The Structure of certain Linear Groups with Quadratic Invariants. By L. E. DICKSON, Ph.D. Received September 1st, 1898. Communicated by Prof. E. H. MOORE, November 10th, 1898.

1. Consider the group $L_{m,n,p}$ of all linear substitutions

$$(1) \quad \left\{ \begin{array}{l} \xi'_i = \sum_{j=1}^m (\alpha_{ij} \xi_j + \gamma_{ij} \eta_j) \\ \eta'_i = \sum_{j=1}^m (\beta_{ij} \xi_j + \delta_{ij} \eta_j) \end{array} \right\} \quad (i = 1, \dots, m)$$

in the $GF[p^n]^*$ which have the absolute invariant

$$\xi_1 \eta_1 + \xi_2 \eta_2 + \dots + \xi_m \eta_m.$$

The conditions thus imposed upon the coefficients are

$$(2) \quad \left\{ \begin{array}{ll} \sum_{i=1}^m \alpha_{ij} \beta_{ij} = 0, & \sum_{i=1}^m \gamma_{ij} \delta_{ij} = 0 \\ \sum_{i=1}^m (\alpha_{ij} \beta_{ik} + \alpha_{ik} \beta_{ij}) = 0, & \sum_{i=1}^m (\gamma_{ij} \delta_{ik} + \gamma_{ik} \delta_{ij}) = 0 \\ \sum_{i=1}^m (\alpha_{ij} \delta_{ik} + \beta_{ij} \gamma_{ik}) = 0, & \sum_{i=1}^m (\alpha_{ij} \delta_{ij} + \beta_{ij} \gamma_{ij}) = 1 \end{array} \right\}$$

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

The inverse of the substitution (1) of the group $L_{m,n,p}$ is

$$(1)_{-1} \quad \left\{ \begin{array}{l} \xi'_i = \sum_{j=1}^m (\delta_{ji} \xi_j + \gamma_{ji} \eta_j) \\ \eta'_i = \sum_{j=1}^m (\beta_{ji} \xi_j + \alpha_{ji} \eta_j) \end{array} \right\} \quad (i = 1, \dots, m).$$

Indeed, the product (1) $(1)_{-1}$ replaces ξ_k by

$$\sum_{i=1}^m \left\{ \sum_{j=1}^m (\alpha_{ji} \delta_{jk} + \beta_{ji} \gamma_{jk}) \xi_i + \sum_{j=1}^m (\gamma_{ji} \delta_{jk} + \gamma_{jk} \delta_{ji}) \eta_i \right\} \equiv \xi_k.$$

Further, (1) and its inverse have the same determinant ± 1 . In fact, if we reflect on the main diagonal the determinant of $(1)_{-1}$, and then

[* For the abstract theory of the Galois field of order p^n , denoted by the symbol $GF[p^n]$, we refer to the paper by Prof. Moore in the *Congress Mathematical Papers* of 1893.]

interchange the first and second, the third and fourth, &c., rows as well as columns, we obtain the determinant of the substitution (1).

Denote by (2)₋₁ the relations obtained from (2) [and equivalent to them] by replacing α_{ij} , β_{ij} , γ_{ij} , δ_{ij} , by δ_{ji} , β_{ji} , γ_{ji} , α_{ji} respectively.

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

$$\begin{aligned} W_{i,j,\lambda} : \quad \xi'_i &= \xi_i + \lambda \eta_j, & \xi'_j &= \xi_j - \lambda \eta_i; \\ V_{i,j,\lambda} : \quad \eta'_i &= \eta_i + \lambda \xi_j, & \eta'_j &= \eta_j - \lambda \xi_i; \\ Q_{i,j,\lambda} : \quad \xi'_i &= \xi_i + \lambda \xi_j, & \eta'_j &= \eta_j - \lambda \eta_i; \\ T_{i,\lambda} : \quad \xi'_i &= \lambda \xi_i, & \eta'_i &= \lambda^{-1} \eta_i; \\ P_{ij} &= (\xi_i \xi_j)(\eta_i \eta_j); & S_{ij} &= (\xi_i \eta_i)(\xi_j \eta_j). \end{aligned}$$

2. THEOREM.—*The substitutions of the above types generate a sub-group $L'_{m,n,p}$ of index 2 under $L_{m,n,p}$, the former being extended to the latter by the substitution $(\xi_i \eta_i)$. $L'_{m,n,p}$ contains, for $p > 2$, all the substitutions of $L_{m,n,p}$ of determinant $+1$; for $p = 2$, all satisfying* the relation in the GF $[2^n]$,*

$$\sum_{i,j}^{1,\dots,m} \alpha_{ij} \delta_{ij} = m.$$

Let Σ be an arbitrary substitution (1) of $L_{m,n,p}$. We first find a substitution S derived from the above $W_{i,j,\lambda}$, &c., which (like Σ) replaces ξ_i by

$$f_i \equiv \sum_{j=1}^m (\alpha_{ij} \xi_j + \gamma_{ij} \eta_j),$$

where, by (2)₋₁,

$$\sum_{j=1}^m \alpha_{ij} \gamma_{ij} = 0.$$

(a) If $\alpha_{11} \neq 0$, we may take for S the product

$$T_{1,\alpha_{11}} Q_{1,2,\alpha_{12}} W_{1,2,\gamma_{12}} \dots Q_{1,m,\alpha_{1m}} W_{1,m,\gamma_{1m}}.$$

(b) If $\alpha_{11} = 0$, $\gamma_{11} \neq 0$, we may choose for S

$$S_{12} T_{1,\gamma_{11}} Q_{1,2,\gamma_{12}} W_{1,2,\alpha_{12}} Q_{1,3,\alpha_{13}} W_{1,3,\gamma_{13}} \dots Q_{1,m,\alpha_{1m}} W_{1,m,\gamma_{1m}}.$$

(c) If $\alpha_{ij} = \gamma_{ij} = 0$ ($j = 1 \dots s-1$), while α_{is} and γ_{is} are not both zero, we obtain by (a) or (b) a substitution S' replacing ξ_i by f_i . Then will $S = S'P_{1s}$.

* *Bulletin of the American Mathematical Society*, July, 1898.

We may therefore set $\Sigma = S\Sigma'$, Σ' being a new substitution of $L_{m,n,p}$ which leaves ξ_1 fixed. Let it replace η_1 by

$$f'_1 \equiv \sum_{j=1}^m (\beta_{1j} \xi_j + \delta_{1j} \eta_j),$$

where, by (2)₋₁, we have

$$\delta_{11} = 1, \quad \beta_{11} + \beta_{12} \delta_{12} + \dots + \beta_{1m} \delta_{1m} = 0.$$

Hence $S_1 \equiv V_{2,1, -\beta_{12}} Q_{2,1, -\delta_{12}} \dots V_{m,1, -\beta_{1m}} Q_{m,1, -\delta_{1m}}$

replaces η_1 by f'_1 . We may therefore set $\Sigma' = S'\Sigma_1$, Σ_1 being a new substitution of $L_{m,n,p}$ which leaves ξ_1 and η_1 fixed. For Σ_1 , the relations (2)₋₁ give

$$\alpha_{j1} = \gamma_{j1} = \beta_{j1} = \delta_{j1} = 0 \quad (j = 2, \dots, m),$$

together with relations connecting the α_{ij} , β_{ij} , γ_{ij} , δ_{ij} ($i, j = 2, \dots, m$) of precisely the form (2)₋₁ when written for $m-1$ couples of indices. Proceeding with Σ_1 as we did with Σ , we reach finally a substitution Σ_{m-1} , affecting only ξ_m , η_m , and hence either

$$T_{m, \alpha_{mm}} \quad \text{or} \quad (\xi_m \eta_m) T_{m, \gamma_{mm}}.$$

Therefore $\Sigma = L' \quad \text{or} \quad L' (\xi_m \eta_m),$

where L' is derived from the substitutions tabulated at the end of §1.

COROLLARY.—For $m > 2$, $L'_{m,n,p}$ may be generated by the S_{ij} , $W_{i,j,\lambda}$, together with $T_{1,v}$, where v is some not-square in the $GF[p^n]$.

This follows from the formulæ of composition

$$Q_{i,i,\lambda} = S_{jk}^{-1} W_{i,j,\lambda} S_{jk}, \quad V_{i,j,\lambda} = S_{ik}^{-1} Q_{i,j,\lambda} S_{ik} \quad (k \neq i \text{ or } j);$$

$$P_{i,j} T_{j,-1} = Q_{j,i,-1} Q_{i,j,1} Q_{j,i,-1};$$

$$T_{1,\mu} T_{2,\mu} = S_{12} P_{12} T_{1,-1} V_{1,2,\mu^{-1}} W_{1,2,\mu} V_{1,2,\mu^{-1}};$$

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

3. The order $O'_{m,n,p}$ of the group $L'_{m,n,p}$ is now readily determined. The linear function f_1 may take $P_{m,n}-1$ values, where $P_{m,n}$ denotes the number of solutions in the $GF[p^n]$ of

$$\alpha_{11} \gamma_{11} + \alpha_{12} \gamma_{12} + \dots + \alpha_{1m} \gamma_{1m} = 0.$$

By considering the cases $\alpha_{11} \gamma_{11} = 0$ and $\alpha_{11} \gamma_{11} \neq 0$, we derive the recursion formula

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

Since $P_{1,n} = 2p^n - 1$,

we find by induction that

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

Further, the number of values of f'_1 is $p^{n(2m-2)}$. Hence

$$O'_{m,n,p} = p^{n(2m-2)} (P_{m,n} - 1) O'_{m-1,n,p},$$

with the initial value

$$O'_{1,n,p} = p^n - 1 = \frac{1}{2} (P_{1,n} - 1).$$

Hence the order $O'_{m,n,p}$ equals

$$(p^{nm} - 1)(p^{n(2m-2)} - 1)p^{n(2m-2)}(p^{n(2m-4)} - 1)p^{n(2m-4)} \dots (p^{2n} - 1)p^{2n}.$$

4. Consider, for $m > 2$, the following sub-group of $L'_{m,n,p}$,

$$L''_{m,n,p} \equiv \{W_{i,j,\lambda}, S_{ij} \ (i, j = 1, \dots, m, i \neq j)\},$$

λ taking every value in the $GF[p^n]$. It contains every $Q_{i,j,\lambda}$, $V_{i,j,\lambda}$, $P_{i,j}T_{j,-1}$, $T_{1,\lambda}T_{2,\lambda}$, $T_{1,\lambda}$.

Let I be an invariant sub-group of $L''_{m,n,p}$ containing a substitution S , given by (1), neither the identity nor $T_{1,-1}T_{2,-1} \dots T_{m,-1}$, which* changes the sign of every index.

5. LEMMA I. — *I contains a substitution, not the identity, which multiplies ξ_1 by a constant.*

If $f_1 \equiv \sum_{j=1}^m (\alpha_{1j}\xi_j + \gamma_{1j}\eta_j)$ does not reduce to $\alpha_{11}\xi_1$, we have the following two cases.

(a) $\gamma_{11} \neq 0$.—Then $L''_{m,n,p}$ contains the product T ,

$$T_{1,\gamma_{11}^{-1}}T_{2,\gamma_{11}^{-1}}V_{2,1,-\gamma_{11}\alpha_{12}}Q_{2,1,-\gamma_{11}^{-1}\gamma_{12}}V_{3,1,-\alpha_{13}}Q_{3,1,-\gamma_{13}} \dots \\ \dots V_{m,1,-\alpha_{1m}}Q_{m,1,-\gamma_{1m}},$$

which replaces η_1 by f_1 and ξ_1 by $\gamma_{11}^{-1}\xi_1$. Hence I contains $S_1 = T^{-1}ST$, which replaces ξ_1 by $\gamma_{11}^{-1}\eta_1$. If S_1 multiplies ξ_2 by a constant, I contains its transformed by $P_{12}T_{1,-1}$, which will multiply ξ_1 by the same constant. In the contrary case there exists a substitution T_1 in L'' ,

* It may be shown that it is the only substitution of L'' commutative with every substitution in L'' .

leaving ξ_1 and η_1 fixed, and not commutative with S_1 . For, if we equate the expressions by which $S_1 V_{2,3,\lambda}$ and $V_{2,3,\lambda} S_1$ replace η_3 , we get

$$\eta'_3 - \lambda \xi'_3 = \eta'_3 + () \xi_2 + () \xi_3.$$

Similarly, if S_1 be commutative with $Q_{3,2,\lambda}$, we find

$$\xi'_3 + \lambda \xi'_2 = \xi'_3 + () \xi_2 + () \eta_3.$$

Hence $\xi'_2 = () \xi_3$, contrary to hypothesis. The group I therefore contains $S_1^{-1} T_1^{-1} S_1 T_1 \neq 1$, which leaves ξ_1 fixed.

(b) $\gamma_{11} = 0$.—Suppose,* for example, that $a_{12} \neq 0$. Then I'' contains the product T ,

$$T_{3, a_{12}} T_{2, a_{12}} Q_{2, 1, a_{11}} Q_{2, 3, a_{12}^{-1} a_{13}} W_{2, 3, \gamma_{13} a_{12}} Q_{2, 4, a_{14}} W_{2, 4, \gamma_{11}} \dots \\ \dots Q_{2, m, a_{1m}} W_{2, m, \gamma_{1m}},$$

which replaces ξ_2 by f_1 without altering ξ_1 . Then I contains S_1 , the transformed of S by T' , which replaces ξ_1 by ξ_2 .

If S_1 multiplies ξ_3 by a constant, its transformed by $P_{13} T_{1,-1}$, multiplies ξ_1 by the same constant. In the contrary case, S_1 is not commutative with both $V_{3,1,\lambda}$ and $V_{3,2,\lambda}$, which leave ξ_1 and ξ_2 fixed. Indeed, $S_1 V_{3,k,\lambda}$ and $V_{3,k,\lambda} S_1$ replace η_k by respectively

$$\eta'_k - \lambda \xi'_3, \quad \eta'_k + () \xi_3 + () \xi_k.$$

Hence would $\xi'_3 = \rho \xi_3$. It follows that I contains

$$S_1^{-1} V_{3,k,\lambda}^{-1} S_1 V_{3,k,\lambda} \quad (k = 1, 2),$$

which leave ξ_1 fixed, and do not both reduce to the identity.

NOTE.—It is clear from the proof that the final substitution multiplying ξ_1 by a constant does not reduce to $T_{1,-1} T_{2,-1} \dots T_{m,-1}$, unless S reduces to the same product.

6. LEMMA II.—The group I contains a substitution, not the identity, leaving fixed ξ_1 and η_1 .

By Lemma I., the group I contains a substitution S , which replaces ξ_1 by $a\xi_1$ and η_1 by

$$\beta_{11} \xi_1 + a^{-1} \eta_1 + \sum_{j=2}^m (\beta_{1j} \xi_j + \delta_{1j} \eta_j).$$

* If $a_{12} = a_{13} = \dots = a_{1m} = 0$, not every $\gamma_{1j} = 0$ by hypothesis. If $\gamma_{12} \neq 0$, we take in place of S its transformed by S_{23} , for which $a'_{12} \neq 0$.

(a) $\beta_{11} = 0$, $\beta_{ij} = \delta_{ij} = 0$ ($j = 2, \dots, m$).—Then $S = T_{1,a} S_1$, where, by the relations (2), S_1 involves only the indices ξ_i, η_i ($i = 2, \dots, m$). Thus, if $a = +1$, S leaves ξ_1 and η_1 fixed. Suppose, then, that $a \neq 1$.

If $S_1 = T_{2,-1} T_{3,-1} \dots T_{m,-1}$, the value $a = -1$ is excluded by the hypothesis on S . Since $S_1^2 = 1$, we have

$$S^2 = T_{1,a^2} \neq 1.$$

Transforming it by $P_{1,2} T_{3,-1}$, we obtain in I a substitution leaving ξ_1 and η_1 fixed.

If S_1 does not reduce to the above product, there exists a substitution Σ_1 in the group $L''_{m,m,p}$ affecting the same indices as does S_1 , and not commutative with S_1 . Then will I contain

$$S^{-1} \Sigma_1^{-1} S \Sigma_1 \equiv S_1^{-1} \Sigma_1^{-1} S_1 \Sigma_1 \neq 1,$$

which leaves ξ_1 and η_1 fixed.

(b) $\beta_{11} = 0$, β_{ij}, δ_{ij} not all zero.—Then, by § 2, $L''_{m,m,p}$ contains a substitution T , leaving ξ_1 and η_1 fixed, and replacing ξ_2 by

$$\sum_{j=2}^m (\beta_{1j} \xi_j + \delta_{1j} \eta_j).$$

Therefore I contains S_1 , the transformed of S by T , which replaces ξ_1 by $a\xi_1$, η_1 by $a^{-1}\eta_1 + \xi_2$.

Consider the substitutions Σ of L'' , such that $S_1^{-1} \Sigma^{-1} S_1 \Sigma$ leaves ξ_1 and η_1 fixed. If one such product be not the identity, the Lemma is proven. We may therefore suppose that it is the identity for every suitable Σ , e.g., $Q_{3,2,\lambda}$, $V_{3,3,\lambda}$, $T_{3,\mu}$, $T_{1,\lambda} T_{2,\lambda}^{-1}$. Equating the two values by which $S_1 V_{2,3,\lambda}$ and $V_{2,3,\lambda} S_1$ replace η_3 , and the two values by which they replace η_3 , we get

$$\xi'_3 = \delta_{23} \xi_3 - \delta_{23} \xi_2, \quad \xi'_2 = -\delta_{32} \xi_3 + \delta_{33} \xi_2.$$

Equating the values by which $S_1 Q_{3,2,\lambda}$ and $Q_{3,2,\lambda} S_1$ replace ξ_3 , and those by which they replace η_3 , we find

$$\xi'_2 = a_{33} \xi_2 - \gamma_{32} \eta_3, \quad \eta'_3 = -\beta_{23} \xi_2 + \delta_{22} \eta_3.$$

For $m > 3$, we may suppose S_1 to be commutative with $V_{3,4,\lambda}$, so that we have

$$\xi'_3 = \mu \xi_3, \quad \eta'_3 = \mu^{-1} \eta_3.$$

Transforming S_1 by $P_{13} T_{3,-1}$, we are led to Case (a).

For $m = 3$, S_1 becomes, on applying (2),

$$S_1 : \begin{cases} \xi'_1 = \alpha \xi_1, & \eta'_1 = \alpha^{-1} \eta_1 + \xi_2, \\ \xi'_2 = \pm \xi_2, & \eta'_2 = \mp \alpha \xi_1 \mp \beta_{23} \delta_{23} \xi_2 \pm \eta_2 + \beta_{23} \xi_3 + \delta_{23} \eta_3, \\ \xi'_3 = \pm \xi_3 - \delta_{23} \xi_2, & \eta'_3 = \pm \eta_3 - \beta_{23} \xi_2. \end{cases}$$

If $p^n > 2$, two distinct quantities $\lambda \neq 0$ exist in the $GF[p^n]$. Hence, if we equate the values by which $T_{1,\lambda} T_{2,\lambda^{-1}} S_1$ and $S_1 T_{1,\lambda} T_{2,\lambda^{-1}}$ replace η_2 , we find that $\beta_{23} = \delta_{23} = 0$. We are thus led to Case (a).

Consider the case $p^n = 2$. We may suppose that $\beta_{23} \delta_{23} = 0$, since otherwise the transformed of S_1 by $P_{12} T_{2,-1}$ falls under Case (c) below.

If $\beta_{23} = 0$, $\delta_{23} = 1$, $S_1 \equiv Q_{3,3,1} V_{1,2,1}$, and we have

$$S_1 V_{1,3,1}^{-1} S_1 V_{1,3,1} = V_{1,2,1}.$$

If $\delta_{23} = 0$, $\beta_{23} = 1$, $S_1 = V_{2,3,1} V_{1,2,1}$, and we have

$$S_1 Q_{2,3,1}^{-1} S_1 Q_{2,3,1} = V_{1,2,1}.$$

(c) $\beta_{11} \neq 0$.

Since $\sum_{j=1}^m \beta_{1j} \delta_{1j} = 0$,

we may suppose, for example, that $\beta_{12} \neq 0$, $\delta_{12} \neq 0$. Transforming S by $T_{2,i_2} T_{3,i_3}$, we may suppose that $\delta_{12} = 1$. The product

$$Q_{3,2,-\delta_{13}} V_{2,3,\beta_{13}} \cdots Q_{m,2,-\delta_{1m}} V_{2,m,\beta_{1m}}$$

transforms S into S_1 , which replaces ξ_1 by $\alpha \xi_1$, and η_1 by

$$\beta_{11} \xi_1 + \alpha^{-1} \eta_1 - \alpha^{-1} \beta_{11} \xi_2 + \eta_2.$$

Denote by μ the coefficient of ξ_2 . If, among the substitutions $Q_{3,2,\mu} W_{3,3,1}$, $T_{3,\mu} T_{2,\mu} S_{23}$, &c., of the group L'' , which leave $\mu \xi_2 + \eta_2$ invariant, there exist one, say R , which is not commutative with S_1 , then I contains

$$S_1^{-1} R^{-1} S_1 R \neq 1,$$

which leaves ξ_1 and η_1 fixed. In the contrary case, we find, on equating the values by which $S_1 Q_{3,2,\mu} W_{2,3,1}$ and $Q_{3,2,\mu} W_{2,3,1} S_1$ replace the index ξ_3 ,

$$\eta'_3 = () \eta_3 - \alpha_{23} \eta_2 + \mu \alpha_{23} \xi_2.$$

By one of the relations (2)₋₁, we have $a_{23} = 0$. Then, if S_1 be commutative with $T_{3,\mu} T_{2,\mu} S_{23}$,

$$\xi'_3 = \pm \xi_3, \quad \eta'_3 = \pm \eta_3.$$

We are again led to Case (a).

7. Applying anew the reasoning of §§ 5, 6, we conclude that, if $m \equiv 4$, I contains a substitution leaving fixed $\xi_1, \eta_1, \xi_2, \eta_2$; finally, that I contains a substitution leaving fixed

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

Transforming it by the product of $P_{1,m-1} T_{1,-1}$ and $P_{2,m} T_{2,-1}$, we obtain a substitution S of the group I which alters only $\xi_1, \eta_1, \xi_2, \eta_2$, and does not reduce to the identity. Applying the relations (2), it is seen to have the form

$$S \begin{cases} \xi'_1 = a_{11} \xi_1 + \gamma_{11} \eta_1 + a_{12} \xi_2 + \gamma_{12} \eta_2, \\ \eta'_1 = \beta_{11} \xi_1 + \delta_{11} \eta_1 + \beta_{12} \xi_2 + \delta_{12} \eta_2, \\ \xi'_2 = a_{21} \xi_1 + \gamma_{21} \eta_1 + a_{22} \xi_2 + \gamma_{22} \eta_2, \\ \eta'_2 = \beta_{21} \xi_1 + \delta_{21} \eta_1 + \beta_{22} \xi_2 + \delta_{22} \eta_2. \end{cases}$$

8. THEOREM.—If $m > 2$, I contains a substitution $V_{a,b,\rho}$.

CASE I.— $\gamma_{11} \neq 0$. Transforming S by

$$T_{1,\gamma_{11}^{-1}} T_{3,\gamma_{11}^{-1}} V_{2,1,-a_{12}} Q_{2,1,-\gamma_{12}},$$

we obtain a substitution S_1 in I which replaces ξ_1 by $\gamma_{11}^{-1} \eta_1$, but otherwise of the same form as S . Applying the relations (2), S_1 is seen to take the form

$$\begin{cases} 0 & \gamma_{11}^{-1} & 0 & 0 \\ \gamma_{11} & -\gamma_{11}^{-1} \beta_{12} \delta_{12} & \beta_{12} & \delta_{12} \\ 0 & -\gamma_{11}^{-1} \beta_{12} \gamma_{22} & 0 & \gamma_{22} \\ 0 & -\gamma_{11}^{-1} \delta_{12} \gamma_{22}^{-1} & \gamma_{22}^{-1} & 0 \end{cases}.$$

If S_1 be not commutative with S_{23} , I contains

$$S_1^{-1} S_{23} S_1 S_{23} \neq 1,$$

which leaves fixed ξ_1, ξ_3, η_3 (Case III.). But, if S_1 be commutative with S_{23} , the matrix of its coefficients must remain unaltered upon interchanging the last two rows and simultaneously the last two

columns. Hence $\beta_{12} = \delta_{12}$, $\gamma_{22} = \gamma_{22}^{-1} = \pm 1$,

$$S_1 = T_{1, \gamma_{11}} S_{12} Q_{2, 1, -\beta_{12}} V_{1, 2, \beta_{12}} T_{2, \pm 1}.$$

Dropping the subscripts to γ_{11} and β_{12} , we consider two cases :

(a) $\beta = 0$.— I contains the product of S_1 and its transformed by $P_{12} T_{3, -1}$, viz.,

$$T_{1, \gamma} S_{12} T_{2, \pm 1} \cdot T_{2, \gamma} S_{12} T_{1, \pm 1} = T_{1, \pm \gamma} T_{2, \pm \gamma^{-1}}.$$

Transforming this by S_{23} and $S_{23} V_{1, 3, \lambda}$, we get

$$T_{1, \pm \gamma} T_{2, \pm \gamma}, \quad V_{1, 3, \lambda(\pm \gamma - 1)} T_{1, \pm \gamma} T_{2, \pm \gamma}.$$

Hence, unless $\gamma = \pm 1$, I contains a $V \neq 1$. There remains the case $S_1 = S_{12} T_{1, \pm 1} T_{2, \pm 1}$, which $V_{1, 2, \lambda}$ transforms into

$$V_{1, 2, -\lambda} W_{1, 2, \lambda} S_{12} T_{1, \pm 1} T_{2, \pm 1}.$$

Hence I contains $V_{1, 2, -\lambda} W_{1, 2, \lambda}$, which replaces ξ_1 by

$$(\lambda^2 + 1) \xi_1 + \lambda \eta_3,$$

and consequently falling under Case II.

(b) $\beta \neq 0$.—Transforming S_1 by $V_{1, 2, \mp \beta}$, we get

$$V_{1, 2, \pm \beta} T_{1, \gamma} S_{12} Q_{2, 1, -\beta} T_{2, \pm 1}.$$

Its product by S_1^{-1} , which may be written

$$T_{2, \pm 1} Q_{2, 1, \beta} S_{12} T_{1, \gamma^{-1}} W_{1, 2, -\beta \gamma^{-1}},$$

gives $V_{1, 2, \pm \beta} W_{1, 2, -\beta \gamma^{-1}}$ (Case II.).

CASE II.— $\gamma_{11} = 0$, α_{12} and γ_{12} not both zero. According as $\alpha_{12} \neq 0$ or $\gamma_{12} \neq 0$, the substitution T ,

$$T_{2, \alpha_{12}} T_{3, \alpha_{12}} Q_{2, 1, \alpha_{12}}, \quad S_{23} T_{2, \gamma_{12}} T_{3, \gamma_{12}} Q_{2, 1, \alpha_{11}},$$

replaces ξ_2 by $\alpha_{11} \xi_1 + \gamma_{11} \eta_1 + \alpha_{12} \xi_3 + \gamma_{12} \eta_3$ and leaves ξ_1 fixed. Hence $S_1 \equiv T^{-1} S T$ replaces ξ_1 by ξ_3 and leaves ξ_3, η_3 fixed.

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

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

which leaves ξ_1 fixed (Case III.). But, if S_1 be commutative with $V_{1, 2, \lambda}$, it reduces to

$$P_{12} T_{2, -1} Q_{2, 1, \delta_{11}} V_{1, 2, -\beta_{11}} = \begin{Bmatrix} 0 & 0 & 1 & 0 \\ \beta_{11} & \delta_{11} & -\beta_{11} \delta_{11} & 1 \\ -1 & 0 & \delta_{11} & 0 \\ 0 & -1 & \beta_{11} & 0 \end{Bmatrix}.$$

Then I contains

$$(P_{12}T_{2,-1})^{-1}S_1(P_{12}T_{2,-1})S_1^{-1} = Q_{2,1,\delta_{11}}Q_{1,2,\delta_{11}}.$$

Its transformed by $T_{1,\rho}T_{3,\rho}$ is $Q_{2,1,\rho^{-1}\delta_{11}}Q_{1,2,\rho\delta_{11}}$. Thus I contains the product (where δ is written for δ_{11})

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

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

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

Hence, by Case I., (a), I contains a $V \neq 1$, unless $1+\delta^2 = 0$ or 1 . If $1+\delta^2 = 0$, the cube of $Q_{2,1,\delta}Q_{1,2,\delta}$ gives $T_{1,-1}T_{2,-1}$, so that for $p > 2$ we reach a $V \neq 1$. For $p = 2$, we obtain* from $Q_{2,1,1}Q_{1,2,1}$ the substitution $Q_{3,1,1}$. If $\delta = 0$, we have

$$S_1^2 = T_{1,-1}T_{2,-1}V_{1,2,-2\delta_{11}}, \quad S_1^4 = V_{1,2,4\delta_{11}}.$$

For the case $p = 2$, $Q_{1,2,1}$ transforms $S_1 = P_{12}V_{1,2,\delta_{11}}$ into a substitution $\neq 1$, leaving ξ_1 fixed (Case III.).

CASE III.— $\gamma_{11} = \alpha_{12} = \gamma_{12} = 0$.—We may readily verify that S reduces to

$$T_{1,\alpha_{11}}V_{1,2,\beta_{12}}Q_{2,1,-\delta_{12}}T_{2,\alpha_{22}}.$$

Its transformed by $T_{3,\alpha_{22}}^{-1}T_{2,\alpha_{22}}^{-1}V_{1,2,\lambda}$ gives

$$V_{1,2,\lambda(\alpha_{11}\alpha_{22}-1)}T_{2,\alpha_{22}}T_{1,\alpha_{11}}V_{1,2,\beta_{12}}Q_{2,1,-\delta_{12}}.$$

Hence I contains $V_{1,2,\lambda(\alpha_{11}\alpha_{22}-1)}$.

For the case $\alpha_{22} = \alpha_{11}^{-1}$, I contains

$$\begin{aligned} S' &= S(T_{3,-\alpha_{11}}T_{2,\alpha_{11}}P_{12})^{-1}S(T_{3,-\alpha_{11}}T_{2,\alpha_{11}}P_{12}) \\ &= V_{1,2,\beta(\alpha-1)}Q_{2,1,-\alpha\delta}Q_{1,2,-\delta} \end{aligned}$$

if we write α for α_{11} , β for β_{12} , δ for δ_{12} .

Transforming S' by S_{13} and the result by $P_{12}T_{2,-1}$, we obtain respectively,

$$Q_{1,2,\beta(\alpha-1)}W_{1,2,\alpha\delta}V_{1,2,-\delta}$$

$$Q_{2,1,-\beta(\alpha-1)}W_{1,2,\alpha\delta}V_{1,2,-\delta}.$$

The product of the former by the reciprocal of the latter gives

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

* Jordan, *Traité des Substitutions*, p. 204, ll. 15-17.

If $\beta(\alpha-1) \neq 0$, I contains a $V \neq 1$ (end of Case II.). If $\alpha = 1$,

$$S' = Q_{2, 1, -\delta} Q_{1, 2, -\delta}.$$

More generally, for $\alpha_{22} = \alpha_{11}^{-1}$, I contains

$$S(P_{12}T_{3, -1})^{-1} S(P_{12}T_{3, -1}) = Q_{2, 1, -\lambda_2} Q_{1, 2, -\lambda_2}.$$

There remains the case $\delta = 0$, $\beta(\alpha-1) = 0$, when S reduces to $T_{1, \alpha} T_{2, \alpha^{-1}}$ or $V_{1, 2, \rho}$.

9. Having a substitution of the form $V_{a, b, \rho}$, the group I will contain its transformed by $T_{a, \lambda} T_{c, \lambda}$, giving $V_{a, b, \rho\lambda^{-1}}$. Hence I contains $V_{a, b, \mu}$ ($\mu = \text{arbitrary}$).

Transforming it by $P_{a, i} P_{b, j}$, which belongs to L'' , we obtain $V_{i, j, \mu}$. This is transformed by S_{ik} and S_{ij} into respectively $Q_{i, j, \mu}$ and $W_{i, j, \mu}$. Further, I contains

$$S_{12} = W_{1, 2, -1} Q_{1, 2, +1} V_{1, 2, -1} Q_{2, 1, -1} Q_{1, 2, +1} W_{1, 2, -1}.$$

Hence the invariant sub-group I coincides with $L''_{m, n, p}$. We have therefore reached the following result:—

THEOREM.—For $p > 2$, the maximal invariant sub-group of $L''_{m, n, p}$ is of order 2 or 1, according as L'' contains $T_{1, -1} T_{2, -1} \dots T_{m, -1}$ or does not; while, for $p = 2$, $L''_{m, n, p}$ coincides with $L'_{m, n, p}$ and is simple.

10. The group* $L_{m, n, 2}$ with the factors of composition 2 and $O'_{m, n, 2}$ (given in §3) is a direct generalization of Jordan's first hypo-Abelian group G_0 .†

It is proved below (§§ 16, 18) that the senary group $L''_{3, n, p}$ ($p > 2$) does not contain a substitution of the form $T_{i, \nu}$, ν being a not-square in the $GF[p^n]$, and it seems probable that a like result holds for the general group $L''_{m, n, p}$. If this conjecture be always true, L'' is of index 2 under L' , and L'' is simple only when m is odd, with -1 a not-square in the $GF[p^n]$ ($p > 2$); while, if m be even or if -1 be a square, L'' has the factors of composition 2 and $\frac{1}{2}O'_{m, n, p}$. Independent of the truth of our conjecture, we have the result that, if m be

* The structure of this group was determined by the writer in March, 1897, and published in the *Quarterly Journal*, June, 1898. The present paper uses the simplified treatment given in the article "The Structure of the Hypo-Abelian Groups," *Bulletin of the American Mathematical Society*, July, 1898.

† *Traité des Substitutions*, pp. 199–206.

odd and -1 a not-square, simple groups of order $\frac{1}{2}O'_{m,n,p}$ exist. Indeed, this result follows whether or not $T_{1,-1}$ belongs to $L''_{n,n,p}$.

Isomorphism of $L''_{n,n,p}$ with the group $G_{4,n,p}$ of Quaternary Linear Substitutions in the $GF[p^n]$ of determinant unity, §§ 11-19.

11. Consider the composition of quaternary substitutions

$$S: \xi'_i = \sum_{j=0}^3 a_{ij} \xi_j \quad (i = 0, 1, 2, 3).$$

If (a'_{ij}) operates first, we have the composition formula

$$(a''_{ij}) = (a_{ij})(a'_{ij}),$$

where
$$a''_{ij} = \sum_{k=0}^3 a_{ik} a'_{kj} \quad (i, j = 0, 1, 2, 3).$$

Denoting the second minors of the determinant $|a_{ij}|$ as follows:—

$$\begin{vmatrix} a_{ij} & a_{il} \\ a_{kj} & a_{kl} \end{vmatrix} \equiv D_{kl}^{ij} \equiv D_{ij}^{kl} \equiv -D_{kj}^{il} \equiv -D_{il}^{kj},$$

we readily verify the formula

$$D''_{kl}{}^{ij} = \sum_{r,s=0}^3 D_{ks}^{ir} D_{sl}{}^{rj}.$$

12. If, therefore, we build a senary substitution Σ whose thirty-six coefficients are the determinants

$$\pm D_{kl}^{ij} \quad \begin{pmatrix} i < k \\ j < l \end{pmatrix},$$

such that the pair i_k is constant for the six elements of any row, and the pair ${}_j^l$ constant for the six elements of any column, and furthermore such that the two elements

$$\pm D_{kl}^{ij}, \quad \pm D_{lk}^{ji}$$

are symmetrically placed with respect to the main diagonal, we obtain a correspondence between the substitutions S and Σ , such that to a given S corresponds one Σ , and to every product $S'S$ corresponds the product $\Sigma'\Sigma$. (An explicit formulation of the proof is given in § 14 for the most interesting case.) The determinant of Σ equals the *second compound** Δ_6 of the determinant $|a_{ij}|$ of the fourth order. Hence†

$$|\Sigma| = |S|^3.$$

* Muir, *Theory of Determinants*, §§ 170-176.

† *Ibid.*, § 174.

13. Of the various isomorphisms thus defined, we proceed to select the one which establishes the isomorphism of the groups $L''_{3,n,p}$, $G_{4,n,p}$.

We begin with the second compound of $|a_{ij}|$, viz.,

$$\Delta_0 \equiv \begin{vmatrix} D_{11}^{00} & D_{12}^{00} & D_{13}^{00} & D_{12}^{01} & D_{13}^{01} & D_{13}^{02} \\ D_{21}^{00} & D_{22}^{00} & D_{23}^{00} & D_{22}^{01} & D_{23}^{01} & D_{23}^{02} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ D_{31}^{20} & D_{32}^{20} & D_{33}^{20} & D_{32}^{21} & D_{33}^{21} & D_{33}^{22} \end{vmatrix}.$$

The value of the determinant is unaltered if we move the first and second rows into the places of the sixth and fourth rows respectively, and the first and second columns into the places of the sixth and fourth columns. The elements of the determinant appear in their new order in the following scheme, where a, b, c take either value ± 1 independently*:

	ξ_0	η_0	ξ_1	η_1	ξ_2	η_2
ξ_0	$1D_{33}^{00}$	aD_{31}^{01}	bD_{33}^{01}	$-abD_{32}^{00}$	cD_{33}^{02}	acD_{31}^{00}
η_0	aD_{23}^{10}	$1D_{22}^{11}$	abD_{23}^{11}	$-bD_{22}^{10}$	acD_{23}^{12}	cD_{21}^{10}
ξ_1	bD_{33}^{10}	abD_{31}^{11}	$1D_{33}^{11}$	$-aD_{32}^{10}$	bcD_{33}^{12}	$abcD_{31}^{10}$
η_1	$-abD_{23}^{00}$	$-bD_{22}^{01}$	$-aD_{23}^{01}$	$1D_{22}^{00}$	$-abcD_{23}^{02}$	$-bcD_{21}^{00}$
ξ_2	cD_{33}^{20}	acD_{31}^{21}	bcD_{33}^{21}	$-abcD_{32}^{20}$	$1D_{33}^{22}$	aD_{31}^{20}
η_2	acD_{13}^{00}	cD_{12}^{01}	$abcD_{13}^{01}$	$-bcD_{12}^{00}$	aD_{13}^{02}	$1D_{11}^{00}$

This matrix has the symmetry with respect to the main diagonal and the other properties required for the isomorphism. Further, the square array of signs

$$\begin{array}{cccccc} 1 & a & b & -ab & c & ac \\ \dots & \dots & \dots & \dots & \dots & \dots \\ ac & c & abc & -bc & a & 1 \end{array}$$

has the property that any row is obtained from the first row by

* It may be verified that for no other arrangement of signs will the substitution leave $\xi_0\eta_0 + \xi_1\eta_1 + \xi_2\eta_2$ invariant.

multiplying the latter by the leading term of the given row. Hence the determinant of the above substitution

$$= 1^2 a^2 b^3 (-ab)^2 c^2 (ac)^2 \Delta_0 \equiv |a_{ij}|^3.$$

14. We find by inspection that the above substitution may be written as follows:—

$$\Sigma: \left\{ \begin{array}{l} \xi'_i = \epsilon_i \sum_j^{0,1,2} (D_{33}^{ij} \epsilon_j \xi_j + a D_{3j+2}^{i,j+1} \epsilon_j \eta_j) \\ \eta'_i = \epsilon_i \sum_j^{0,1,2} (a D_{i+2,3}^{i+1,j} \epsilon_j \xi_j + D_{i+2,j+2}^{i+1,j+1} \epsilon_j \eta_j) \end{array} \right\} \quad (i = 0, 1, 2),$$

where the sums $i+1, i+2, j+1, j+2$ are taken modulo 3, and where

$$\epsilon_0 = 1, \quad \epsilon_1 = b, \quad \epsilon_2 = c, \quad \epsilon_i^2 = 1.$$

Introduce the new indices*

$$w_i = \epsilon_i \xi_i, \quad y_i = a \epsilon_i \eta_i \quad (i = 0, 1, 2),$$

so that

$$\sum_{i=0}^2 w_i y_i = a \sum_{i=0}^2 \xi_i \eta_i.$$

The substitution Σ takes the simple form

$$\Sigma_1: \left\{ \begin{array}{l} x'_i = \sum_j^{0,1,2} (D_{33}^{ij} w_j + D_{3j+2}^{i,j+1} y_j) \\ y'_i = \sum_j (D_{i+2,3}^{i+1,j} w_j + D_{i+2,j+2}^{i+1,j+1} y_j) \end{array} \right\} \quad (i = 0, 1, 2).$$

If we make Σ_1 correspond to S , we may verify at once that $\Sigma'_1 \Sigma_1$ will correspond to $S'S$. We use our earlier formula in the form

$$D''_{ki}{}^j = \sum_s^{0,1,2} (D_{k3}^{is} D_{3i}^{sj} + D_{k,s+1}^{is} D_{s+1,i}^{sj}),$$

where $s+1$ is taken modulo 3.

15. THEOREM.—*The substitution Σ_1 merely multiplies the function $\sum_i^{0,1,2} x_i y_i$ by the determinant Δ_0 of Σ_1 .*

The conditions are as follows (see § 1):—

$$(1) \quad \sum_j^{0,1,2} D_{33}^{ij} D_{3j+2}^{i,j+1} = \sum_j^{0,1,2} D_{i+2,3}^{i+1,j} D_{i+2,j+2}^{i+1,j+1} = 0.$$

* This is equivalent to transforming Σ by a substitution of determinant $a \equiv \pm 1$.

These are algebraic identities, being one-half of the expansions of the determinants

$$\left| \begin{array}{cccc} a_{i0} & a_{i1} & a_{i2} & a_{i3} \\ a_{30} & a_{31} & a_{32} & a_{33} \\ \hline a_{i0} & a_{i1} & a_{i2} & a_{i3} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{array} \right|, \quad \left| \begin{array}{cccc} a_{i+10} & a_{i+11} & a_{i+12} & a_{i+13} \\ a_{i+20} & a_{i+21} & a_{i+22} & a_{i+23} \\ \hline a_{i+10} & a_{i+11} & a_{i+12} & a_{i+13} \\ a_{i+20} & a_{i+21} & a_{i+22} & a_{i+23} \end{array} \right|.$$

$$(2) \quad \sum_j^{0,1,2} (D_{33}^{ij} D_{k+2j+2}^{k+1j+1} + D_{3j+2}^{ij+1} D_{k+23}^{k+1j}) = \delta_{ik} \Delta_6 \quad (i, k = 0, 1, 2),$$

where $\delta_{ii} = 1$, $\delta_{ik} = 0$ for $i \neq k$.

The left side of (2) is the expansion of

$$\left| \begin{array}{cccc} a_{i0} & a_{i1} & a_{i2} & a_{i3} \\ a_{30} & a_{31} & a_{32} & a_{33} \\ \hline a_{k+10} & a_{k+11} & a_{k+12} & a_{k+13} \\ a_{k+20} & a_{k+21} & a_{k+22} & a_{k+23} \end{array} \right| = + \delta_{ik} \Delta_6$$

for every $i, k = 0, 1, 2$.

16. THEOREM.—The substitution Σ_1 can reduce to the form

$$T_{0,\nu}: \quad \begin{cases} x'_0 = \nu x_0, & x'_i = x_i \\ y'_0 = \nu^{-1} y_0, & y'_i = y_i \end{cases} \quad (i = 1, 2),$$

if, and only if, ν be a square in the $GF[p^n]$.

Consider the "partial" transformation (whose determinant may be zero) derived from Σ_1 ,

$$\Sigma_y: \quad y'_i = \sum_j^{0,1,2} D_{i+2j+2}^{i+1j+1} y_j \quad (i = 0, 1, 2).$$

Its determinant is seen to equal

$$\Delta_3^2 \equiv \left| \begin{array}{ccc} a_{00} & a_{01} & a_{02} \\ a_{10} & a_{11} & a_{12} \\ a_{20} & a_{21} & a_{22} \end{array} \right|^2.$$

The analogous substitution derived from $T_{0,\nu}$ is

$$\begin{pmatrix} \nu^{-1} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

of determinant ν^{-1} , which must therefore be a square.

Inversely, if ν be a square, to the substitution

$$S = \begin{pmatrix} \nu^{\frac{1}{2}} & 0 & 0 & 0 \\ 0 & \nu^{-\frac{1}{2}} & 0 & 0 \\ 0 & 0 & \nu^{-\frac{1}{2}} & 0 \\ 0 & 0 & 0 & \nu^{\frac{1}{2}} \end{pmatrix}$$

corresponds the substitution $\Sigma_1 = T_{0,\nu}$.

17. THEOREM.—*To the substitution $\Sigma_1 = 1$ correspond exactly the two substitutions $S = \pm 1$, multiplying every index by the constant ± 1 .*

Indeed the "partial" transformation

$$(\Delta_3^{-1} D_{i,2j,2}^{i+1,j+1}) \quad (i, j = 0, 1, 2)$$

is the reciprocal of the transformation of determinant Δ_3 ,

$$\begin{pmatrix} a_{00} & a_{01} & a_{02} \\ a_{10} & a_{11} & a_{12} \\ a_{20} & a_{21} & a_{22} \end{pmatrix};$$

so that, for $\Sigma_1 = 1$, the latter must have the form

$$\begin{pmatrix} \Delta_3 & 0 & 0 \\ 0 & \Delta_3 & 0 \\ 0 & 0 & \Delta_3 \end{pmatrix}.$$

By comparing their determinants, we have

$$\Delta_3 = \Delta_3^3, \quad \Delta_3 = \pm 1.$$

Further, the determinant of Σ_1 being the cube of the determinant of S , the latter must be $+1$. Hence

$$a_{33} = \pm 1.$$

Building the second minors of

$$(a_{ij}) \quad (i, j = 0, 1, 2, 3),$$

which have one and but one element from the main diagonal, we find that

$$a_{ij} = a_{ji} = 0 \quad (i, j = 0, 1, 2).$$

COROLLARY.—If we consider the substitution (a_{ij}) to be identical with $(-a_{ij})$, and denote the pair by S_1 , we obtain a simple isomorphism between the groups $\{S_1\}$ and $\{\Sigma_1\}$.

The group of the S_1 is of index 1 or 2 under the group of all quaternary linear substitutions in the $GF[p^n]$ according as $p = 2$ or $p > 2$.

18. Denote by $G_{4,n,p}$ the group of quaternary linear substitutions S in the $GF[p^n]$ which have the determinant unity. Its order* is

$$(p^{4n}-1)(p^{4n}-p^n)(p^{4n}-p^{2n})p^{3n}.$$

Denote the corresponding substitution Σ_1 of determinant unity by Σ'_1 . Hence, for $p > 2$, the order of the group $\{\Sigma'_1\}$ is

$$\frac{1}{2} (p^{3n}-1)(p^{4n}-1)p^{4n}(p^{2n}-1)p^{2n}.$$

This being the order of the group $L''_{3,n,p}$ which $\eta'_{i,\nu}$ ($\nu = \text{not-square}$ in the $GF[p^n]$) extends to the group $L'_{3,n,p}$ of all senary linear substitutions of determinant unity in the $GF[p^n]$, leaving $\Sigma x_i y_i$ invariant, it follows, from the theorem of § 16, that $\{\Sigma'_1\} \equiv L''_{3,n,p}$.

Likewise, for $p = 2$, the order of the group $\{\Sigma'_1\}$ is

$$(2^{3n}-1)(2^{4n}-1)2^{4n}(2^{2n}-1)2^{2n}.$$

This equals the order of the group $L'_{3,n,2} \equiv L''_{3,n,2}$ of all senary linear substitutions in the $GF[2^n]$, which leave invariant $\Sigma x_i y_i$, and which, if written in the form (1) of § 1, satisfy the relation

$$\sum_{i,j}^{1,2,3} a_{ij} \delta_{ij} = 1.$$

Writing the left member in the notation used for our substitutions Σ_1 , it becomes

$$\begin{aligned} & \sum_{i,j}^{0,1,2} D_{33}^{ij} D_{i+2,j+2}^{i+1,j+1} \\ & \equiv D_{33}^{00} D_{22}^{11} + D_{33}^{01} D_{20}^{12} + D_{33}^{02} D_{21}^{16} + D_{33}^{10} D_{02}^{21} + D_{33}^{11} D_{00}^{22} + D_{33}^{12} D_{01}^{20} \\ & \quad + D_{33}^{20} D_{12}^{01} + D_{33}^{21} D_{10}^{02} + D_{33}^{22} D_{11}^{00}, \end{aligned}$$

* *Annals of Mathematics*, October, 1897.

which may be given the form

$$\begin{vmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{vmatrix} + 2a_{33} \begin{vmatrix} a_{00} & a_{01} & a_{02} \\ a_{10} & a_{11} & a_{12} \\ a_{20} & a_{21} & a_{22} \end{vmatrix}.$$

Hence, for every p , the group $\{\Sigma'_1\}$ coincides with the group $L''_{3,n,p}$.

19. From the known* structure of $G_{4,n,p}$, we readily deduce that of the isomorphic group $\{\Sigma'_1\}$. The quaternary group of substitutions of determinant unity has the maximal invariant sub-group generated by the substitution M ,

$$M = \begin{pmatrix} \mu & 0 & 0 & 0 \\ 0 & \mu & 0 & 0 \\ 0 & 0 & \mu & 0 \\ 0 & 0 & 0 & \mu \end{pmatrix}, \quad \mu^4 = 1, \quad \mu^{p^n-1} = 1.$$

To M corresponds in $\{\Sigma'_1\}$ the substitution which multiplies every index by μ^2 . Hence,

(1) If $p=2$, μ has the value 1 only, so that $\{\Sigma'_1\} \equiv L''_{3,n,2}$ is simple.

(2) If $p^n = 4t+3$, so that -1 is a not-square in the $GF[p^n]$, $\mu = \pm 1$. Hence $L''_{3,n,p}$ is simple.

(3) If $p^n = 4t+1$, so that $-1 = \text{square}$, $\mu = \pm 1$ or $\pm \sqrt{-1}$. Hence $L''_{3,n,p}$ has the maximal invariant sub-group of order 2, generated by the substitution multiplying every index by -1 .

The above results agree with those obtained earlier in the paper for the general group $L''_{m,n,p}$.

20. Furthermore, our investigation gives an immediate proof of the following theorem for continuous groups:—

The quaternary group of all real linear homogeneous transformations of determinant unity is hemihedrally isomorphic with the senary group of all real linear homogeneous transformations of determinant unity which leave invariant a homogeneous quadratic function.

* *Annals of Mathematics*, October, 1897.

The corresponding projective groups are simply isomorphic, and each is a simple group of fifteen parameters—results due to Lie. Moreover, to every projective transformation (finite or infinitesimal) of ordinary space, we obtain at once the corresponding projective transformation leaving invariant the surface

$$\sum_{i=0}^2 x_i y_i = 0,$$

and hence that leaving invariant an arbitrary non-degenerate surface of the second order in space of five dimensions.

To obtain the general infinitesimal transformation of the form Σ_1 , we set

$$a_{ii} = 1 + a_{ii} \delta t, \quad a_{ij} = a_{ij} \delta t \quad (i, j = 0, \dots, 3).$$

We readily obtain the following expressions :—*

$$\delta x_i \equiv x'_i - x_i = \delta t \{ (a_{33} + a_{ii}) x_i + a_{i-1} x_{i-1} + a_{i+1} x_{i+1} + a_{3, i+1} y_{i-1} - a_{3, i+2} y_{i+1} \},$$

$$\delta y_i \equiv y'_i - y_i = \delta t \{ (a_{i+1, i+1} + a_{i+2, i+2}) y_i - a_{i+1, i} y_{i+1} - a_{i+2, i} y_{i+2} + a_{i+2, 3} x_{i+1} - a_{i+1, 3} x_{i+2} \}.$$

$$\delta \left(\sum_{i=0}^2 x_i y_i \right) = (a_{00} + a_{11} + a_{22} + a_{33}) \sum_{i=0}^2 x_i y_i.$$

The condition for absolute invariance of $\Sigma x_i y_i$ is thus the same as the condition derived from

$$| a_{ij} | = 1.$$

It is seen that the above infinitesimal transformation contains all sixteen arbitrary parameters a_{ij} .

21. THEOREM.—For $p^n = 4l+1$, the group $L_{m, n, p}$ is simply isomorphic with the group† of orthogonal substitutions on $2m$ indices in the $GF[p^n]$.

Since -1 is in this case the square of a quantity I of the $GF[p^n]$, we may introduce the new indices X_i, Y_i defined thus :

$$\xi_i = X_i + IY_i, \quad \eta_i = X_i - IY_i \quad (i = 1, \dots, m).$$

Then

$$\sum_{i=1}^m \xi_i \eta_i = \sum_{i=1}^m (X_i^2 + Y_i^2).$$

* As usual, the subscripts $i, i \pm 1, i \pm 2$ are to be taken modulo 3.

† The writer has determined the structure of the orthogonal group on m indices in the $GF[p^n]$ for every integer $m \neq 4, n$, and prime number p : *Proceedings of the California Academy of Sciences*, Third Series, Vol. I., Nos. 4 and 5; *Bulletin of the Amer. Math. Soc.*, February and May, 1898.

22. Consider the group of linear substitutions (1) on m pairs of indices in the $GF[p^n]$ which have the absolute invariant

$$\phi \equiv \sum_{i=1}^m \xi_i \eta_i + \sum_{i=1}^m (\alpha_i \xi_i + \gamma_i \eta_i),$$

where* the α_i and γ_i are not all zero.

If a substitution T converts ϕ into Φ , the group leaving ϕ invariant is transformed by T to the group leaving Φ invariant. Taking as T the following product belonging to the group $L_{m,n,p}$ leaving $\sum_{i=1}^m \xi_i \eta_i$ invariant:

$$T \equiv W_{1,m,-\gamma_m} Q_{1,m,-\alpha_m} \cdots W_{1,2,-\gamma_2} Q_{1,2,-\alpha_2} T_{1,\alpha_1^{-1}},$$

we find that
$$\Phi \equiv T(\phi) = \sum_{i=1}^m \xi_i \eta_i + \xi_1 + \lambda \eta_1,$$

where
$$\lambda \equiv \sum_{i=1}^m \alpha_i \gamma_i.$$

23. Suppose first that $p^n = 2$. Then $\lambda = 0$ or 1.

(a) For $\lambda = 1$, the group leaving Φ invariant is the second hypo-Abelian group G_1 (Jordan, *Traité des Substitutions*, pp. 206–213 and 440). For $m > 1$, G_1 has a simple sub-group of index 2 and of order

$$(2^m + 1)(2^{2m-2} - 1) 2^{2m-2} (2^{2m-4} - 1) 2^{2m-4} \cdots (2^2 - 1) 2^1,$$

which is composed of all the substitutions of G_1 which satisfy the relation†

$$\sum_{i,j}^{1,\dots,m} \alpha_{ij} \delta_{ij} + \alpha_{11} + \beta_{11} + \gamma_{11} + \delta_{11} \equiv m \pmod{2}.$$

(b) For $\lambda = 0$, we introduce the new indices

$$\left. \begin{aligned} \bar{\eta}_i &= \eta_i + \xi_1, & \bar{\eta}_1 &= \eta_1 \\ \bar{\xi}_1 &= \xi_1, & \bar{\xi}_i &= \xi_i \end{aligned} \right\} \quad (i = 2, \dots, m).$$

Then
$$\sum_{i=1}^m \bar{\xi}_i \bar{\eta}_i \equiv \sum_{i=1}^m \xi_i \eta_i + \xi_1.$$

This transformation of indices is equivalent to the Abelian substitution

* We will suppose that $\alpha_1 \neq 0$, changing, if necessary, the notation, which is allowable on account of the symmetry of $\sum \xi_i \eta_i$.

† "The Structure of the Hypo-Abelian Groups," *Bulletin of the Amer. Math. Soc.*, July, 1898.

L'_1 (Jordan, p. 174). Hence the group with the invariant $\Phi_{\lambda=0}$ is conjugate within the Abelian group $H_{m,1,2}$ in the $GF[2]$ to the first hypo-Abelian group $L_{m,1,2}$ defined in § 1 (the group G_0 of Jordan, p. 199).

Combining the results of cases (a) and (b), we have proved the following

THEOREM.—*The group of linear substitutions modulo 2 on $2m$ indices which leave invariant*

$$\sum_{i=1}^m (\xi_i \eta_i + \alpha_i \xi_i + \gamma_i \eta_i)$$

is conjugate within the Abelian group to the first or else to the second hypo-Abelian group.

24. For $p^n > 2$ the group with the invariant Φ must leave separately invariant

$$\sum_{i=1}^m \xi_i \eta_i, \quad \xi_1 + \lambda \eta_1;$$

and is therefore a sub-group of the group $L_{m,n,p}$. We will designate the group as $B_{m,n,p}$. For $m > 1$, it contains (§ 2) a sub-group $B'_{m,n,p}$ of index 2, which the transposition $(\xi_m \eta_m)$ extends to $B_{m,n,p}$. We treat in turn the cases $\lambda = 0$ and $\lambda \neq 0$.

25. For $\lambda = 0$ the substitutions of $B'_{m,n,p}$ have the form

$$S : \left\{ \begin{array}{l} \xi'_1 = \xi_1, \quad \eta'_1 = \beta_{11} \xi_1 + \eta_1 + \sum_{j=2}^m (\beta_{1j} \xi_j + \delta_{1j} \eta_j) \\ \xi'_i = \alpha_{i1} \xi_1 + \sum_{j=2}^m (\alpha_{ij} \xi_j + \gamma_{ij} \eta_j) \\ \eta'_i = \beta_{i1} \xi_1 + \sum_{j=2}^m (\beta_{ij} \xi_j + \delta_{ij} \eta_j) \end{array} \right\} \quad (i = 2, \dots, m),$$

where $\beta_{11} + \sum_{j=2}^m \beta_{1j} \delta_{1j} = 0, \quad (\beta)$

and where the $\alpha_{ij}, \gamma_{ij}, \beta_{ij}, \delta_{ij}$ ($i, j = 2, \dots, m$) are subject to the same conditions as the substitution*

$$S_1 : \left\{ \begin{array}{l} \xi'_i = \sum_{j=2}^m (\alpha_{ij} \xi_j + \gamma_{ij} \eta_j) \\ \eta'_i = \sum_{j=2}^m (\beta_{ij} \xi_j + \delta_{ij} \eta_j) \end{array} \right\} \quad (i = 2, \dots, m)$$

* The determinant of S_1 equals the determinant of S .

belonging to the group $L'_{m-1, n, p}$. To prove this statement and its inverse, we note that $B'_{m, n, p}$ contains every product of the form (see § 2)

$$R \equiv V_{2, 1, -\beta_{12}} Q_{2, 1, -\delta_{12}} \cdots V_{m, 1, -\beta_{1m}} Q_{m, 1, -\delta_{1m}}$$

which leaves ξ_1 fixed and replaces η_1 by

$$\beta_{11}\xi_1 + \eta_1 + \sum_{j=2}^m (\beta_{1j}\xi_j + \delta_{1j}\eta_j),$$

provided (β) holds. Hence every substitution of $B'_{m, n, p}$ is of the form RS_1 . The number of solutions in the $GF[p^n]$ of (β) being $p^{n(2m-2)}$, the order of $B'_{m, n, p}$ equals $p^{n(2m-2)} O'_{m-1, n, p}$, the latter factor being the order of $L'_{m-1, n, p}$.

To each substitution S there corresponds a single one S_1 . We readily verify that to the product SS' there corresponds the product $S_1S'_1$ of the corresponding substitutions. Hence,

THEOREM.—*The group $B'_{m, n, p}$ is isomorphic with the group $L'_{m-1, n, p}$; to the substitution 1 of the latter correspond the $p^{n(2m-2)}$ substitutions R of the former.*

Hence the group of the substitutions R which is generated by the $2(m-1)$ commutative substitutions

$$V_{i, 1, \lambda}, \quad Q_{i, 1, \lambda} \quad \left(\begin{array}{l} i = 2, \dots, m \\ \lambda \text{ arbitrary in } GF[p^n] \end{array} \right)$$

is an invariant sub-group of $B'_{m, n, p}$ of index $p^{n(2m-2)}$, the quotient group being $L'_{m-1, n, p}$.

This last result follows at once from the corollary to § 2. Thus the $Q_{i, j, \lambda}$ and S_U ($i, j = 2, \dots, m$), together with some one $T_{2, \nu}$ ($\nu = \text{not-square}$), generate the group $L'_{m-1, n, p}$. We have therefore only to verify the formulæ

$$Q_{i, j, \alpha}^{-1} Q_{i, 1, \lambda} Q_{i, j, \alpha} = Q_{i, 1, \lambda},$$

$$Q_{j, i, \alpha}^{-1} Q_{i, 1, \lambda} Q_{j, i, \alpha} = Q_{i, 1, \lambda} Q_{j, 1, \alpha\lambda},$$

$$Q_{i, j, \alpha}^{-1} V_{i, 1, \lambda} Q_{i, j, \alpha} = V_{i, 1, \lambda} V_{j, 1, -\alpha\lambda},$$

$$Q_{j, i, \alpha}^{-1} V_{i, 1, \lambda} Q_{j, i, \alpha} = V_{i, 1, \lambda}.$$

$$S_U^{-1} Q_{i, 1, \lambda} S_U = V_{i, 1, \lambda},$$

$$T_{2, \nu}^{-1} Q_{2, 1, \lambda} T_{2, \nu} = Q_{2, 1, \lambda\nu}.$$

26. Consider the group $B'_{m,n,p}$ with the invariants

$$\sum_{i=1}^m \xi_i \eta_i, \quad \xi_1 + \lambda \eta_1 \quad (\lambda \neq 0).$$

Its substitutions (1) must satisfy the relations (2), together with the following:—

$$(3) \quad \begin{cases} \alpha_{11} + \lambda \beta_{11} = 1, & \alpha_{ij} + \lambda \beta_{ij} = 0 \\ \gamma_{11} + \lambda \delta_{11} = \lambda, & \gamma_{ij} + \lambda \delta_{ij} = 0 \end{cases} \quad (j = 2, \dots, m).$$

Writing the same relations for the inverse of (1),

$$(3)^{-1} \quad \begin{cases} \delta_{11} + \lambda \beta_{11} = 1, & \delta_{ji} + \lambda \beta_{ji} = 0 \\ \gamma_{11} + \lambda \alpha_{11} = \lambda, & \gamma_{ji} + \lambda \alpha_{ji} = 0 \end{cases} \quad (j = 2, \dots, m).$$

27. THEOREM. — *The group $B'_{m,n,p}$ results from the extension of $L'_{m-1,n,p}$ on the indices ξ_i, η_i ($i = 2, \dots, m$) by the substitutions (which leave $\xi_1 + \lambda \eta_1$ invariant)*

$$S_{12} T_{1\lambda} T_{2\lambda} \quad \text{and} \quad Q_{2,1,\lambda} W_{1,2,\lambda\lambda}.$$

Let an arbitrary substitution S of $B'_{m,n,p}$ replace ξ_1 by

$$f_1 \equiv \sum_{j=1}^m (\alpha_{1j} \xi_j + \gamma_{1j} \eta_j),$$

where

$$(4) \quad \gamma_{11} + \lambda \alpha_{11} = \lambda, \quad \sum_{j=1}^m \alpha_{1j} \gamma_{1j} = 0.$$

From the substitutions $S_{12} T_{1\lambda} T_{2\lambda}, Q_{2,1,\lambda}, W_{1,2,\lambda\lambda}$, and those of the group $L'_{m-1,n,p}$, all of which belong to $B'_{m,n,p}$, we can derive a substitution T which shall replace ξ_1 by f_1 .

(a) If $\alpha_{1i} = \gamma_{1i} = 0$ ($i = 2, \dots, m$), we have $f_1 = \xi_1$ or $\lambda \eta_1$, so that we may take $T = 1$ or $S_{12} T_{1\lambda} T_{2\lambda}$ respectively.

(b) If $\alpha_{12} \neq 0$, for example, the group $L'_{m-1,n,p}$ contains a substitution T' replacing η_2 by

$$\alpha_{12} \xi_2 + \left(\gamma_{12} + \frac{\alpha_{11} \gamma_{11}}{\alpha_{12}} \right) \eta_2 + \sum_{j=3}^m (\alpha_{1j} \xi_j + \gamma_{1j} \eta_j);$$

indeed, by (4), the necessary condition is satisfied,

$$\alpha_{12} \left(\gamma_{12} + \frac{\alpha_{11} \gamma_{11}}{\alpha_{12}} \right) + \sum_{j=3}^m \alpha_{1j} \gamma_{1j} = 0.$$

We may thus take for T the product

$$Q_{2,1,-\lambda^{-1} \gamma_{11} \alpha_{12}^{-1}} W_{1,2,-\gamma_{11} \alpha_{12}^{-1}} T' Q_{2,1,\lambda^{-1}} W_{1,2,1},$$

which replaces ξ_1 by

$$f_1 \equiv (1 - \lambda^{-1} \gamma_{11}) \xi_1 + \gamma_{11} \eta_1 + \alpha_{12} \xi_2 + [\gamma_{12} + \gamma_{11} \alpha_{12}^{-1} (\alpha_{11} + \lambda^{-1} \gamma_{11} - 1)] \eta_2 \\ + \sum_{j=3}^m (\alpha_{1j} \xi_j + \gamma_{1j} \eta_j).$$

Thus, for both cases (a) and (b), we may set $S = TT_1$, where T_1 leaves fixed ξ_1 , and therefore also η_1 , so that T_1 belongs to $L'_{m-1, n, p}$.

28. THEOREM.—*The order of $B'_{m, n, p}$ is*

$$(p^{n(2m-2)} - 1) p^{n(2m-3)} (p^{n(2m-4)} - 1) p^{n(2m-5)} \dots (p^{2n} - 1) p^n.$$

Indeed, the order is the product of $O'_{m-1, n, p}$ by $R_{m, n, p}$, the number of solutions in the $GF[p^n]$ of the pair of equations (4), λ being a fixed quantity $\neq 0$. Eliminating γ_{11} from (4), we have

$$\lambda \alpha_{11} (1 - \alpha_{11}) + \alpha_{12} \gamma_{12} + \dots + \alpha_{1m} \gamma_{1m} = 0.$$

For $\alpha_{1m} \gamma_{1m} = 0$ this equation has

$$(2 \cdot p^n - 1) R_{m-1, n, p}$$

solutions. For $\alpha_{1m} \gamma_{1m} \neq 0$ the expression

$$\lambda \alpha_{11} (1 - \alpha_{11}) + \alpha_{12} \gamma_{12} + \dots + \alpha_{1, m-1} \gamma_{1, m-1}$$

has $(p^{n(2m-3)} - R_{m-1, n, p})$ values $\mu \neq 0$, for each of which $\alpha_{1m} \gamma_{1m} + \mu = 0$ has $(p^n - 1)$ sets of solutions. Hence we have the recursion formula

$$R_{m, n, p} = (p^n - 1) p^{n(2m-3)} + p^n R_{m-1, n, p},$$

with the initial value $R_{1, n, p} = 2$. By induction,

$$R_{m, n, p} = p^{n(m-1)} (p^{n(m-1)} + 1).$$

29. THEOREM.—*Within the group $L'_{m, n, p}$, the groups $B'_{m, n, p}$ for which λ is a square are all conjugate; likewise the groups $B'_{m, n, p}$ for which λ is a not-square are conjugate.*

Indeed, on applying to $\xi_1 + \lambda \eta_1$ the substitution $T_{1, \mu}$ belonging to $L'_{m, n, p}$, we obtain

$$\mu (\xi_1 + \lambda \mu^{-2} \eta_1).$$

30. THEOREM.—*Within the group $L'_{m, 2n, p}$ in the $GF[p^{2n}]$ all the groups $B'_{m, n, p}$ are conjugate.*

The substitution $T \equiv T_{1, \lambda^{\frac{1}{2}}} T_{2, \lambda^{\frac{1}{2}}} \dots T_{m, \lambda^{\frac{1}{2}}}$ belongs to the $GF[p^{2n}]$ if λ be a not-square. T leaves $\sum_{i=1}^m \xi_i \eta_i$ fixed,

and converts $\xi_1 + \lambda\eta_1$ into $\lambda^4(\xi_1 + \eta_1)$. Further, T transforms the general substitution of the $GF[p^n]$

$$S : \begin{cases} \xi'_i = \sum_{j=1}^m (a_{ij}\xi_j + \gamma_{ij}\eta_j) \\ \eta'_i = \sum_{j=1}^m (\beta_{ij}\xi_j + \delta_{ij}\eta_j) \end{cases} \quad (i = 1, \dots, m)$$

which leaves $\sum \xi_i\eta_i$ and $\xi_1 + \eta_1$ invariant into

$$T^{-1}ST : \begin{cases} \xi'_i = \sum_{j=1}^m (a_{ij}\xi_j + \lambda\gamma_{ij}\eta_j) \\ \eta'_i = \sum_{j=1}^m (\lambda^{-1}\beta_{ij}\xi_j + \delta_{ij}\eta_j) \end{cases} \quad (i = 1, \dots, m),$$

which belongs to the $GF[p^n]$, and leaves invariant

$$\sum_{i=1}^m \xi_i\eta_i, \quad \xi_1 + \lambda\eta_1.$$

We denote by $M'_{m,n,p}$ that particular group $B'_{m,n,p}$ for which $\lambda = 1$. Its order equals the order of the Abelian* group $H_{m-1,n,p}$ on $m-1$ pairs of indices in the $GF[p^n]$. For $p = 2$, $H_{m,n,2}$ contains $M'_{m,n,2}$ as a sub-group.

31. THEOREM.—*The groups $M'_{m,n,2}$ and $H_{m-1,n,2}$ are simply isomorphic.*

If we take† $\xi \equiv \xi_1 + \eta_1$ as a new index in place of ξ_1 and apply the relations (3) and (3)₋₁ for $\lambda = 1$, the general substitution of $M'_{m,n}$ takes the form S of § 25. The theorem follows by making the abridged substitution S_1 correspond to S .

The fact that the groups have the same order also follows from the isomorphism. Indeed, from the relations (3), (3)₋₁, and the first one of the set (2), it readily follows that, if S_1 be the identity, so is also S .

32. THEOREM.—*For $p^n = 4l+1$, the group $M'_{m,n,p}$ is simply isomorphic with the group of orthogonal substitutions of determinant unity on $2m-1$ indices in the $GF[p^n]$.*

In the case considered, -1 is the square of a mark I of the $GF[p^n]$. Introduce new indices X, Y, X_i, Y_i defined as follows:—

$$\begin{aligned} \xi_1 &= X + Y, & \eta_1 &= -X + Y, \\ \xi_i &= IX_i + Y_i, & \eta_i &= IX_i - Y_i \quad (i = 2, \dots, m). \end{aligned}$$

* Dickson, "A Triply Infinite System of Simple Groups," *The Quarterly Journal of Pure and Applied Mathematics*, July, 1897.

† This transformation of indices corresponds to the Abelian substitution L_1 . Hence the transformed substitutions are also Abelian.

The group $M'_{m,n,p}$ has the invariants

$$\xi_1 + \eta_1 \equiv 2Y,$$

$$\sum_{i=1}^m \xi_i \eta_i \equiv Y^2 - (X^2 + X_2^2 + Y_2^2 + \dots + X_m^2 + Y_m^2).$$

Expressed in terms of the new indices, every substitution of $M'_{m,n,p}$ is seen to be independent of the index Y , and therefore a linear homogeneous substitution on the indices X, Y, X_i, Y_i , leaving invariant

$$X^2 + \sum_{i=2}^m (X_i^2 + Y_i^2).$$

33. THEOREM.*—*The quaternary group $M'_{2,n,p}$ has a sub-group of index 2, which is simply isomorphic with the group of linear fractional substitutions of determinant unity in the $GF[p^n]$.*

Applying (3) and (3)₁ to certain of the relations (2), we get

$$a_{12}^2 = \beta_{12}^2 = a_{22}\beta_{22}, \quad \beta_{21}^2 = \delta_{21}^2 = \beta_{22}\delta_{22},$$

$$\gamma_{12}^2 = \delta_{12}^2 = \gamma_{22}\delta_{22}, \quad a_{21}^2 = \gamma_{21}^2 = a_{22}\gamma_{22}.$$

It follows that $a_{22}, \beta_{22}, \gamma_{22}, \delta_{22}$ are all squares or all not-squares in the $GF[p^n]$. This is evident if not more than one of them be zero; while for two of them zero it follows, since

$$a_{22}\delta_{22} + \beta_{22}\gamma_{22} = 1.$$

We may therefore take them to be $\nu a^2, \nu \beta^2, \nu \gamma^2, \nu \delta^2$, respectively, where ν is either unity or some particular not-square. We may then set

$$a_{21} = \nu a \gamma, \quad \beta_{21} = \nu \beta \delta,$$

taking the ambiguities of sign into a and δ , for example. In virtue of the relations

$$a_{11}\beta_{11} + a_{21}\beta_{21} = 0, \quad a_{11}\gamma_{11} + a_{12}\gamma_{12} = 0, \quad \beta_{11} = \gamma_{11},$$

the signs in $a_{12} = \pm \nu a \beta, \quad \gamma_{12} = \pm \nu \gamma \delta$

[* It was suggested by the Referees that this theorem should follow readily from the known theorems on the real projective transformations of a real ruled quadric. Indeed, those projective transformations which leave the generators of one set individually unchanged form a group simply isomorphic with the linear fractional group in the variable parameter giving the generators of the other set. It seems to the writer, however, that the carrying over of theorems on projective groups into theorems on groups in a Galois field must be employed with considerable caution; the reverse process is certainly impossible in general. The process is probably limited to the case in which the theorem holds in an arbitrary Galois field.—*January 28th, 1899.*]

must agree. Writing α for $\pm\alpha$, γ for $\pm\gamma$, the expressions for α_{11} and β_{11} remain unaltered, and the general substitution of $M'_{2,n,p}$ takes the form

$$\begin{pmatrix} \alpha_{11} & 1-\alpha_{11} & \nu\alpha\beta & \nu\gamma\delta \\ 1-\alpha_{11} & \alpha_{11} & -\nu\alpha\beta & -\nu\gamma\delta \\ \nu\alpha\gamma & -\nu\alpha\gamma & \nu\alpha^2 & \nu\gamma^2 \\ \nu\beta\delta & -\nu\beta\delta & \nu\beta^2 & \nu\delta^2 \end{pmatrix}.$$

The relations (2) now reduce to the following:—

$$\begin{aligned} \nu^2(\alpha\delta-\beta\gamma)^2 &= 1, \quad \alpha_{11}(\alpha_{11}-1) = \nu^2\alpha\beta\gamma\delta, \\ \rho \{1-2\alpha_{11}+\nu(\alpha\delta+\beta\gamma)\} &= 0, \end{aligned}$$

where ρ may be successively $\nu\alpha\gamma$, $\nu\alpha\beta$, $\nu\beta\delta$, $\nu\gamma\delta$. If these do not vanish simultaneously, the three relations combine to give either

$$(1) \quad \begin{cases} \alpha_{11} = \nu\alpha\delta, \\ +1 = \nu(\alpha\delta-\beta\gamma), \end{cases}$$

or

$$(2) \quad \begin{cases} \alpha_{11} = \nu\beta\gamma, \\ -1 = \nu(\alpha\delta-\beta\gamma). \end{cases}$$

The determinant of the above substitution is

$$D \equiv \nu^2(\alpha^2\delta^2-\beta^2\gamma^2) - 2 \begin{vmatrix} 1-\alpha_{11} & -\nu\alpha\beta & -\nu\gamma\delta \\ \nu\alpha\gamma & \nu\alpha^2 & \nu\gamma^2 \\ \nu\beta\delta & \nu\beta^2 & \nu\delta^2 \end{vmatrix}.$$

Applying (1) and (2), this becomes respectively

$$\begin{aligned} D &= \nu^2(\alpha^2\delta^2-\beta^2\gamma^2) - 2\nu^3\beta\gamma(\alpha\delta-\beta\gamma)^2 = \nu(\alpha\delta-\beta\gamma) = 1, \\ D &= \nu^2(\alpha^2\delta^2-\beta^2\gamma^2) + 2\nu^3\alpha\delta(\alpha\delta-\beta\gamma)^2 = \nu(\alpha\delta-\beta\gamma) = -1. \end{aligned}$$

Thus, if $p > 2$, the alternative (2) must be excluded, since the substitutions of M' have the determinant $+1$. For $p = 2$, the relation

$$\sum_{i,j}^{1,\dots,m} a_{ij}\delta_{ij} = m$$

reduces to

$$\alpha_{11} = \nu\alpha\delta.$$

Next, we suppose that all four values of ρ vanish. Then $\alpha_{11} = 0$ or 1 , while, by inspection,

$$D = (2\alpha_{11}-1)(\nu^2\alpha^2\delta^2-\nu^2\beta^2\gamma^2).$$

Since $D = +1$ and $\nu^2 (a\delta - \beta\gamma)^2 = 1$,

we have, for $a_{11} = 1$, $\nu^2 a^2 \delta^2 = 1$, $\nu\beta\gamma = 0$;

for $a_{11} = 0$, $\nu^2 \beta^2 \gamma^2 = 1$, $\nu a\delta = 0$.

We may take the ambiguities of sign into a and γ , for example, so that $\nu a\delta = +1$, $\nu\beta\gamma = 0$, when $a_{11} = 1$; while $\nu a\delta = 0$, $\nu\beta\gamma = -1$, when $a_{11} = 0$. Hence we are always led to the alternative (1), so that every substitution of M' may be given the form

$$\begin{pmatrix} \nu a\delta & -\nu\beta\gamma & \nu a\beta & \nu\gamma\delta \\ -\nu\beta\gamma & \nu a\delta & -\nu a\beta & -\nu\gamma\delta \\ \nu a\gamma & -\nu a\gamma & \nu a^2 & \nu\gamma^2 \\ \nu\beta\delta & -\nu\beta\delta & \nu\beta^2 & \nu\delta^2 \end{pmatrix},$$

where $\nu (a\delta - \beta\gamma) = 1$.

Giving it the notation $\begin{bmatrix} a & \gamma \\ \beta & \delta \end{bmatrix}_\nu$, we may verify that two such substitutions compound as follows:—

$$\begin{bmatrix} a' & \gamma' \\ \beta' & \delta' \end{bmatrix}_\nu \begin{bmatrix} a & \gamma \\ \beta & \delta \end{bmatrix}_\nu = \begin{bmatrix} a'a + \beta'\gamma & \gamma'a + \delta'\gamma \\ a'\beta + \beta'\delta & \gamma'\beta + \delta'\delta \end{bmatrix}_\nu.$$

Hence the sub-group of $M'_{2,n,p}$, of index 2, formed of those substitutions in which $\nu = 1$ (or a square) is simply isomorphic with the group of linear fractional substitutions in the $GF[p^n]$ having the determinant $+1$.

34. Consider the largest sub-group $K_{m,n,p}$ common to the Abelian group $H_{m,n,p}$ and the group $L_{m,n,p}$. The inverse* of a substitution (1) of H is obtained by replacing a_{ij} , β_{ij} , γ_{ij} , δ_{ij} by respectively δ_j^i , $-\beta_{ji}$, $-\gamma_{ji}$, a_{ji} . The inverse of a substitution (1) of L is obtained by replacing the same by δ_{ji} , $+\beta_{ji}$, $+\gamma_{ji}$, a_{ji} , respectively. Hence, if $p > 2$, every substitution (1) of K has

$$\beta_{ji} = \gamma_{ji} = 0 \quad (i, j = 1, \dots, m);$$

and therefore is the product of the two dualistic substitutions

$$\xi'_i = \sum_{j=1}^m a_{ij} \xi_j, \quad \eta'_i = \sum_{j=1}^m \delta_{ij} \eta_j \quad (i = 1, \dots, m),$$

* Jordan, § 218.

where δ_{ij} is the adjoint of α_{ij} in the determinant $|\alpha_{ij}|$. K is thus generated by the $T'_{i,\lambda}$ and $Q_{i,j,\lambda}$. Its order and structure follow from that of the general linear homogeneous group* on m indices in the $GF[p^n]$.

35. THEOREM.—For $p > 2$ the largest sub-group common to $H_{m,n,p}$ and $B_{m,n,p}$ (for $\lambda = 1$) is $K_{m-1,n,p}$.

It is clearly that sub-group of $K_{m,n,p}$ which has the invariant $\xi_1 + \eta_1$. Hence

$$\alpha_{11} = \delta_{11} = 1, \quad \alpha_{1j} = \delta_{1j} = 0 \quad (j = 2, \dots, m).$$

Writing these relations for the inverse of (1), we have

$$\delta = \alpha_{j1} = 0 \quad (j = 2, \dots, m).$$

The substitutions of the sub-group have therefore the form

$$\left\{ \begin{array}{ll} \xi'_i = \xi_i, & \xi'_i = \sum_{j=2}^m \alpha_{ij} \xi_j \\ \eta'_i = \eta_i, & \eta'_i = \sum_{j=2}^m \delta_{ij} \eta_j \end{array} \right\} \quad (j = 2, \dots, m).$$

On the Influence of Gravity on Elastic Waves, and, in particular, on the Vibrations of an Elastic Globe. By T. J. P.A. BROMWICH, B.A., Fellow of St. John's College, Cambridge.
Received December 7th, 1898. Read December 8th, 1898.
Received in recast form January 23rd, 1899.

This paper contains solutions of four elastic problems, all originally suggested by hypotheses which might modify the velocity of propagation of shocks along the surface of the earth. The first, second, and third deal with gravitational effects; hence, in these three I have assumed the material incompressible in order to avoid the difficulties that arise, even in the statical problem, if the material be compressible (Love's *Elasticity*, Vol. I., Art. 127). In the fourth

* Dickson, *Annals of Mathematics*, pp. 161–183, 1897.