identities

$$\sum_j l_{ij} m_{kj} = \Delta\delta_{ik} \qquad (i, k = 1, \cdots, n)$$

in the form

$$\sum_j \lambda_{ij} \cdot p^{\alpha_{ij}} m_{kj} = \Delta\delta_{ik} \qquad (i, k = 1, \cdots, n). \tag{12}$$

Now, in view of (11), there exists precisely one class $((l'_{jk}))$ satisfying the conditions

$$0 \leqq l'_{jk} < p^{\alpha_{jk}}, \qquad \Delta l'_{jk} \equiv m_{kj}, \mod p^{\alpha_{jk}} \qquad (j, k = 1, \cdots, n). \tag{13}$$

From (13), in view of (7), we have

$$\Delta p^{\alpha_{ij}} l'_{jk} \equiv p^{\alpha_{ij}} m_{kj}, \mod p^{\alpha_{ik}} \qquad (i, j, k = 1, \cdots, n),$$

where the modulus is independent of j. Therefore by substitution in (12) we have

$$\Delta \sum_j p^{\alpha_{ij}} \lambda_{ij} l'_{jk} \equiv \Delta\delta_{ik}, \mod p^{\alpha_{ik}} \qquad (i, k = 1, \cdots, n).$$

Dividing this by Δ and restoring l_{ij}, we have

$$\sum_j l_{ij} l'_{jk} \equiv \delta_{ik}, \mod p^{\alpha_{ik}} \qquad (i, k = 1, \cdots, n),$$

which shows that $((l'_{ij}))$ is the inverse of $((l_{ij}))$ and that $\Delta' = |l'_{ij}|$ is prime to p.

Further $((l'_{ij}))$ satisfies (8). For let $(i_1, i_2, i_3, \cdots, i_r)(j_1, \cdots, j_s), \cdots, (\cdots)$ be any substitution on the integers $1, 2, \cdots, n$ expressed in terms of its inde-

* The main features of the argument used in leading up to this theorem and in proving it are derived from a set of group-postulates given in lectures by MOORE in 1897. Compare also MOORE, these Transactions, vol. 3 (1902), p. 485; vol. 6 (1905), p. 179; and DICKSON, *Ibid.*, vol. 6 (1905), p. 198.

pendent cycles, and such that i_1 goes into i_2. Then by the definition of determinants

$$m_{i_1, i_2} = \sum \pm l_{i_2, i_3} \cdots l_{i_r, i_1} \prod (l_{j_1, j_2} \cdots l_{j_s, j_1}) \quad (i_1, i_2 = 1, \cdots, n),$$

where the product sign extends over all the cycles after the first, and the summation covers all the substitutions which replace i_1 by i_2. Introducing p-factors, we have

$$m_{i_1, i_2} = \sum \pm p^{\alpha_{i_2, i_3} + \alpha_{i_3, i_4} + \cdots + \alpha_{i_r, i_1}} \lambda_{i_2, i_3} \lambda_{i_3, i_4} \cdots \lambda_{i_r, i_1} \prod (l_{j_1, j_2} \cdots l_{j_2, j_1}) \quad (i_1, i_2 = 1, \cdots, n).$$

But by the repeated application of (10) we see that

$$\alpha_{i_2, i_3} + \alpha_{i_3, i_4} + \cdots + \alpha_{i_r, i_1} \geqq \alpha_{i_2, i_1},$$

and therefore that

$$m_{i_1, i_2} \equiv 0, \mod p^{\alpha_{i_2, i_1}} \quad (i_1, i_2 = 1, \cdots, n).$$

From this, by means of (13) and (9), we see that

$$l'_{ij} \equiv 0, \mod p^{\alpha_{ij}} \quad (i, j = 1, \cdots, n),$$

and consequently that $((l'_{ij}))$ satisfies (8). Hence $((l'_{ij}))$ is in S_α and, since $(\Delta', p) = 1$, it is also in G_α.

Change of nomenclature.

11. Hereafter the only classes of matrices considered will be those of S_α; and it will be convenient to regard all *congruent matrices as identical*, so that each class reduces to a single matrix, which is usually chosen so that each element is the least positive residue of its corresponding modulus. We have then in S_α a finite number of distinct matrices, one from each class, forming a closed set under composition. The law of composition will read

$$(l_{ij})(l'_{ij}) = (l''_{ij}), \qquad l''_{ik} \equiv \sum_j l_{ij} l'_{jk}, \mod p^{\alpha_{ik}} \quad (i, k = 1, \cdots, n).$$

Subgroups G_β of the chief group G_α.

12. Every linear congruence group, whose matrices satisfy the condition $(\Delta, p) = 1$, is obviously a subgroup of the chief group. This condition also shows that its p-factors $p^{\beta_{ij}}$ ($\beta_{ij} \geqq \alpha_{ij}$) cannot all be > 1; in particular, since it contains the matrix (δ_{ij}), its axial p-factors are 1, i. e., $\beta_{ii} = 0$ $(i = 1, \cdots, n)$.

Of particular interest are the subgroups whose λ-factors λ_{ij} include all integral values, mod $p^{\alpha_{ij} - \beta_{ij}}$, that satisfy (11). In regard to them, by reference to theorems 3 and 5, we immediately derive

THEOREM 6. *If the moduli satisfy* (3) *and the p-factors satisfy* (5), *the totality G_β of the matrices whose elements, of the form* (4), *satisfy* (11), *form*

a group G_β, a subgroup of the chief group G_α, if, and only if, the p-factors also satisfy (6).

Equimodular properties.

13. If two or more rows are equimodular, i. e., have identically the same moduli, and if the corresponding columns are also equimodular, the process of interchanging rows and their corresponding columns may be employed, if necessary, to juxtapose these rows and these columns. Hereafter it will be assumed, therefore, that equimodular rows and their corresponding equimodular columns are adjacent.

14. Under this arrangement every matrix will be divided into equimodular rectangles, of which those in the axis are squares. If no two rows and the corresponding columns are equimodular, each rectangle reduces to a single element. Throughout any rectangle the p-factors of the chief group are clearly equal to one another by (7). Moreover it will be convenient hereafter to restrict the application of the notation G_β to those subgroups which not only satisfy the conditions of theorem 6, but also have their p-factors p^{β_ν} equal to ane another throughout every equimodular rectangle. Therefore (§ 12) the p-factors of G_β are 1 throughout every axial square.

15. THEOREM 7. *The determinant Δ of any matrix of the set S_α is congruent, modulo p, to the product of the separate determinants of its axial squares. In particular, if no two rows and the corresponding columns are equimodular, Δ is congruent, modulo p, to the product of its axial elements.*

16. Proof. It will be sufficient to prove that if any term T of the expansion of Δ is prime to p, it is the product of elements taken entirely from the axial squares. Let $T = \pm l_{1,i_1} l_{2,i_2} \cdots l_{n,i_n}$, where $i_1, i_2, \cdots, i_n$ represent some permutation of the integers $1, 2, \cdots, n$. Denote any one of the cycles of this permutation by $(j_1, j_2, \cdots, j_r)$. Then

$$T = \pm \Pi (l_{j_1,j_2} l_{j_2,j_3} \cdots l_{j_r,j_1}),$$

where the product covers all the different cycles. Now if T is prime to p, equation (8) shows that $\alpha_{j_1 j_2} = \cdots = \alpha_{j_r j_1} = 0$. From this and (7) we derive the rn relations

$$0 \geqq a_{j_1,k} - a_{j_2,k}, \cdots, 0 \geqq a_{j_r,k} - a_{j_1,k} \qquad (k = 1, \cdots, n).$$

But these are all equations (and not inequalities), because of the identities

$$(a_{j_1,k} - a_{j_2,k}) + \cdots + (a_{j_r,k} - a_{j_1,k}) = 0 \qquad (k = 1, \cdots, n).$$

Therefore the (j_1)th, (j_2)th, $\cdots$ and (j_r)th rows are equimodular. Similarly the corresponding columns are also equimodular. Consequently the elements

$l_{j_1, j_2}, \cdots, l_{j_r, j_1}$ are all contained in the same axial square; and all the factors of T are contained in axial squares.

17. Corollary. In the matrices of the chief group *every axial square determinant must be prime to* p, and in particular, if no two rows and the corresponding columns are equimodular, every axial element must be prime to p.

Change of notation.

18. In order to take account of equimodular properties, it will be best to use a more explicit notation. Let the number of sets of equimodular rows and corresponding columns be r, and the number of rows in the first i sets be $n_i (i = 1, \cdots, r)$, so that the total number is $n_r = n$ and the number in the ith set is $n_i - n_{i-1}$, provided we define n_0 to be 0. Let (l_{μ_i, ν_j}) be a matrix and l_{μ_i, ν_j} an element in the (ij)th equimodular rectangle, taken mod $p^{\alpha_{ij}}$, where

$$\begin{cases} n_{i-1} < \mu_i \leqq n_i, & 1 \leqq i \leqq r, \\ n_{j-1} < \nu_j \leqq n_j, & 1 \leqq j \leqq r. \end{cases}$$

For any group G_β (as defined in § 14) let

$$l_{\mu_i, \nu_j} = p^{\beta_{ij}} \lambda_{\mu_i, \nu_j} \qquad (\mu_i, \nu_j = 1, \cdots, n). \tag{14}$$

Finally, let the equimodular sets be arranged so that

$$a_{ii} \geqq a_{i+1, i+1} \qquad (i = 1, \cdots, r-1).$$

Hereafter, unless otherwise stated, this notation will be used.

19. Theorem 8. *The p-exponents of any group* G_β *or* G_α *expressed in the modified notation satisfy the conditions*

$$\beta_{ij} + \beta_{ji} > 0 \qquad (i, j = 1, \cdots, n; i \neq j), \tag{15}$$

i. e., if two equimodular rectangles are symmetrically situated with respect to the axis, all the elements of at least one are divisible by p *in every matrix of the group.*

Proof. From (5) we see that

$$\begin{aligned} \beta_{ij} &\geqq a_{ik} - a_{jk}, & a_{kj} - a_{ki} \\ \beta_{ji} &\geqq a_{jk} - a_{ik}, & a_{ki} - a_{kj} \end{aligned} \qquad (k = 1, \cdots, r; i, j = 1, \cdots, r).$$

Since for any given i and j $(i \neq j)$ at least one of the above $4r$ differences is $\neq 0$, the theorem follows.

The order of a group G_β.

20. THEOREM 9. *The order N_β of a linear congruence group G_β is given by the formula*

$$N_\beta = p^{\sum_{i,j=1}^{r} (n_i - n_{i-1})(n_j - n_{j-1})(a_{ij} - \beta_{ij})} \prod_{i=1}^{r} \prod_{k=1}^{n_i - n_{i-1}} \left(1 - \frac{1}{p^k}\right). \tag{16}$$

Proof. The number of matrices in the set S_β is obviously equal to the product of the λ-moduli $p^{a_{ij}-\beta_{ij}}$. The order of G_β is obtained from this by the insertion of the proper factors as given by JORDAN's* formula, since each axial square forms a JORDAN matrix.

Factors of composition.

21. In G_β consider the totality K_β of matrices (l_{μ_i, ν_j}) which are $\equiv I$, mod $(p^{\delta_{ij}})$, i. e., in which

$$l_{\mu_i, \nu_j} \equiv \delta_{\mu_i, \nu_j}, \mod p^{\delta_{ij}} \qquad (\mu_i, \nu_j = 1, \cdots, n). \tag{17}$$

This means that in the matrices of K_β the elements in the axis are $\equiv 1$, mod p, the other elements in the axial squares are $\equiv 0$, mod p, and all the remaining elements are $\equiv 0$, mod 1, i. e., are unrestricted.

Now it is easy to see that K_β is an invariant subgroup of G_β. Moreover its order is a power of p, because the number of values of each element is a power of p and the different elements are independent of each other. It is therefore soluble.

The quotient-group G_β / K_β is evidently the *direct product of r axial square Jordan groups, each taken mod p*. Since the composition-factors of JORDAN groups are well known,† those of G_β, and therefore of G_α, are thus determined.

22. THEOREM 10. *K_β is the largest invariant subgroup of G_β whose order is a power of p.*

Proof. If there were a larger subgroup of that kind, K', and if K' contained K_β, it would correspond to an invariant subgroup of G_β / K_β of order a power of p, which would contradict the known properties of JORDAN groups; if K' did not contain K_β, it would clearly lead to a similar contradiction.

Soluble groups.

23. THEOREM 11. *The necessary and sufficient condition that a linear congruence group G_β (or G_α) be soluble is*

(a) if $p > 3$, that no two rows and the corresponding columns are equimodular,

* JORDAN, *Traité des Substitutions*, 1870, pp. 95–97.

† JORDAN, *Traité*, pp. 99–110.

(*b*) *if* $p = 2$ *or* 3, *that no three rows and the corresponding columns are equimodular.*

Proof. This follows from the fact that an n-ary JORDAN group, mod p, is soluble, if $n = 1$, and insoluble, if $n > 1$, except when $n = 2$ and $p = 2$ or 3.

Invariant matrices.

24. THEOREM 12. *If* $p > 2$, *the invariant matrices* (l_{μ_i, ν_j}) *of any group* G_β *are characterized by the congruences*

$$\left.\begin{aligned} l_{\mu_i, \nu_j} &= 0 \qquad (\mu_i \neq \nu_j) \\ l_{\mu_i, \mu_i} &\equiv l_{\nu_j, \nu_j}, \qquad \text{mod } p^{\alpha_{ij} - \beta_{ij}} \end{aligned}\right\} \qquad (\mu_i, \nu_j = 1, \cdots, n), \tag{18, 19}$$

and therefore form an axial (abelian invariant) subgroup H *of order* $p^a(p-1)$, *where* $a \geqq a_{11} - 1$.

Proof. The proof will be simplified by using the original notation of § 1. Let (l_{ij}) be an invariant matrix and (m_{ij}) be any matrix whatever of G_β, so that $(l_{ij})(m_{ij}) = (m_{ij})(l_{ij})$. Then the congruences

$$\sum_{j=1}^{n} l_{ij} m_{jk} \equiv \sum_{j=1}^{n} m_{ij} l_{jk}, \qquad \text{mod } p^{\alpha_{ik}} \qquad (i, k = 1, \cdots, n)$$

must be satisfied by every matrix (m_{ij}) of the group. These congruences may be written

$$(l_{ii} - l_{kk}) m_{ik} + l_{ik}(m_{kk} - m_{ii}) + \sum_{j}' (l_{ij} m_{jk} - m_{ij} l_{jk}) \equiv 0, \text{ mod } p^{\alpha_{ik}} \ (i, k = 1, \cdots, n), \tag{20}$$

where the $'$ on the summation sign is to indicate that $j \neq i$, $j \neq k$.

(*a*) First put $m_{ij} = 0$ $(i \neq j;\ i, j = 1, \cdots, n)$; then (m_{ij}) is axial, $m_{ii} (i = 1, \cdots, n)$ is prime to p, and (20) becomes $l_{ik}(m_{kk} - m_{ii}) \equiv 0$, mod $p^{\alpha_{ik}} (i, k = 1, \cdots, n)$. Moreover, since $p > 2$, it is possible to make $m_{kk} - m_{ii}$ prime to p, if $i \neq k$, and therefore to derive the congruences $l_{ik} \equiv 0$, mod $p^{\alpha_{ik}} (i \neq k;\ i, k = 1, \cdots, n)$, which are equivalent to the equations

$$l_{ik} = 0 \qquad (i \neq k;\ i, k = 1, \cdots, n). \tag{21}$$

By means of these equations, (20) reduces to the form $(l_{ii} - l_{kk}) m_{ik} \equiv 0$, mod $p^{\alpha_{ik}}$, which may be written $(l_{ii} - l_{kk}) p^{\beta_{ik}} \mu_{ik} \equiv 0$, mod $p^{\alpha_{ik}}$ $(i, k = 1, \cdots, n)$.

(*b*) Now choose (m_{ij}) so that μ_{ik} is prime to p; thus we derive the congruences

$$l_{ii} \equiv l_{kk}, \qquad \text{mod } p^{\alpha_{ik} - \beta_{ik}} \qquad (i, k = 1, \cdots, n). \tag{22}$$

Moreover (21) and (22) are evidently sufficient as well as necessary conditions. By change of notation they become (18) and (19).

Corollary. Since (by § 14) $\beta_{ii} = 0$ $(i = 1, \cdots, n)$, therefore in the invariant matrices *the axial elements of any axial square are equal.* Moreover, those of the ith axial square are congruent to the others, mod $p^{a_{ij}-\beta_{ij}}$ and mod $p^{a_{ji}-\beta_{ji}}(j = 1, \cdots, n)$. If we denote the greatest of the integers $a_{ij} - \beta_{ij}$, $a_{ji} - \beta_{ji}$ $(j = 1, \cdots, n)$ by a_i, then by (5) $a_i \leqq a_{ii}$. H is the direct product of a cyclic group of order $p - 1$ and an abelian group of order p^a and type $(a_{11} - 1,\ a_{22} - a_2, \cdots, a_{rr} - a_r)$. If $a_i = a_{ii}(i = 2, \cdots, n)$, *all the axial elements are equal and H is cyclic of order* $p^{a_{11}-1}(p - 1)$.

Examples.

25. Example 1. Let the modular matrix be $\left(\begin{smallmatrix} p & p^2 \\ 1 & p \end{smallmatrix}\right)$. Then the p-factors of S_a and of G_a are $\left(\begin{smallmatrix} 1 & p \\ 1 & 1 \end{smallmatrix}\right)$, the matrices of S_a are of the form $\left(\begin{smallmatrix} \lambda_{11} & p\lambda_{12} \\ 0 & \lambda_{22} \end{smallmatrix}\right)$, and they belong to G_a, if λ_{11} and λ_{22} are prime to p. The composition of matrices gives

$$\begin{pmatrix} \lambda_{11} & p\lambda_{12} \\ 0 & \lambda_{22} \end{pmatrix}\begin{pmatrix} \lambda'_{11} & p\lambda'_{12} \\ 0 & \lambda'_{22} \end{pmatrix} = \begin{pmatrix} \lambda_{11}\lambda'_{11} & p(\lambda_{11}\lambda'_{12} + \lambda_{12}\lambda'_{22}) \\ 0 & \lambda_{22}\lambda'_{22} \end{pmatrix}.$$

For the p-factors $(p^{\beta_{ij}}) = \left(\begin{smallmatrix} 1 & p^2 \\ 1 & 1 \end{smallmatrix}\right)$, the matrices of S_β and of G_β are of the form $\left(\begin{smallmatrix} \lambda_{11} & 0 \\ 0 & \lambda_{22} \end{smallmatrix}\right)$. The λ-moduli of G_a are $\left(\begin{smallmatrix} p & p \\ 1 & p \end{smallmatrix}\right)$ and its order is $p(p-1)^2$. K_a is of order p and its matrices are of the form $\left(\begin{smallmatrix} 1 & p\lambda_{12} \\ 0 & 1 \end{smallmatrix}\right)$. If ϵ is a primitive root of p, G_a is generated by the matrices $S = \left(\begin{smallmatrix} \epsilon & 0 \\ 0 & \epsilon \end{smallmatrix}\right)$ of order $p - 1$, $T = \left(\begin{smallmatrix} 1 & 0 \\ 0 & \epsilon \end{smallmatrix}\right)$ of order $p - 1$, and $U = \left(\begin{smallmatrix} 1 & p \\ 0 & 1 \end{smallmatrix}\right)$ of order p, where $T^{-1}UT = U^\epsilon$ and S is invariant. Therefore, if $p > 2$, G_a is the direct product of the cyclic group $\{S\}$ and the metacyclic group $\{T, U\}$.

Example 2. Let the modular exponents a_{ij} be

$$\begin{pmatrix} 3 & 3 & 3 \\ 1 & 2 & 2 \\ 1 & 2 & 2 \end{pmatrix}.$$

The last two rows and the last two columns are equimodular. The matrices of G_a are of the form

$$\begin{pmatrix} \lambda_{11} & p^2\lambda_{12} & p^2\lambda_{13} \\ \lambda_{21} & \lambda_{22} & \lambda_{23} \\ \lambda_{31} & \lambda_{32} & \lambda_{33} \end{pmatrix},$$

where the axial square determinants λ_{11} and $\left|\begin{smallmatrix} \lambda_{22} & \lambda_{23} \\ \lambda_{32} & \lambda_{33} \end{smallmatrix}\right|$ are prime to p. It is of order $p^{11}(p-1)^2(p^2-1)$ and is insoluble if $p > 3$. Its invariant matrices are of the form

$$\begin{pmatrix} \lambda & 0 & 0 \\ 0 & \lambda + p\mu & 0 \\ 0 & 0 & \lambda + p\mu \end{pmatrix},$$

if $p > 2$, and form a group generated by matrices of orders $p^2(p-1)$ and p.

Example 3. Let the modular exponents be

$$\begin{pmatrix} 6 & 9 & 6 \\ 3 & 5 & 5 \\ 0 & 4 & 2 \end{pmatrix}.$$

Then the p-exponents are

$$\begin{pmatrix} 0 & 4 & 6 \\ 0 & 0 & 3 \\ 0 & 3 & 0 \end{pmatrix}$$

and G_a is of order $p^{21}(p-1)^3$.

PART II.

APPLICATION TO THE GROUP OF ISOMORPHISMS OF ANY ABELIAN GROUP.

26. The great importance of the isomorphisms of a given group is largely due to the fact that they enable us to construct new groups of which the given group is an invariant sub-group. However, very little is known about isomorphisms in general, and even when the given group belongs to the simplest and most fundamental class, viz. of abelian (commutative) groups, the group of isomorphisms has not been thoroughly studied except in a few extremely special cases.

For instance, the *i-group* (group of isomorphisms) of the cyclic group has been discussed by BURNSIDE * and MILLER †. It is itself abelian. The *i*-group of the abelian group of order p^m and type $(1, 1, 1, \cdots)$ was considered by MOORE ‡, and was shown by him to be abstractly identical with the JORDAN linear congruence group, mod p.

The type $(k, 1)$ was studied by MILLER.§ The type $(2, 2)$ was treated

* BURNSIDE, *Theory of Groups of a Finite Order* (1897), pp. 239–242.

† MILLER, these Transactions, vol. 4 (1903), pp. 153–160.

‡ MOORE, Bulletin of the American Mathematical Society, ser. 2, vol. 2 (1895), pp. 33–43.

§ MILLER, these Transactions, vol. 2 (1901), pp. 259–264.

erroneously by O. E. GLENN.* The general type has been barely touched upon. Some general theorems have been proved by MILLER. †

In the present paper the general case of any abelian group of order p^m is considered. There is no loss of generality in this restriction on the order, because the i-group of an abelian group of any other order is the direct product of the i-groups of its SYLOW subgroups, whose orders are powers of primes.

The method used is a generalization of that used by MOORE for the type $(1, 1, 1, \cdots)$. The i-group is represented as a chief group of classes of congruent matrices (linear congruence group), whose moduli are the invariants of the abelian group. By means of this concrete representation of the group, some of its properties are easily found.

The abelian group A.

27. Let A be any abelian group of order p^m and of type

$$(\underbrace{a_1, \cdots, a_1}_{n_1}, \underbrace{a_2, \cdots, a_2}_{n_2-n_1}, \cdots, \underbrace{a_r, \cdots, a_r}_{n_r-n_{r-1}}). \tag{23}$$

Its invariants, $n = n_r$ in number, are divided into r sets of equal invariants, those of the ith set, $n_i - n_{i-1}$ in number, being $p^{a_i} (i = 1, \cdots, r;\ n_0 = 0)$. Suppose them arranged in decreasing order of magnitude, so that

$$a_i > a_{i+1} \qquad (i = 1, \cdots, r-1). \tag{24}$$

The order of A is equal to the product of its invariants, i. e.,

$$p^m = p^{\sum_{i=1}^{r} (n_i - n_{i-1}) a_i}. \tag{25}$$

Let $A_1, \cdots, A_n$ be a system of independent generators of A, those of order p^{a_i} being $A_{n_{i-1}+1}, \cdots, A_{\mu_i}, \cdots, A_{n_i} (i = 1 \cdots, r)$.

The group G of isomorphisms of A.

28. Let G be the i-group of A and let L be any isomorphism of A into itself. Then L must effect a correspondence between the above system of independent generators and another system $A'_1, \cdots, A'_n$, each of which is a product of powers of the original generators. In symbols, we have

$$L : A_{\mu_i} \sim A'_{\mu_i},\ A'_{\mu_i} = \prod_{j=1}^{r} \prod_{\nu_j = n_{j-1}+1}^{n_j} (A_{\nu_j})^{l_{\mu_i, \nu_j}} \quad \begin{pmatrix} \mu_i = n_{i-1}+1, \cdots, n_i \\ i = 1, \cdots, r \end{pmatrix},$$

*GLENN, American Mathematical Monthly, vol. 12, no. 11 (1905), pp. 205–207; GLENN's condition $\Delta \not\equiv 0, \bmod p^2$, is too broad, and his result for the order of the i-group is too large.

† MILLER, Annals of Mathematics, ser. 2, vol. 3 (1902), pp. 183–184.

or, more briefly,

$$L : A_{\mu_i} \sim A'_{\mu_i}, \quad A'_{\mu_i} = \prod_{\nu_j=1}^{n} (A_{\nu_j})^{l_{\mu_i, \nu_j}} \qquad (\mu_i = 1, \cdots, n). \tag{26}$$

Representation as a linear congruence group.

29. The exponents l_{μ_i, ν_j} $(\mu_i, \nu_j = 1, \cdots, n)$ in (26) may be considered as forming a matrix (l_{μ_i, ν_j}), taken modd p^{α_j} $(j = 1, \cdots, r)$.* Moreover if L' is another isomorphism defined as follows:

$$L' : A'_{\sigma_k} \sim A''_{\sigma_k}, \quad A''_{\sigma_k} = \prod_{\mu_i=1}^{n} (A'_{\mu_i})^{l'_{\sigma_k, \mu_i}} \qquad (\sigma_k = 1, \cdots, n),$$

then the product $L'L$ becomes

$$L'L : A_{\sigma_k} \sim A''_{\sigma_k}, \quad A''_{\sigma_k} = \prod_{\nu_j=1}^{n} (A_{\nu_j})^{\sum_{\mu_i=1}^{n} l'_{\sigma_k, \mu_i} l_{\mu_i, \nu_j}} \qquad (\sigma_k = 1, \cdots, n).$$

That is, the composition of the isomorphisms L and L' takes place under exactly the same law as the composition of the matrices (l'_{μ_i, ν_j}) and (l_{μ_i, ν_j}). Therefore since the isomorphisms form a group G, the matrices representing them form a linear congruence group, modd p^{α_j}, which is *abstractly identical* with G. We shall call it G.

30. Since in this case $a_{ij} = a_j$, the moduli satisfy (3). By (7) we see that α_{ij} is the greater of the quantities 0 and $a_j - a_i$, i. e., by (24),

$$\alpha_{ij} = \begin{cases} a_j - a_i, & \text{if } i > j, \\ 0, & \text{if } i \leqq j \end{cases} \qquad (i, j = 1, \cdots, r). \tag{27}$$

Therefore the elements of the matrices of G are of the form

$$l_{\mu_i, \nu_j} = \begin{cases} p^{\alpha_j - \alpha_i} \lambda_{\mu_i, \nu_j}, & \text{if } i > j, \\ \lambda_{\mu_i, \nu_j}, & \text{if } i \leqq j \end{cases} \qquad (\mu_i, \nu_j = 1, \cdots, n). \tag{28}$$

This is also easily verified by means of the fact that in the isomorphism (26), A'_{μ_i} is of order at most p^{α_i}.

31. THEOREM 13. *If an abelian group A has n invariants p^{α_j} $(j = 1, \cdots, r)$, as defined in* § 27, *its i-group G is abstractly identical with the chief n-ary linear congruence group G_α, modulis p^{α_j}.*† That is, in (28) the λ-factors can have any integral values satisfying (11).

32. Proof. (*a*) If (26) is an isomorphism, (11) is satisfied. For, since the identical isomorphism I makes every generator A_{μ_i} correspond to itself, it is represented by the matrix (δ_{μ_i, ν_j}), whose determinant is $\equiv 1$, mod p. If the

* This makes the moduli the same throughout every column.

† This is not the only representation of G as a chief linear congruence group, but it is the most convenient one.

inverse isomorphism L^{-1} is represented by the matrix (l'_{μ_i,ν_j}), it follows from $LL^{-1}=I$ that $|l_{\mu_i,\nu_j}|\cdot|l'_{\mu_i,\nu_j}|\equiv 1$, mod p, and therefore that $|l_{\mu_i,\nu_j}|$ is prime to p.

(*b*) If (26) is not an isomorphism, (11) is not satisfied, i. e., Δ is divisible by p. For, in that case, either the generators $A'_{\mu_i}(\mu_i=1,\cdots,n)$ are not independent, or for some value of μ_i, A'_{μ_i} is of order $<p^{a_i}$. In either case there is a relation of the form

$$\prod_{\mu_i=1}^{n}(A'_{\mu_i})^{p^{a'_i}h_{\mu_i}}=1, \tag{29}$$

where $h_{\mu_i}\not\equiv 0$, mod p $(\mu_i=1,\cdots,n)$, and

$$a'_i<a_i \text{ for some value of } i. \tag{30}$$

From (26), by substitution in (29), we derive

$$\prod_{\nu_j=1}^{n}(A_{\nu_j})^{\sum_{\mu_i=1}^{n}p^{a'_i}h_{\mu_i}l_{\mu_i,\nu_j}}=1,$$

and therefore also

$$\sum_{\mu_i=1}^{n}p^{a'_i}h_{\mu_i}l_{\mu_i,\nu_j}\equiv 0, \qquad \text{mod } p^{a_j} \qquad (\nu_j=1,\cdots,n),$$

which may be expanded, by (28), into the form

$$\sum_{\mu_i=1}^{n_{j-1}}p^{a'_i}h_{\mu_i}\lambda_{\mu_i,\nu_j}+\sum_{\mu_j=n_{j-1}+1}^{n_j}p^{a'_j}h_{\mu_i}\lambda_{\mu_j,\nu_j}+\sum_{\mu_i=n_j+1}^{n_r}p^{a_j-(a_i-a'_i)}h_{\mu_i}\lambda_{\mu_i,\nu_j}\equiv 0, \text{ mod } p^{a_j}. \tag{31}$$

Among the differences $a_i-a'_i$ $(i=1,\cdots,r)$ there is just one, $a_j-a'_j$, which is greater than every succeeding and less than no preceding difference. That is,

$$a_j-a'_j\begin{cases}>a_i-a'_i, & \text{if } i=j+1,\cdots,r,\\ \geqq a_i-a'_i, & \text{if } i=1,\cdots,j.\end{cases} \tag{32}$$

Then by (30),

$$a_j-a'_j>0, \tag{33}$$

and by (24) and (32),

$$a'_i-a'_j>0, \text{ if } i=1,\cdots,j-1. \tag{34}$$

Therefore in (31) every term, as well as the modulus, is divisible by $p^{a'_j}$. Dividing out this factor, we obtain

$$\sum_{\mu_i=1}^{n_{j-1}}p^{a'_i-a'_j}h_{\mu_i}\lambda_{\mu_i,\nu_j}+\sum_{\mu_j=n_{j-1}+1}^{n_j}h_{\mu_j}\lambda_{\mu_j,\nu_j}+\sum_{\mu_i=n_j+1}^{n_r}p^{(a_j-a'_j)-(a_i-a'_i)}h_{\mu_i}\lambda_{\mu_i,\nu_j}\equiv 0, \text{ mod } p^{a_j-a'_j},$$

where, by (32), (33), and (34), the modulus and all the terms except those of the middle summation are divisible by p. Therefore, by reducing the modulus to p, we obtain

$$\sum_{\mu_j=n_{j-1}+1}^{n_j} h_{\mu_j}\lambda_{\mu_j,\nu_j} \equiv 0, \mod p \qquad (\nu_j = n_{j-1}+1, \cdots, n_j),$$

which shows that the jth axial square determinant $|\lambda_{\mu_j,\nu_j}|$ is $\equiv 0$, mod p, and, by theorem 7, that the entire determinant is $\equiv 0$, mod p.

33. Evidently the following converse of theorem 13 holds:

THEOREM 14. *Every chief linear congruence group, whose moduli are the same throughout every column represents the i-group of some abelian group of order a power of p.*

Symmetry.

34. From (28) it follows that λ_{μ_i,ν_j} is taken mod p^{a_k}, where k is i or j, the greater if $i \neq j$. Hence if two equimodular rectangles are symmetrically situated with respect to the axis, the λ-factors λ_{μ_i,ν_j} and $\lambda_{\rho_j,\sigma_i}$ of their elements are *residues of the same modulus*, viz., p^{a_k}.

The order of the i-group.

35. THEOREM 15. *The order N of the i-group G of an abelian group A defined as in § 27 is given by the formula*

$$N = p^{\sum_{i=1}^{r}(n_i^2-n_{i-1}^2)a_i} \prod_{i=1}^{r}\prod_{k=1}^{n_i-n_{i-1}}\left(1-\frac{1}{p^k}\right). \tag{35}$$

Proof. This is easily derived from (16) by means of theorem 13 and § 34. Take the square common to the first i sets of rows and the first i sets of columns and subtract from it the square common to the first $i-1$ sets of rows and columns; the region remaining will contain precisely those elements, $n_i^2 - n_{i-1}^2$ in number, whose λ-factors are taken mod p^{a_i}.

Extreme cases.

36. The two opposite extremes among abelian groups A having n invariants are, (a) that in which the invariants are all distinct, (b) that in which they are all equal ($=p^a$).

(a) In this case the i-group G is soluble, because no two columns of its matrices are equimodular (although the rows are all equimodular). Its order takes the form

$$N = p^{\sum_{i=1}^{n}(2i-1)a_i}\left(1-\frac{1}{p}\right)^n. \tag{36}$$

(*b*) In this case the matrices of G reduce to a single axial square, G becomes a JORDAN group, and its order takes the form

$$N = p^{n^2\alpha} \prod_{k=1}^{n} \left(1 - \frac{1}{p^k}\right). \tag{37}$$

Since the order of A is $p^{n\alpha}$, it follows that, if p is large, the order of G is approximately equal to the nth power of the order of A.

I-groups as related to Jordan groups of the same degree.

37. As stated in the introduction to Part I, most linear congruence groups are abstractly distinct from JORDAN groups of the same degree. This will now be shown to be true of *all i-groups.*

THEOREM 16. *An i-group G of an abelian group of order p^m having n invariants, i. e., a chief n-ary linear congruence group modulis p^{a_j} $(j = 1, \cdots, r)$, is abstractly distinct from any chief n-ary Jordan group G' modulo p^a,* or subgroup thereof, if $p > n + 1$.*

Proof. A glance at the formulas for the orders of the groups shows that G cannot be abstractly identical with G' itself. If it were possible for G to be abstractly identical with a subgroup of G', its order would have to be a divisor of the order of G'; and this clearly could not happen, unless a were at least $a_r + 1$. In G consider the two matrices

$$R = \begin{Vmatrix} 1 & 0 & 0 & \cdots & 1 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & 1 \end{Vmatrix} \text{ of period } p^{a_r},$$

and

$$S = \begin{Vmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ p^{a_1-1} & 0 & 0 & \cdots & 1 \end{Vmatrix} \text{ of period } p.$$

Then we have

$$R^{-1}SR = \begin{Vmatrix} 1 - p^{a_1-1} & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & & & & \\ p^{a_1-1} & 0 & 0 & \cdots & 1 \end{Vmatrix},$$

* The trivial case $r = 1$, $a_1 = a$, $G = G'$, is left out of account.

which is different from S; hence R and S are non-commutative matrices, the product of whose periods is p^{a_r+1}. But in G' it has been shown* that for $p > n+1$ every matrix of period p^b is commutative with every matrix of period p^c, if $b + c \leqq a$. That is, if the product of the periods of two matrices in G' is p^{a_2+1}, they must be commutative. Therefore G' does not contain two non-commutative matrices of the same periods as R and S in G, and does not contain a sub-group abstractly identical with G.

If G is itself a JORDAN group, similar reasoning leads to the

Corollary. A chief n-ary JORDAN group, mod p^a, does not contain a sub-group abstractly identical with any other chief n-ary JORDAN group, mod $p^{a'}$, if $p > n+1$.

38. Since the prime factors of the order of an i-group, besides p, are factors of $p-1$, p^2-1, etc., there results immediately

THEOREM 17. *(a) Every abelian group has isomorphisms of even order. (b) If the invariants of an abelian group of order 2^m are all distinct, all its isomorphisms are of order a power of 2. (c) If an abelian group of order p^m has at least two equal invariants, it has isomorphisms whose order is divisible by 3.*

The largest invariant subgroup of order a power of p.

39. The results of Part I, §§ 21–24 can be applied immediately to i-groups and translated into the language of isomorphisms. Thus from §§ 21, 22 we derive

THEOREM 18. *In the i-group of an abelian group A the largest invariant subgroup K of order a power of p consists of the isomorphisms which transform every independent generator of A into itself multiplied by the product of any operator of lower order and any operator of the same order which is the p-th power of an operator of higher order; or, more generally, K consists of the isomorphisms which transform every operator into itself multiplied by the product of any operator of lower order and any operator of the same order which could not be used as an independent generator. Its order is equal to*

$$p^{\sum_{i=1}^{r} [(n_i^2 - n_{i-1}^2)a_i - (n_i - n_{i-1})^2]} \tag{38}$$

Soluble i-groups.

40. From § 23 we derive

THEOREM 19. *The necessary and sufficient condition that the i-group of A be soluble is*

(a) if $p > 3$, that all the invariants of A are distinct,

(b) if $p = 2$ or 3, that no three of the invariants of A are equal.

* RANUM, Bulletin of the American Mathematical Society, vol. 13 (1906–7).

Invariant isomorphisms.

41. Finally, from § 24, by identifying the $a_i\,(i = 2, \cdots, r)$ of that article with the a_i of this section, we derive

THEOREM 20. *In the i-group of A the invariant isomorphisms are those which transform every operator of A into the same power of itself.* They form a cyclic invariant subgroup of order $p^{\alpha_1-1}(p-1)$.*

Examples.

42. Example 1. Let A be an abelian group of order p^3 and type $(2, 1)$. Then any isomorphism L of A into itself may be written

$$L: \begin{cases} A_1 \sim A_1', & A_1' = A_1^{\lambda_{11}} A_2^{\lambda_{12}}, \\ A_2 \sim A_2', & A_2' = A_1^{p\lambda_{21}} A_2^{\lambda_{22}}; \end{cases}$$

and thus the i-group of A may be represented as a chief group G, mod $\left(\begin{smallmatrix} p^2 & p \\ p^2 & p \end{smallmatrix}\right)$, whose matrices are of the form $\left(\begin{smallmatrix} \lambda_{11} & \lambda_{12} \\ p\lambda_{21} & \lambda_{22} \end{smallmatrix}\right)$, where λ_{11} and λ_{22} are prime to p. Its order is $p^3(p-1)^2$. K is of order p^3 and its matrices are of the form $\left(\begin{smallmatrix} 1+p\lambda & \lambda_{12} \\ p\lambda_{21} & 1 \end{smallmatrix}\right)$. If $p > 2$ and ϵ is a primitive root of p^2, we may take as generators $R = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, of order p, $S = \left(\begin{smallmatrix} 1 & 0 \\ p & 1 \end{smallmatrix}\right)$, of order p, $T = \left(\begin{smallmatrix} \epsilon & 0 \\ 0 & \epsilon \end{smallmatrix}\right)$, of order $p(p-1)$, and $U = \left(\begin{smallmatrix} 1 & 0 \\ 0 & \epsilon \end{smallmatrix}\right)$, of order $p-1$. If ϵ is chosen so that $\epsilon^{p-1} \equiv 1 + p$, mod p^2, and if ϵ^{-1} is a root of the congruence $\epsilon x \equiv 1$, mod p^2, then the additional generational relations are $S^{-1}RS = RT^{p-1}$, $U^{-1}RU = R^{\epsilon}$, $U^{-1}SU = S^{\epsilon^{-1}}$, and T is invariant.

Since R and S are non-commutative matrices of order p, G is not abstractly identical with a subgroup of any binary JORDAN group, but, as might be expected, it is abstractly identical with the subgroup of the ternary JORDAN group modulo p, whose matrices are of the form

$$\begin{pmatrix} \alpha & \gamma & \delta \\ 0 & \beta & \epsilon \\ 0 & 0 & \alpha \end{pmatrix}.$$

Example 2. Let A be of order p^{28} and of type $(9, 9, 6, 4)$. Then the modular exponents of G are

$$\begin{Bmatrix} 9 & 9 & 6 & 4 \\ 9 & 9 & 6 & 4 \\ 9 & 9 & 6 & 4 \\ 9 & 9 & 6 & 4 \end{Bmatrix},$$

* This theorem was proved abstractly by MILLER, these Transactions, vol. 2 (1901), p. 260.

the p exponents are

$$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 3 & 3 & 0 & 0 \\ 5 & 5 & 2 & 0 \end{bmatrix},$$

and the exponents of p in the λ-moduli are

$$\begin{bmatrix} 9 & 9 & 6 & 4 \\ 9 & 9 & 6 & 4 \\ 6 & 6 & 6 & 4 \\ 4 & 4 & 4 & 4 \end{bmatrix},$$

which are clearly symmetrically situated with respect to the axis. The order of G is $p^{89}(p-1)^3(p^2-1)$ and the order of K is p^{88}.