THE STRUCTURE OF THE HYPOABELIAN GROUPS.

BY DR. L. E. DICKSON.

(Read in abstract before the Chicago Section of the American Mathematical Society, April 9, 1898.)

1. THIS paper gives a marked simplification both in the general conceptions and in the detailed developments of the theory of the two hypoabelian groups of Jordan and of the writer's generalization * to the Galois field of order 2^n of the first hypoabelian group. It is important, especially for the generalization, to give these groups an abstract definition independent of the theory of "exposants d'échange," by means of which Jordan derived them. The crucial point in the simplified treatment lies in the discovery of the explicit relations

$$\sum_{i,j}^{1\ldots m} \alpha_j^{(i)}\delta_j^{(i)} = m, \qquad \sum_{i,j}^{1\ldots m} \alpha_j^{(i)}\delta_j^{(i)} + \alpha_1' + \beta_1' + \gamma_1' + \delta_1' = m,$$

satisfied by the substitutions of the simple sub-groups J and J_1, respectively, but ruling out the remaining substitutions of the total hypoabelian groups G and G_1. We may therefore avoid the dependence made † in §§ 274 and 289 upon the last book of the Traité (see §672, page 506).

Basing the investigation upon the groups J and J_1, which are to be proved simple, and not upon G and G_1 as in the earlier treatments, we wholly avoid the delicate analysis and calculations necessary in §§275 and 290. For the first hypoabelian group, the sub-division into cases is diminished one-half. For the second hypoabelian group, decided simplifications may be made in §§284, 286–8. Some errors have been detected; thus the groups G and G_1 do not have the same order, as stated in Jordan, §279. §291 is wholly wrong.

2. The groups G and G_1 are sub-groups of the *simple* ‡

* "The first hypoabelian group generalized," *The Quarterly Journal of Mathematics*, 1898.

† The indefinite references in Jordan remained an enigma to me until quite recently. Jordan himself could not recall them upon my personal request last year.

‡ Dickson: "A triply infinite system of simple groups," *The Quarterly Journal*, July, 1897.

Abelian group H composed of the linear substitutions on $2m$ indices in the $GF[2^n]$,

$$(1)\qquad \begin{cases} \xi_i' = \sum_{j=1}^{m} (\alpha_j^{(i)} \xi_j + \gamma_j^{(i)} \eta_j), \\ \eta_i' = \sum_{j=1}^{m} (\beta_j^{(i)} \xi_j + \delta_j^{(i)} \eta_j), \end{cases} \qquad (i = 1, \cdots, m)$$

whose coefficients satisfy the relations:

$$(2)\qquad \begin{cases} \sum_{i=1}^{m} \begin{vmatrix} \alpha_j^{(i)} \gamma_j^{(i)} \\ \beta_j^{(i)} \delta_j^{(i)} \end{vmatrix} = 1, \quad \sum_{i=1}^{m} \begin{vmatrix} \alpha_j^{(i)} \gamma_k^{(i)} \\ \beta_j^{(i)} \delta_k^{(i)} \end{vmatrix} = 0, \\ \sum_{i=1}^{m} \begin{vmatrix} \alpha_j^{(i)} \alpha_k^{(i)} \\ \beta_j^{(i)} \beta_k^{(i)} \end{vmatrix} = 0, \quad \sum_{i=1}^{m} \begin{vmatrix} \gamma_j^{(i)} \gamma_k^{(i)} \\ \delta_j^{(i)} \delta_k^{(i)} \end{vmatrix} = 0, \end{cases}$$

$$(j, k = 1, \cdots, m;\ j \neq k).$$

In virtue of these relations the reciprocal* to (1) is:

$$(1)^{-1}\qquad \begin{cases} \xi_i' = \sum_{j=1}^{m} (\delta_i^{(j)} \xi_j + \gamma_i^{(j)} \eta_j) \\ \eta_i' = \sum_{j=1}^{m} (\beta_i^{(j)} \xi_j + \alpha_i^{(j)} \eta_j) \end{cases} \qquad (i = 1, \cdots, m)$$

so that we reach a set of relations (2_1) by replacing in (2) $\alpha_j^{(i)}$, $\beta_j^{(i)}$, $\gamma_j^{(i)}$, $\delta_j^{(i)}$ by respectively $\delta_i^{(j)}$, $\beta_i^{(j)}$, $\gamma_i^{(j)}$, $\alpha_i^{(j)}$.

Among the substitutions (1) occur the following (where only the indices altered are written):

$$N_{i,j,\lambda}: \quad \xi_i' = \xi_i + \lambda\eta_j,\ \xi_j' = \xi_j + \lambda\eta_i;$$
$$R_{i,j,\lambda}: \quad \eta_i' = \eta_i - \lambda\xi_j,\ \eta_j' = \eta_j - \lambda\xi_i;$$
$$Q_{i,j,\lambda}: \quad \xi_i' = \xi_i + \lambda\xi_j,\ \eta_j' = \eta_j - \lambda\eta_i;$$
$$T_{i,\lambda}: \quad \xi_i' = \lambda\xi_i, \qquad \eta_i' = \lambda^{-1}\eta_i;$$
$$P_{i,j} = (\xi_i\xi_j)(\eta_i\eta_j);\ M_iM_j = (\xi_i\eta_i)(\xi_j\eta_j).$$

PART I.—THE GROUP J, §§ 3–10.

3. Consider the group generated as follows:

$$J = \{M_iM_j,\ N_{i,j,\lambda} \quad (i, j = 1, \cdots, m;\ i \neq j)\},$$

where λ runs through all the quantities of the $GF[2^n]$. J contains $Q_{i,j,\lambda}$, the transformed of $N_{i,j,\lambda}$ by M_jM_k, and

* Jordan, § 218.

also $R_{i,j,\lambda}$, the transformed of $Q_{i,j,\lambda}$ by M_iM_k. Further, J contains the substitutions

$$P_{i,j} = Q_{j,i,1}^{-1} Q_{i,j,1} Q_{j,i,1},$$
$$T_{1,\mu}T_{2,\mu} = M_1M_2P_{1,2}R_{1,2,\mu^{-1}}N_{1,2,\mu}R_{1,2,\mu\ 1}.$$

Having $T_{1,\mu}T_{2,\mu}$, J contains its transformed by $P_{i,j}$ and hence contains the product

$$T_{1,\mu}T_{2,\mu} \cdot T_{2,\mu^{-1}}T_{3,\mu^{-1}} \cdot T_{3,\mu}T_{1,\mu} = T_{1,\mu^2}.$$

Thus if $m \geqq 3$, J contains all the substitutions

$$P_{i,j}, T_{i,\lambda}, \quad Q_{i,j,\lambda}, \quad R_{i,j,\lambda}, \quad N_{i,j,\lambda}, \quad M_iM_j.$$

4. THEOREM. *The group J consists of the totality of substitutions* (1) *which satisfy the relations** (2) *and*

$$(3) \qquad \begin{cases} \sum_{j=1}^{m} \beta_j^{(i)} \delta_j^{(i)} = 0, \quad \sum_{j=1}^{m} \alpha_j^{(i)} \gamma_j^{(i)} = 0 \quad (i = 1, \cdots, m) \\ \sum_{i,j}^{1 \ldots m} \alpha_j^{(i)} \delta_j^{(i)} = m. \end{cases}$$

First, we prove that, if Σ be a substitution (1) which satisfies the relations (2) and (3), then will also $M_rM_s\Sigma$ and $N_{r,s,\lambda}\Sigma$ satisfy them. It will then follow by induction that every substitution of J satisfies the relations. The product $N_{r,s,\lambda}\Sigma$ when expressed in the form (1) has the coefficients

$$\begin{aligned} &\bar{\alpha}_j^{(i)} = \alpha_j^{(i)}, \quad \bar{\beta}_j^{(i)} = \beta_j^{(i)} \quad (i, j = 1, \cdots, m), \\ &\bar{\gamma}_j^{(i)} = \gamma_j^{(i)}, \quad \bar{\delta}_j^{(i)} = \delta_j^{(i)} \quad (i, j = 1, \cdots, m;\ j \neq r, s), \\ &\bar{\gamma}_r^{(i)} = \gamma_r^{(i)} + \lambda\alpha_s^{(i)}, \quad \bar{\gamma}_s^{(i)} = \gamma_s^{(i)} + \lambda\alpha_r^{(i)} \\ &\bar{\delta}_r^{(i)} = \delta_r^{(i)} + \lambda\beta_s^{(i)}, \quad \bar{\delta}_s^{(i)} = \delta_s^{(i)} + \lambda\beta_r^{(i)} \end{aligned} \quad (i = 1, \cdots, m)$$

Thus $$\sum_{j=1}^{m} \bar{\alpha}_j^{(i)}\bar{\gamma}_j^{(i)} = \sum_{j=1}^{m} \alpha_j^{(i)}\gamma_j^{(i)} + \alpha_r \cdot \lambda\alpha_s + \alpha_s \cdot \lambda\alpha_r = 0,$$

$$\sum_{i,j}^{1 \ldots m} \bar{\alpha}_j^{(i)}\bar{\delta}_j^{(i)} = \sum_{i,j}^{1 \ldots m} \alpha_j^{(i)}\delta_j^{(i)} + \lambda \sum_{i=1}^{m} (\alpha_r^{(i)}\beta_s^{(i)} + \alpha_s^{(i)}\beta_r^{(i)}) = m.$$

---

* The conditions that a substitution (1) have the absolute invariant

$$\sum_{i=1}^{m} \xi_i\eta_i$$

in the $GF[2^n]$ are seen to be the relations (2) and (3), omitting the last one $\Sigma\ \alpha\delta = m$. The first hypoabelian group G is thus completely defined by the invariant $\Sigma\ \xi_i\eta_i$.

The product $M_r\Sigma$ satisfies the first set of conditions (3), but not the last one, since its coefficients $\overline{\overline{\alpha}}$, etc., give

$$\sum_{i,j}^{1\ldots m} \overline{\overline{\alpha_j^{(i)}}}\,\overline{\overline{\delta_j^{(i)}}} = \sum_{i,j}^{1\ldots m} \alpha_j^{(i)}\delta_j^{(i)} + \sum_{i=1}^{m} (\gamma_r^{(i)}\beta_r^{(i)} - \alpha_r^{(i)}\delta_r^{(i)}) = m+1.$$

But the product $M_r M_s \Sigma$ evidently satisfies all of the conditions (3), the modulus being 2.

Inversely, every substitution (1) *satisfying the relations* (2) *and* (3) *belongs to the group* J.

We first find a substitution S in J which replaces ξ_1 by

$$f_1 \equiv \sum_{j=1}^{m} (\alpha_j'\xi_j + \gamma_j'\eta_j),$$

where

$$\sum_{j=1}^{m} \alpha_j'\gamma_j' = 0.$$

If $\alpha_1' \neq 0$, we may take for S the product

$$T_{1,\alpha_1'} Q_{1,2,\alpha_2'} N_{1,2,\gamma_2'} \cdots Q_{1,m,\alpha_m'} N_{1,m,\gamma_m'}.$$

If $\alpha_1' = 0$, $\gamma_1' \neq 0$, we may choose for S

$$T_{1,\gamma_1'^{-1}} Q_{2,1,\gamma_2'} R_{1,2,\alpha_2'} \cdots Q_{m,1,\gamma_m'} R_{1,m,\alpha_m'} M_1 M_2.$$

Finally, if $\alpha_j' = \gamma_j' = 0$ $(j = 1, \cdots, k-1)$, α_k' or $\gamma_k' \neq 0$, there exists by the preceding cases a substitution S' in the group J, replacing ξ_k by f_1. We thus take $S = S'P_{1,k}$.

Thus, if Σ denote the given substitution (1), we may set $\Sigma = S\Sigma'$, where Σ' is a new substitution leaving ξ_1 fixed and, by the proof above, satisfying the relations (2) and (3). Let Σ' replace η_1 by

$$f_1' = \sum_{j=1}^{m} (\beta_j'\xi_j + \delta_j'\eta_j),$$

where by (2_1) and (3),

$$\delta_1' = 1, \quad \beta_1' + \beta_2'\delta_2' + \cdots + \beta_m'\delta_m' = 0. \tag{4}$$

A substitution in J leaving ξ_1 fixed and replacing η_1 by f_1' is given by

$$S' = R_{2,1,\beta_2'} Q_{2,1,\delta_2'} \cdots R_{m,1,\beta_m'} Q_{m,1,\delta_m'}.$$

Setting $\Sigma' = S'\Sigma_1$, Σ_1 will be a substitution leaving ξ_1 and η_1 fixed and satisfying the relations (2_1) and (3). Hence it takes the form

$$\begin{cases} \xi_1' = \xi_1, \ \xi_i' = \sum_{j=2}^{m} (\alpha_j^{(i)}\xi_j + \gamma_j^{(i)}\eta_j) \\ \eta_1' = \eta_1, \ \eta_i' = \sum_{j=2}^{m} (\beta_j^{(i)}\xi_j + \delta_j^{(i)}\eta_j) \end{cases} \quad (i = 2, \cdots, m)$$

with conditions for the coefficients analogous to (2) and (3). Proceeding similarly with Σ_1, we find ultimately that

$$\Sigma = SS' \cdots S_{m-2}S_{m-2}' T_{m,\, \alpha_m^{(m)}},$$

since a substitution altering only ξ_m and η_m and satisfying (2) and (3) is of the form $T_{m,\,\alpha}$.

COROLLARY. The substitutions $M_i = (\xi_i \eta_i)$ do not belong to the Group J.

5. The order $\Omega_{m,n}$ of J is readily determined. The number of distinct functions f_1 by which the substitutions of J can replace ξ_1 is $P_{m,n} - 1$, if $P_{m,n}$ denotes the number of solutions of

$$\sum_{j=1}^{m} \alpha_j'\gamma_j' = 0.$$

But $$\alpha_1'\gamma_1' = \lambda, \quad \alpha_2'\gamma_2' + \cdots + \alpha_m'\gamma_m' = \lambda$$

gives $(2^{n+1} - 1)P_{m-1,n}$ sets of solutions when $\lambda = 0$, and $(2^n - 1)(2^{n(2m-2)} - P_{m-1,n})$ sets of solutions when λ runs through the marks $\neq 0$ of the $GF[2^n]$. Thus

$$P_{m,n} = 2^n P_{m-1,n} + (2^n - 1)2^{n(2m-2)}.$$

By (4) the number of functions f' is $2^{n(2m-2)}$. Thus

$$\Omega_{m,n} = (P_{m,n} - 1)2^{2n(m-1)}\Omega_{m-1,n}.$$

Enumerating the substitutions of the form $T_{m,\,\alpha}$, we have

$$\Omega_{1,n} = 2^n - 1 = \tfrac{1}{2}(P_{1,n} - 1).$$

Hence

$$\Omega_{m,n,} = \tfrac{1}{2}(P_{m,n} - 1)2^{2n(m-1)}(P_{m-1,n} - 1)2^{2n(m-2)} \cdots (P_{1,n} - 1).$$

From the above investigation we derive the recursion formula

$$P_{s,n} - 1 = 2^n(P_{s-1,n} - 1) + (2^n - 1)(2^{2n(s-1)} + 1),$$

the initial term $P_{1,n} - 1$ being $2(2^n - 1)$. Then by induction we derive the result

$$P_{s,n} - 1 = (2^{ns} - 1)(2^{n(s-1)} + 1).$$

We thus obtain for the order of J the simple formula

$$\Omega_{m,n} = (2^{nm} - 1)[(2^{2n(m-1)} - 1)2^{2n(m-1)}][(2^{2n(m-2)} - 1)2^{2n(m-2)}] \cdots [(2^{2n} - 1)2^{2n}].$$

Simplicity of the group J, §§ 6–9.

6. Let I be an invariant sub-group of J not the identity. By the proof in the *Quarterly Journal*, l. c., § 4, I contains a substitution not the identity and replacing ξ_1 by $a\xi_1$. Further, if $m \geqq 3$, I contains a substitution not the identity, leaving ξ_1 and η_1 fixed. The proof differs slightly from § 5 of the paper cited. Thus, for case (1), we may suppose S_1 to be commutative with every substitution of J which leaves ξ_1, η_1, ξ_2 fixed. Equating the two values by which $S_1 R_{2,3,\lambda}$ and $R_{2,3,\lambda} S_1$ replace η_2 and the two by which they replace η_3, we have

$$\xi_3' = \delta_3'' \xi_2 + \delta_2'' \xi_3, \quad \xi_2' = \delta_2''' \xi_3 + \delta_3''' \xi_2.$$

Equating the two values by which $S_1 Q_{3,2,\lambda}$ and $Q_{3,2,\lambda} S_1$ replace ξ_3 and the two by which they replace η_2, we have

$$\xi_2' = \alpha_3''' \xi_2 + \gamma_2''' \eta_3, \quad \eta_3' = \beta_3'' \xi_2 + \delta_2'' \eta_3.$$

Applying the conditions (2) and (3), S_1 takes the form

$$S_1 \begin{cases} \xi_1' = a\xi_1, \quad \eta_1' = a^{-1}\eta_1 + \xi_2, \quad \eta_2' = a\xi_1 + \beta_2'' \xi_2 \\ \qquad\qquad\qquad\qquad\qquad\qquad + \eta_2 + \beta_2''' \xi_3 + \alpha_2''' \eta_\beta + \cdots \\ \xi_2' = \xi_2, \quad \xi_3' = \xi_3 + \alpha_2''' \xi_2, \quad \eta_3' = \eta_3 + \beta_2''' \xi_2, \cdots \end{cases}$$

where* $\beta_2'' = \alpha_2''' \beta_2''' + \beta_4'' \delta_4'' + \cdots + \beta_m'' \delta_m''$.

The demonstration may now be completed as in *The Quarterly Journal*. In the proof of case (2) we need only make the trivial variation of replacing M_3 by $M_2 M_3$ which is permissible since M_2 leaves $\xi_2 + \eta_2$ unchanged.

7. Applying again the reasoning of §6 we conclude that, if $m \geqq 4$, I contains a substitution leaving $\xi_1, \eta_1, \xi_2, \eta_2$ fixed; finally, that I contains a substitution leaving fixed

$$\xi_i, \ \eta_i \quad (i = 1, \cdots, m-2).$$

Transforming it by $P_{1,m-1} P_{2,m}$ we reach a substitution S of

* I do not find that a_2''' must be zero, so that S_1 would reduce to $T_{1,a} R_{1,2,1}$ when $m = 3$, as stated by Jordan.

I altering only $\xi_1, \eta_1, \xi_2, \eta_2$. Applying the conditions (2_1) (3) we see that it has the form

$$S: \begin{cases} \xi_1' = \alpha_1'\xi_1 + \gamma_1'\eta_1 + \alpha_2'\xi_2 + \gamma_2'\eta, & \eta_1' = \beta_1'\xi_1 + \delta_1'\eta_1 \\ & \quad + \beta_2'\xi_2 + \delta_2'\eta_2, \\ \xi_2' = \alpha_1''\xi_1 + \gamma_1''\eta_1 + \alpha_2''\xi_2 + \gamma_2''\eta_2, & \eta_2' = \beta_1''\xi_1 + \delta_1''\eta_1 \\ & \quad + \beta_2''\xi_2 + \delta_2''\eta_2. \end{cases}$$

8. *If $m > 2$, the group I contains a substitution $R_{\alpha,\,\beta,\,\rho}$.*

Case I: $\gamma_1' \neq 0$. Transform S by $T_{1,\,\gamma_1'^{-1}} R_{2,\,1,\,\alpha_2'} Q_{2,\,1,\,\gamma_2'}$ we reach a substitution S_1 in I which replaces ξ_1 by $\gamma_1'^{-1}\eta_1$ but otherwise of the same form as S.

If S_1, be commutative with M_2M_3, it reduces * to

$$T_{1,\,\gamma_1'} M_1 M_2 Q_{2,\,1,\beta_2'} R_{1,\,2,\,\beta_2'}.$$

Case (I_a): $\beta_2' = 0$. If $\gamma_1' = 1$, I contains M_1M_2 and therefore its transformed by $N_{1,\,2,\,1}\, Q_{1,\,2,\,1}$, giving $R_{1,\,2,\,1} Q_{2,\,1,\,1}$ (Case III). If $\gamma_1' \neq 1$, I contains

$$T_{1,\,\gamma_1'} M_1 M_2 \cdot P_{1,\,2}^{-1} T_{1,\,\gamma_1'} M_1 M_2 P_{1,\,2} = T_{1,\,\gamma_1'} T_{2,\gamma_2'}{}^{-1},$$

and hence its transformed by M_2M_3 giving $T_{1,\,\gamma_1'} T_{2,\,\gamma_1'}$. This in turn $R_{1,\,2,\,\lambda}$ transforms into $R_{1,\,2,\,\lambda(1+\gamma_1'^2)} T_{1,\,\gamma_1'} T_{2.\,\gamma_1'}$. Hence I contains $R_{1,\,2,\,\lambda(1+\gamma_1'^2)} \neq 1$.

Case (I_b): $\beta_2' \neq 0$. If $n > 1$, a mark $\rho \neq 1, \neq 0$ exists. The transformed of S_1 by $T_{2,\,\rho}$ will not be commutative with M_2M_3. If $n = 1$, I contains

$$(M_1M_2Q_{2,\,1,\,1}R_{1,\,2,\,1})^{-1} P_{1,\,2} M_1 M_2 Q_{2,\,1,\,1} R_{1,\,2,\,1} P_{1,\,2} = P_{1,\,2} Q_{2,\,1,\,1},$$

when by Jordan, p. 204, ll. 15–17, I contains $Q_{3,\,1,\,1}$.

If, however, S_1 be not commutative with M_2M_3, I contains $S_1^{-1} M_2M_3S_1M_2M_3 \neq 1$ which leaves ξ_1, ξ_3, η_3 fixed (Case III.).

Case II. $\gamma_1' = 0$, α_2' and γ_2' not both zero.

J contains a substitution T leaving ξ_1 fixed and replacing ξ_2 by

$$\alpha_1'\xi_1 + \gamma_1'\eta_1 + \alpha_2'\xi_2 + \gamma_2'\eta_2;$$

viz, if $\alpha_2' \neq 0$, $T \equiv T_{2,\,\alpha_2'} Q_{2,\,1,\,\alpha_1'}$;

while, for $\gamma_2' \neq 0$, $T \equiv M_2M_3 T_{2,\,\gamma_2'} Q_{2,\,1,\,\alpha_1'}$.

Hence $S_1 \equiv T^{-1}ST$ replaces ξ_1 by ξ_2 and leaves ξ_3, η_3 fixed.

If S_1 be not commutative with $R_{1,\,2,\,\lambda}$, I contains

$$S_1^{-1} R_{1,\,2,\,\lambda} S_1 R_{1,\,2,\,\lambda} \neq 1$$

which leaves ξ_1 fixed (Case III.).

* I do not find that β_2' must $= 0$ as stated in Jordan, p. 204, l. 1.

If S_1 be commutative with $R_{1,2,\lambda}$ it reduces to

$$P_{1,2}Q_{2,1,\delta_1'}R_{1,2,\beta_1'}.$$

Then I contains

$$P_{1,2}S_1\,P_{1,2}S_1^{-1} = Q_{2,1,\delta_1'}Q_{1,2,\delta_1'}.$$

But, when $\delta_1' = 0$, I contains $P_{1,2}R_{1,2,\beta_1'}$ whose transformed by $Q_{1,2,1}$ leaves ξ_1 fixed (Case III.).

If $\delta_1' = 1$, I contains

$$Q_{2,1,1}Q_{1,2,1} \equiv P_{1,2}Q_{2,1,1},$$

when, as in Case (I_b), I contains $Q_{3,1,1}$.

If $\delta_1' \neq 0, \neq 1$, the transformed of $Q_{2,1,\delta_1'}Q_{1,2,\delta_1'}$ by $T_{1,\rho}$ gives $Q_{2,1,\delta\rho^{-1}}Q_{1,2,\delta\rho}$, so that I contains

$$Q_{2,1,\delta\rho^{-1}}Q_{1,2,\delta\rho}\cdot Q_{2,1,\delta\sigma^{-1}}Q_{1,2,\delta\sigma},$$

which, for $\sigma = \rho(1+\delta^2) \neq 0$, reduces to

$$T_{1,1+\delta^2}T_{2,1+\delta^2}^{-1}.$$

Case III. $\gamma_1' = \alpha_2' = \gamma_2' = 0$.

We may verify in detail that S reduces to

$$T_{1,\alpha_1'}R_{1,2,\beta_2'}Q_{2,1,\delta_2'}T_{2,\alpha_2''}.$$

Transforming this by $T_{2,\alpha_2''}^{-1}R_{1,2,\lambda}$, we obtain

$$R_{1,2,\lambda(1+\alpha_1'\alpha_2'')}T_{1,\alpha_1'}T_{2,\alpha_2''}R_{1,2,\beta_2'}Q_{2,1,\delta_2'}.$$

Thus if $\alpha_1'\alpha_2'' \neq 1$, I contains $R_{1,2,\lambda(1+\alpha_1'\alpha_2'')} \neq 1$.

For $\alpha_2'' = \alpha_1'^{-1}$, I contains [writing α for α_1' and dropping affixes]

$$S = R_{1,2,\alpha\beta}Q_{2,1,\alpha\delta}T_{1,\alpha}T_{2,\alpha}^{-1},$$

$$P_{1,2}T_{2,\alpha}^{-1}ST_{2,\alpha}P_{1,2} = T_{1,\alpha^{-1}}T_{2,\alpha}R_{1,2,\beta}Q_{1,2,\delta}.$$

Hence I contains their prodnct

$$W \equiv R_{1,2,\beta(1+\alpha)}Q_{2,1,\alpha\delta}Q_{1,2,\delta}.$$

Transforming W by M_1 M_3 and the result by $P_{1,2}$, we obtain respectively,

$$Q_{1,2,\beta(1+\alpha)}N_{1,2,\alpha\delta}R_{1,2,\delta}, \quad Q_{2,1,\beta(1+\alpha)}N_{1,2,\alpha\delta}R_{1,2,\delta}.$$

Hence I contains

$$Q_{2,1,\beta(1+\alpha)}\,Q_{1,2,\beta(1+\alpha)}.$$

Thus if $\beta(1+\alpha) \neq 0$, I contains some $R_{1,2,\rho}$ [see end of Case II]. If $\beta(1+\alpha) = 0$, the transformed of W by $T_{1,\alpha^{1/2}}$ gives

$$Q_{2,1,\delta\alpha^{1/2}}\,Q_{1,2,\delta\alpha^{1/2}},$$

so that we reach an $R_{1,2,\rho}$ unless $\delta = 0$. But for $\delta = 0$, $\beta(1+\alpha) = 0$, S reduces to $R_{1,2,\beta}$ or $T_{1,\alpha}\,T_{2,\alpha,}{}^{-1}$ giving in either case an $R_{1,2,\rho}$.

9. Having a substitution of the form $R_{a,b,\rho}$, I will contain its transform by $T_{a,\lambda}$, giving $R_{a,b,\rho\lambda^{-1}}$. Thus I contains $R_{a,b,\lambda}$ (λ = arbitrary). Transforming it by $P_{j,b}P_{a,i}$ we reach $R_{i,j,\lambda}$. This M_iM_k transforms into $Q_{i,j,\lambda}$, which in turn M_jM_k transforms into $N_{i,j,\lambda}$. Finally, $Q_{1,2,1,}N_{1,2,1,}$ transforms $R_{1,2,1}\,Q_{2,1,1}$ into M_1M_2. Hence I coincides with J, which is, therefore, a *simple group*.

10. For $m = 2$, we may define the sub-group J of index 2 as follows:

$$J = \{M_1M_2,\ N_{1,2,\lambda},\ Q_{1,2,\lambda},\ T_{1,\lambda}\};$$

for it then contains also the substitutions

$$R_{1,2,\lambda} = M_1M_2N_{1,2,\lambda}M_1M_2,$$
$$Q_{2,1,1} = R_{1,2,1}Q_{1,2,1}N_{1,2,1}M_1M_2N_{1,2,1}Q_{1,2,1},$$
$$P_{1,2} = Q_{2,1,1}Q_{1,2,1}Q_{2,1,1}.$$

The order of J is seen to be

$$\tfrac{1}{2}(P_{2,n}-1)\,2^{2n}\,(P_{1,n}-1) = \{2^n(2^{2n}-1)\}^2.$$

PART II.—THE GROUP J_1,* §§ 11–21.

11. Confining ourselves to the $GF[2^1]$, consider the first hypoabelian group J' on the indices $x_2, \cdots, x_m$. Denote by J_1 the group obtained by extending J' by the three substitutions M_1M_2, L_1M_1, U, viz.:

$$L_1M_1:\ x_1' = y_1,\quad y_1' = x_1 + y_1.$$

$$U:\begin{cases} x_1' = x_2 + y_2, & y_1' = y_1 + y_2, \\ x_2' = x_1 + x_2 + y_2, & y_2' = x_1 + y_1 + x_2 + y_2. \end{cases}$$

* J_1 is a sub-group of the Abelian Group (for $p=2$); for

$$U = P_{1,2}L_1Q_{2,1,1}L_2'.$$

12. THEOREM: *Every substitution* of J_1 is included among the linear substitutions*

$$(1)\qquad \begin{cases} x_i' = \sum_{j=1}^{m} (a_j^{(i)} x_j + c_j^{(i)} y_j) \\ y_i' = \sum_{j=1}^{m} (b_j^{(i)} x_j + d_j^{(i)} y_j) \end{cases} \qquad (i = 1 \cdots m)$$

whose coefficients, taken modulo 2, satisfy the relations:†

$$(5)\qquad \sum_{j=1}^{m} a_j^{(i)} c_j^{(i)} + a_1^{(i)} + c^{(i)} \equiv \sum_{j=1}^{m} b_j^{(i)} d_j^{(i)} + b_1^{(i)} + d_1^{(i)} \equiv \delta_{1i}, \qquad (i = 1, \cdots, m)$$

$$(6)\qquad \sum_{i,j}^{1 \cdots m} a_j^{(i)} d_j^{(i)} + a_1' + b_1' + c_1' + d_1' \equiv m,$$

in addition to the relations (2) [*when written in roman letters*]. Writing the relations (5) for the reciprocal of (1) we have

$$(5_1)\qquad \sum_{j=1}^{m} a_i^{(j)} b_i^{(j)} + a_1^{(j)} + b_1^{(j)} \equiv \sum_{j=1}^{m} c_i^{(j)} d_i^{(j)} + c_1^{(j)} + d_1^{(j)} \equiv \delta_{1i},$$

which must be a consequence of the relations (5) and (2).

Since the theorem is true for $L_1 M_1$, U and the substitutions of J' [see § 4], it follows by induction if we prove that, when any substitution Σ satisfies the above relations, $U\Sigma$ and $L_1 M_1 \Sigma$ also satify them.

Expressing $L_1 M_1 \Sigma$ in the form (1), it is seen to have the coefficients $\bar{a}_j^{(i)}$, $\bar{b}_j^{(i)}$, etc., where

$$\bar{a}_1^{(i)} = c_1^{(i)}, \quad \bar{c}_1^{(i)} = a_1^{(i)} + c_1^{(i)}, \quad \bar{b}_1^{(i)} = d_1^{(i)}, \quad \bar{d}_1^{(i)} = b_1^{(i)} + d_1^{(i)},$$
$$\bar{a}_j^{(i)} = a_j^{(i)}, \quad \bar{c}_j^{(i)} = c_j^{(i)}, \quad \bar{b}_j^{(i)} = b_j^{(i)}, \quad \bar{d}_j^{(i)} = d_j^{(i)} \quad (j = 2, \cdots, m).$$

The expression on the left of (6), when built in $\bar{a}_j^{(i)}$, $\bar{b}_j^{(i)}$, etc., reduces to m, on applying (6), in virtue of the relations

$$\sum_{i=1}^{m} c_1^{(i)} b_1^{(i)} = \sum_{i=1}^{m} a_1^{(i)} d_1^{(i)} + 1, \quad \sum_{i=1}^{m} c_1^{(i)} d_1^{(i)} + c_1' + d_1' = 1.$$

---

* The conditions that (1) shall leave

$$x_1 + y_1 + \sum_{i=1}^{m} x_i y_i$$

invariant modulo 2 are seen to be the relations (2) and (5). This invariant thus characterizes the second hypoabelian group G_1.

† Following Kronecker's notation,

$$\delta_{11} = 1, \quad \delta_{1i} = 0 (i \neq 1).$$

Similarly, $U\Sigma$ has the coefficients

$$\bar{a}_1^{(i)} = a_2^{(i)} + c_2^{(i)}, \quad \bar{c}_1^{(i)} = c_1^{(i)} + c_2^{(i)},$$

$$\bar{b}_1^{(i)} = b_2^{(i)} + d_2^{(i)}, \quad \bar{d}_1^{(i)} = d_1^{(i)} + d_2^{(i)},$$

$$\bar{a}_2^{(i)} = a_1^{(i)} + a_2^{(i)} + c_2^{(i)}, \quad \bar{c}_2^{(i)} = a_1^{(i)} + a_2^{(i)} + c_1^{(i)} + c_2^{(i)},$$

$$\bar{b}_2^{(i)} = b_1^{(i)} + b_2^{(i)} + d_2^{(i)}, \quad \bar{d}_2^{(i)} = b_1^{(i)} + b_2^{(i)} + d_1^{(i)} + d_2^{(i)},$$

$$\bar{a}_j^{(i)} = a_j^{(i)}, \quad \bar{b}_j^{(i)} = b_j^{(i)}, \quad \bar{c}_j^{(i)} = c_j^{(i)}, \quad \bar{d}_j^{(i)} = d_j^{(i)} \quad (j = 3, \cdots, m).$$

Thus

$$\sum_{i=1}^{m} (\bar{a}_1^{(i)}\bar{d}_1^{(i)} + \bar{a}_2^{(i)}\bar{d}_2^{(i)})$$

equals

$$\sum_{i=1}^{m} (a_1^{(i)}b_1^{(i)} + a_2^{(i)}b_2^{(i)} + a_1^{(i)}d_1^{(i)} + b_2^{(i)}c_2^{(i)})$$

$$+ \sum_{i=1}^{m} (a_1^{(i)}b_2^{(i)} + a_2^{(i)}b_1^{(i)}) + \sum_{i=1}^{m} (a_1^{(i)}d_2^{(i)} + b_1^{(i)}c_2^{(i)}).$$

The last two sums being zero, this reduces to

$$a_1' + b_1' + 1 + a_2' + b_2' + \sum_{i=1}^{m} (a_1^{(i)}d_1^{(i)} + a_2^{(i)}d_2^{(i)}) + 1.$$

Also

$$\bar{a}_1' + \bar{b}_1' + \bar{c}_1' + \bar{d}_1' = a_2' + c_1' + b_2' + d_1'.$$

Hence $U\Sigma$ satisfies the relation (6). A like result may be proven for the relations (2) and (5). Hence the substitutions (1) satisfying the relations (2), (5), (6) form a *group*. This abstract definition of our group is independent of Jordan's theory of "exposants d'échange," from which also the group property follows.

13. It is interesting to note that it is impossible to generalize to the $GF[2^n]$, $n > 1$, the group of substitutions (1) satisfying the relations (2), (5), (6).

Thus, the coefficients of $L_1 M_1 \Sigma$ satisfy (5) only if

$$(c_1^{(i)})^2 + c_1^{(i)} = 0, \quad (d_1^{(i)})^2 + d_1^{(i)} = 0,$$

i. e., if $c_1^{(i)}$ and $d_1^{(i)}$ belong to the $GF[2^1]$. Similarly, by considering $M_1 L_1 \Sigma$, we find that $a_1^{(i)}$ and $b_1^{(i)}$ must be integers. Likewise the coefficients of $U\Sigma$ satisfy (5) only when

$$(a_1^{(i)})^2 + a_1^{(i)} + (a_2^{(i)})^2 + a_2^{(i)} = 0,$$

i. e., if $a_2^{(i)}$ also belongs to the $GF[2^1]$. By considering $P_{23} U P_{23} \Sigma$, we find that $a_3^{(i)}$ must be integers, etc.

Further no generalization is gained by extending J' by* $L_{1,\lambda}M_1$, since $L_{1,}{}'_{\lambda}L_{1,\ 1}L_{1,}{}'_{\lambda}$ satisfies (5) only when $\lambda = 1$.

14. *Inversely, every linear substitution* (1), *satisfying the relations* (2), (5), (6), *belongs to the group* J_1. The proof varies only slightly from Jordan, §§ 279–281. At the end of § 279, we replace the three products by

$$S'UM_1M_2, \quad S'M_1M_3UM_1M_3, \quad L_1M_1S'UM_1M_2,$$

where S' is the substitution in J' which replaces y_2 by

$$\sum_{j=2}^{m}(a_j'x_j + c_j'y_j).$$

If $a_j' = c_j' = 0$ $(j = 2 \cdots m)$ we take for S respectively:

$$L_1M_1,\ 1,\ L_1M_1 \cdot M_1M_2.$$

At the end of §280, we take for S',

$$\overline{S}M_1L_1U^2 \text{ or } \overline{S}M_1M_3U^3,$$

according as $b_1' = 1$ or 0.

15. The order Ω_m' of the second hypoabelian group J_1 is not equal to the order Ω_m of the first hypoabelian group $J_{n=1}$ as stated by Jordan, § 279. In § 282 the reference should be to § 259 and not to § 260. Thus the number of solutions of

$$\sum_{j=2}^{m}a_j'c_j' + (a_1' + 1)\ (c_1' + 1) = 0$$

is $$P_m \equiv 2^{2m-1} + 2^{m-1}.$$

Hence $$\Omega_m' = 2P_mP_{m-1}\Omega_{m-1},$$

where $\Omega_{m-1} = (2^{m-1}-1)\ (2^{2m-4}-1)2^{2m-4}\cdots(2^2-1)2^2$.

The order of the group J_1 is thus

$$\Omega_m' \equiv (2^m+1)\ (2^{2m-2}-1)2^{2m-2}(2^{2m-4}-1)2^{2m-4}\cdots(2^2-1)2^2.$$

Simplicity of J_1, §§ 16–20.

16. In the main, I will follow Jordan's developments in §§ 283–86, but will replace §§ 287–89, in which a couple of small errors occur, by a simpler method, and finally wholly avoid the elaboration left to the reader in § 290.

In § 283 the treatment of the case $c_1' = 0$ will not verify.†

* For the notation see *The Quarterly Journal*, July, 1897.

† A simple correction suffices for Jordan's proof. Thus, I contains $S^{-1}L_1{}'^{-1}SL_1'$ which leaves x_1 fixed and reduces to the identity only when S itself leaves x_1 fixed.

If $a_j' = c_j' = 0 (j = 2 \cdots m)$, S leaves x_1 fixed. In the contrary case, we may suppose, for example, that $a_3' = 1$. We may thus suppose that $a_2' = c_2'$; for, if not, the transformed of S by $N_{2,3}$ replaces x_1 by

$$a_1'x_1 + a_2'x_2 + (c_2' + a_3')y_2 + a_3'x_3 + (c_3' + a_2')y_3 + \cdots$$

in which the coefficients of x_2 and y_2 are equal. Thus I contains the substitution leaving x_1 fixed

$$S_1 = S^{-1}(M_1L_1)M_1M_2SM_1M_2(L_1M_1).$$

If S_1 is the identity, on comparing the values by which S and $M_1L_1M_1M_2SM_1M_2L_1M_1$ replace y_1, we find that

$$x_1' = (b_2' + d_2')(x_2 + y_2) + d_1'x_1,$$

where by the relations (5),

$$(b_2' + d_2')^2 + d_1' = 1.$$

Since S does not leave x_1 fixed, it replaces x_1 by $x_2 + y_2$. Hence I contains $\overline{S}$, the transformed of S by $N_{2,3}$, which replaces x_1 by $x_2 + y_2 + y_3$. Using this $\overline{S}$ in place of the former S, the product denoted by S_1 will not be the identity and will leave x_1 fixed.

17. We proceed as in § 284, where the greater part of case 3° may be deleted. Indeed, the substitution S_1 given at the top of p. 210 is not hypoabelian; for a substitution replacing y_2 by $x_1 + y_2 + \beta(x_2 + x_3 + y_3)$ does not satisfy the relation (5),

$$0 = \sum_{j=1}^{m} \beta_j''\delta_j'' + \beta_1'' + \delta_1'' \equiv \beta + \beta^2 + 1 = 1.$$

18. As in § 285, I contains the substitution

$$A = [(P_{2,3}Q_{3,2})^{-1}(M_1M_3R_{2,3}Q_{3,2})^{-1}P_{2,3}Q_{3,2}(M_1M_3R_{2,3}Q_{3,2})]^2$$

which, on expansion, becomes

$$A: \begin{cases} x_2' = y_2, & y_2' = x_2 + y_2 + x_3 + y_3, \\ x_3' = y_2 + y_3, & y_3' = y_2 + x_3. \end{cases}$$

The substitutions $B \equiv B^{-1}$ and C of Jordan, p. 210, are seen to belong to our group J_1. Thus I contains

$$A^2 \cdot B^{-1}AB \equiv X: \begin{cases} x_1' = x_1, & y_1' = x_1 + y_1 + x_3, \\ x_2' = y_2, & y_2' = x_2, \\ x_3' = x_3, & y_3' = x_1 + x_3 + y_3. \end{cases}$$

Hence I contains $M_1M_2XM_1M_2 \equiv M_1XM_1$ and, therefore, also $A^{-1}M_1M_2(M_1XM_1)M_2M_1A$ which gives the substitution

$$Y: \begin{cases} x_1' = x_1, \quad x_2' = x_2 + y_2 + x_3 + y_3, \quad x_3' = x_1 + x_2 + y_2, \\ y_1' = x_1 + y_1 + x_2 + y_3, \quad y_2' = x_1 + x_2 + y_2 + y_3, \\ y_3' = y_2 + x_3. \end{cases}$$

Hence I contains the substitutions

$$Z \equiv (M_2M_3P_{2,3})^{-1}YM_2M_3P_{2,3} \cdot Y \equiv Q_{3,2}M_2M_3P_{2,3},$$

$$B \equiv C^{-1}ZC \cdot Y,$$

$$Z[(P_{2,3}Q_{2,3})^{-1}Z(P_{2,3}Q_{2,3}) \cdot B]^3 = Q_{3,2}(Q_{2,3}B)^3 = Q_{3,2},$$

as seen by a simple reduction using the fact that B is commutative with $M_2M_3P_{2,3}$.

Containing $Q_{3,2}$, I contains all the substitutions of J' (see §§ 3 and 9).

19. The substitution $(UM_2)^2M_1M_3P_{2,3}$ transforms $N_{2,3}$ into $G \equiv G^{-1}$ (Jordan, bottom of p. 211).

The group J_1 contains the substitution *

$$U_1 \equiv U_1^{-1} \begin{cases} x_1' = y_2 + x_3 + y_3, \quad y_1' = x_2 + y_2, \\ x_2' = x_1 + y_1 + x_3 + y_3, \quad y_2' = x_1 + x_3 + y_3, \\ x_3' = y_1 + x_2 + y_2 + x_3, \quad y_3' = y_1 + x_2 + y_2 + y_3. \end{cases}$$

But U_1 transforms M_2M_3, $N_{2,3}R_{2,3}Q_{2,3}N_{2,3}$, and $N_{2,3}$ into respectively L_1M_3, $M_1M_2Q_{3,2}N_{2,3}$ and F (bottom of p. 211). Hence I contains M_1M_2 and, therefore, M_1M_3 and consequently the products:

$$L_1M_3 \cdot M_3M_1 = L_1M_1,$$

$$P_{2,3}FP_{2,3} \cdot M_1M_2 \cdot G \cdot M_1M_3 \cdot Q_{2,3}N_{2,3} = U.$$

Hence I coincides with J_1, which is, therefore, *simple.*

20. *For* $m = 2$, J_1 *is of order* 60 *and is generated by* †

$$M_1M_2, \ L_1M_1, \ U, \ M_1UM_1.$$

We proceed as in Jordan, § 279. If $a_2'c_2' = 1$, U will replace x_1 by $f_1 = x_2 + y_2$. If $a_2'c_2' = 0$, we have three cases:

(1) $$a_2' = 0, \ c_2' = 1.$$

* write U_1 for the French capital U (p. 211, l. 13).

† We may drop M_1UM_1 from the list of generators; for,

$$U \cdot M_1UM_1 = L_1M_1 \cdot M_1M_2$$

Then will

$$UM_1M_2,\ M_1UM_1,\ \text{or}\ L_1M_1UM_1M_2.$$

replace x_1 by f_1, according as respectively,

$$a_1' = 0,\ c_1' = 1;\ a_1' = 1,\ c_1' = 0;\ \text{or}\ a_1' = c_1' = 1.$$

(2) $$a_2' = 1,\ c_2' = 0.$$

We choose respectively

$$M_2M_1 \cdot M_1UM_1,\ M_1M_2UM_1M_2,\ L_1M_1 \cdot M_2M_1 \cdot M_1UM_1.$$

(3) $$a_2' = c_2' = 0.$$

We take respectively

$$L_1M_1,\ 1,\ L_1M_1 \cdot M_1M_2.$$

Continuing as in Jordan, § 280, we seek a substitution S, which replaces y_1 by $b_1'x_1 + y_1 + b_2'x_2 + d_2'y_2$, where $b_2'd_2' = 0'$ without altering x_1.

(1) $$b_2' = d_2' = 0.$$

According as $b_1' = 0$ or 1, we take

$$S' = 1 \text{ or } M_1M_2 \cdot L_1M_1.$$

(2) $$b_2' = 1,\ d_2' = 0.$$

We take respectively

$$S' = (M_1UM_1)^2M_1M_2 \text{ or } M_1L_1U^2.$$

(3) $$b_2' = 0,\ d_2' = 1$$

We choose respectively

$$S' = M_1M_2U^2 \text{ or } M_1L_1 \cdot M_1M_2(M_1UM_1)^2M_1M_2.$$

Since no power of M_1UM_1 reduces to U, which is of period 5, J_1 contains more than one cyclical sub-group of order 5. Hence* J_1 is *simple*. To put it into the form of the icosahedral group, we may set

$$S_2 \equiv UM_1M_2,\ S_3 \equiv UM_1UM_2 = L_1M_1,\ S_5 = M_2U^{-1}M_2,$$

where S_j is of period j. It follows that $S_2S_3S_5 = 1$.

21. We have reached the interesting result that the simple group J_1 on m indices is obtained by extending the group

* Burnside: The Theory of Groups, pp. 107–8. The statements of Jordan § 291 are thus wholly wrong.