§ 1. Introduction.

For application to the problem of the distribution of the substitutions of a given group into complete sets of conjugates within the group, a set of canonical forms for its substitutions should have the property that two substitutions are conjugate within the group if, and only if, they are reducible to the same canonical form according to a definite scheme of reduction. In particular, if the canonical form belongs to a higher field than the initial $GF[p^n]$, the new indices introduced must be conjugate with respect to the initial field.

In the present paper is given a set of canonical forms of quaternary abelian substitutions in the $GF[p^n]$ such that the canonical forms likewise belong to the special abelian group $SA(4,p^n)$, the reduction being effected within the group. From them are derived the ultimate canonical forms, not all belonging to the given abelian group. In the former case, the canonical forms depend on the coefficients of the characteristic equation, in the latter case upon its roots.

When the given group is the general linear homogeneous group on $m$ indices with coefficients in the $GF[p^n]$, a set of ultimate canonical forms is furnished by a theorem due (for the case $n = 1$) to Jordan. Likewise for the group of ternary linear homogeneous substitutions of determinant unity in the $GF[p^n]$, a complete set of ultimate canonical forms has been determined. The problem has also been solved for the corresponding binary group. The corresponding problem for a linear group of special character (i.e., not directly related to the general linear group) has not been previously solved so far as is known to the writer. The simplicity of the canonical substitutions for the quaternary abelian group makes comparatively easy the classification of abelian substitutions into

* Presented to the Society (Chicago) December 28, 1900. Received for publication January 5, 1901.
† Traité des substitutions, pp. 114–126. A simple proof by induction of the general theorem has been given by the writer in the American Journal of Mathematics, vol. 22, p. 121, 1900.
sets of conjugates within the abelian group (§ 23). The analogous problem is then solved (§ 25) for the simple quotient-group \( A(4, p^n) \) and the results are discussed for the case \( p^n = 3 \), which leads to a simple group of order 25920 of frequent occurrence in geometrical problems (§§ 26–27). In addition to the checks mentioned in §§ 23, 24 upon the calculations of the paper, it may be stated that the results for the case \( p^n = 3 \) were previously derived by methods independent of those employed in this paper.*

Frequent use will be made of the theorem † that the equation

\[ a\xi^2 + b\eta^2 = 1 \]

has in the \( GF[p^n] (p > 2) \), \( p^n - \nu \) solutions \((\xi, \eta)\), where \( \nu \) denotes +1 or -1 according as \(- a\beta \) is a square or a not-square in the field.

§ 2. Definition of the abelian group.

The quaternary special abelian group \( SA(4, p^n) \) is composed of the linear substitutions

\[
S: \begin{bmatrix}
\xi_1 & \eta_1 & \xi_2 & \eta_2 \\
\xi_1' & \eta_1' & \xi_2' & \eta_2'
\end{bmatrix}
\]

with coefficients in the \( GF[p^n] \) which satisfy the relations ‡

\[
\begin{align*}
(2) & \quad \begin{vmatrix} a_{11} & \gamma_{11} \\ \beta_{11} & \delta_{11} \end{vmatrix} + \begin{vmatrix} a_{12} & \gamma_{12} \\ \beta_{12} & \delta_{12} \end{vmatrix} = 1, \\
(3) & \quad \begin{vmatrix} a_{21} & \gamma_{21} \\ \beta_{21} & \delta_{21} \end{vmatrix} = 0, \\
(4) & \quad \begin{vmatrix} a_{22} & \gamma_{22} \\ \beta_{22} & \delta_{22} \end{vmatrix} = 0,
\end{align*}
\]

and equivalent relations \((2'), (3'), (4')\), formed from the columns of \((1)\) as the former were formed from its rows.

* An account of these elementary methods, sufficient for the case \( p^n = 3 \), was presented January 7, 1901, to the London Mathematical Society.
‡ For \( n = 1 \), the abelian group was studied by Jordan, Traité des substitutions, pp. 171–179; for general \( n \), it was investigated by the writer, Quarterly Journal of Mathematics, vol. 29, pp. 169–178, 1897; vol. 31, pp. 383–4, 1899.
Of the simplest substitutions satisfying these relations, the following are frequently employed in this paper, the notations being standard:†

\[
\begin{align*}
M_i^* & : \xi'_i = \eta_i, \quad \eta'_i = -\xi_i; \\
L_{i\lambda^*} & : \xi'_i = \xi_i + \lambda \eta_i; \\
L'_{i\lambda^*} & : \eta'_i = \eta_i + \lambda \xi_i; \\
T_{i\lambda^*} & : \xi'_i = \lambda \xi_i, \quad \eta'_i = \lambda^{-1} \eta_i; \\
P_{i2} & : \xi'_1 = \xi_2, \quad \eta'_1 = \eta_2, \quad \xi'_2 = \xi_1, \quad \eta'_2 = \eta_1; \\
N_{i\lambda j} & : \xi'_i = \xi_j + \lambda \eta_j, \quad \xi'_j = \xi_j + \lambda \eta_i.
\end{align*}
\]

The order \( N \) of \( SA(4, p^n) \) is \( p^{4n}(p^{4n} - 1)(p^{2n} - 1) \).

Since the general substitution (1) may be derived from the generators \( L_{i\lambda^*}, M_i \) and \( N_{i\lambda j} \), its determinant is unity.

The reciprocal of \( S \), given by (1), is

\[
S^{-1} = \begin{pmatrix}
\delta_{11} - \gamma_{11} & \delta_{21} - \gamma_{21} \\
-\beta_{11} & a_{11} - \beta_{21} & a_{21} \\
\delta_{12} - \gamma_{12} & \delta_{22} - \gamma_{22} \\
-\beta_{12} & a_{12} - \beta_{22} & a_{22}
\end{pmatrix}.
\]

It follows that the first minors (taken without prefixed sign) of \( a_{ij}, \delta_{ij}, \beta_{ij}, \gamma_{ij} \) are respectively \( \delta_{ij}, a_{ij}, \gamma_{ij}, \beta_{ij} \).

§ 3. Characteristic equation of an abelian substitution.

By definition, the characteristic determinant of \( S \) is

\[
\Delta(\kappa) \equiv \begin{vmatrix}
a_{11} - \kappa & \gamma_{11} & a_{12} & \gamma_{12} \\
\beta_{11} & \delta_{11} - \kappa & \beta_{12} & \delta_{12} \\
a_{21} & \gamma_{21} & a_{22} - \kappa & \gamma_{22} \\
\beta_{21} & \delta_{21} & \beta_{22} & \delta_{22} - \kappa
\end{vmatrix}.
\]

The constant term \( \Delta(0) \) of \( \Delta(\kappa) \) expanded according to powers of \( \kappa \) is unity, being the determinant of the substitution. The coefficient of \( -\kappa \) is

\[
\begin{align*}
\delta_{11} \beta_{12} \delta_{12} & + a_{11} a_{12} \gamma_{12} + a_{11} \gamma_{11} \gamma_{12} + a_{11} \gamma_{11} a_{12} \\
\gamma_{21} a_{22} \gamma_{22} & + a_{21} a_{22} \gamma_{22} + \beta_{11} \delta_{11} \delta_{12} + \beta_{11} \delta_{11} \beta_{12} \\
\delta_{21} \beta_{22} \delta_{22} & + \beta_{21} \beta_{22} \delta_{22} + \beta_{21} \delta_{21} \delta_{22} + a_{21} \gamma_{21} a_{22}
\end{align*}
\]

\[
= \delta_{11} + a_{11} + \delta_{22} + a_{22}:
\]

† If an index is not altered, it is not written in the formula.
The coefficient of $\kappa^2$ is the sum of six determinants of the second order. In particular, $\Delta(\kappa)$ has the form

$$\kappa^4 - (a_{11} + \delta_{11} + a_{22} + \delta_{22})\kappa^3 + (\kappa^2 - (a_{11} + \delta_{11} + a_{22} + \delta_{22})\kappa + 1.$$ 

Hence the reciprocal of any root of $\Delta(\kappa) = 0$ is itself a root. The characteristic equation of a special abelian substitution is a reciprocal equation.*

§ 4. Substitutions whose characteristic equations have all their roots in the $GF[p^n]$, no root being $\pm 1$.

Suppose first that all the roots of $\Delta(\kappa) = 0$ belong to the $GF[p^n]$. Designate them by $\kappa$, $\kappa^{-1}$, $\lambda$, $\lambda^{-1}$ and consider first the case in which no root is $\pm 1$. The root $\kappa$ leads to a linear function $\omega = a\xi_1 + b\eta_1 + c\xi_2 + d\eta_2$ which $S$ multiplies by $\kappa$. But $SA(4, p^n)$ contains a substitution $V$ which replaces $\xi_1$ by $\omega$. Then $V^{-1}SV \equiv S_1$ replaces $\xi_1$ by $\kappa\xi_1$. Likewise the root $\kappa^{-1}$, which is also a root of the characteristic equation for $S_1$, leads to a linear function

$$\omega_1 = a_1\xi_1 + b_1\eta_1 + c_1\xi_2 + d_1\eta_2,$$

which $S_1$ multiplies by $\kappa^{-1}$.

If $b_1 \neq 0$, the group contains the abelian substitution

$$U \equiv \begin{pmatrix} b_1^{-1} & 0 & 0 & 0 \\ a_1 & b_1 & c_1 & d_1 \\ -b_1^{-2}d_1 & 0 & b_1^{-1} & 0 \\ c_1 & 0 & 0 & b_1 \end{pmatrix}.$$

Then $U^{-1}S_1U$, being abelian, takes the form

$$\begin{pmatrix} \kappa & 0 & 0 & 0 \\ 0 & \kappa^{-1} & 0 & 0 \\ 0 & 0 & a & \gamma \\ 0 & 0 & \beta & \delta \end{pmatrix}.$$

From the assumption concerning $\Delta(\kappa)$, the equation

$$\begin{vmatrix} a - \kappa & \gamma \\ \beta & \delta - \kappa \end{vmatrix} = 0$$

has as its roots the distinct marks $\lambda$, $\lambda^{-1}$ of the $GF[p^n]$. Hence the given substitution $S$ is conjugate with the canonical form

* The theorem is true for any number $2m$ of indices. For proof, the direct method of the text may be employed; another proof may be based upon the canonical forms of linear substitutions in a Galois field. In a subsequent paper the writer intends to extend the present investigation to the case $2m > 4$. 

We take $\lambda \neq \kappa$ or $\kappa^{-1}$, the contrary cases leading to the type (7) below. Here $\kappa$ has $p^n - 3$ and $\lambda$ has $p^n - 5$ values if $p > 2$; while, for $p = 2$, $\kappa$ has $2^n - 2$ and $\lambda$ has $2^n - 4$ values. But the substitution (6) is transformed by $M_1$ into a similar one with $\kappa$ and $\kappa^{-1}$ interchanged; by $M_2$ into one with $\lambda$ and $\lambda^{-1}$ interchanged; by $P_{12}$ into one with $\kappa$ and $\lambda$, $\kappa^{-1}$ and $\lambda^{-1}$ interchanged. The eight resulting combinations give all the substitutions of the type (6) with the distinct roots $\kappa$, $\kappa^{-1}$, $\lambda$, $\lambda^{-1}$.

The number of types of canonical forms is therefore

$$\frac{1}{8} (p^n - 3) (p^n - 5), \text{ for } p > 2; \quad \frac{1}{8} (2^n - 2) (2^n - 4), \text{ for } p = 2.$$

The most general substitution of $SA(4, p^n)$ commutative with a given substitution (6) has the form

$$\xi' = a \xi_1, \quad \eta' = a^{-1} \eta_1, \quad \xi'_2 = b \xi_2, \quad \eta'_2 = b^{-1} \eta_2.$$ Their number being $(p^n - 1)^2$, it follows that each substitution (6) is one of $N \div (p^n - 1)^2 \equiv p^{2n}(p^{2n} + 1)(p^n + 1)^2$ conjugates within $SA(4, p^n)$.

If, however, $b_1 = 0$ in $a_0$, we may suppose that $c_1 \neq 0$. For, if $c_1 = 0$, $d_1 = 0$, then $M_2^{-1} S_1 M_2$ multiplies $a_1 \xi_1 + d_1 \xi_2$ by $\kappa^{-1}$. With $c_1 = 0$, the group contains the abelian substitution

$$V = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -a_1 c_1^{-1} \\ a_1 & 0 & c_1 & d_1 \\ 0 & 0 & 0 & c_1^{-1} \end{bmatrix}.$$ Hence $V^{-1} S_1 V$ belongs to the group and has the form

$$\begin{bmatrix} \kappa & 0 & 0 & 0 \\ \beta_{11} & \kappa^{-1} & \beta_{12} & 0 \\ 0 & 0 & \kappa^{-1} & 0 \\ \beta_{21} & 0 & \beta_{22} & \kappa \end{bmatrix} \quad (\beta_{21} = \kappa \beta_{12}).$$

Transforming by $L_1, L_2 \sigma$ and taking

$$\beta_{11} + \tau (\kappa - \kappa^{-1}) = 0, \quad \beta_{22} + \sigma (\kappa^{-1} - \kappa) = 0,$$

we find a substitution of the same form, having $\beta_{11} = \beta_{22} = 0$. If $\beta_{12} = 0$, we have the canonical form

$$\xi'_1 = \kappa \xi_1, \quad \eta'_1 = \kappa^{-1} \eta_1, \quad \xi'_2 = \kappa^{-1} \xi_2, \quad \eta'_2 = \kappa \eta_2.$$ If $\beta_{12} \neq 0$, we transform by $T_{2, \beta_{12} \kappa}$ and obtain the type

$$\xi'_1 = \kappa \xi_1, \quad \eta'_1 = \kappa^{-1} \eta_1, \quad \xi'_2 = \kappa^{-1} \xi_2, \quad \eta'_2 = \kappa \eta_2.$$
The number of non-conjugate substitutions (7) with \( \kappa^2 \neq 1 \) is \( \frac{1}{2} (p^n - 3) \) if \( p > 2 \) and \( \frac{1}{2} (2^n - 2) \) if \( p = 2 \). A substitution commutative with (7) has the form

\[
\begin{bmatrix}
\kappa & 0 & 0 & 0 \\
0 & \kappa^{-1} & \kappa^{-1} & 0 \\
0 & 0 & \kappa^{-1} & 0 \\
\kappa & 0 & 0 & \kappa
\end{bmatrix}
\]

(8)

The abelian relations give

\[a\alpha - \beta b = 1, \quad a\gamma + \delta b = 0, \quad \gamma a + b\delta = 0, \quad \beta c + d = 1.\]

Letting \( \Delta = ad - bc \), we have, as the solution of these relations,

\[a = d/\Delta, \quad \beta = c/\Delta, \quad \gamma = b/\Delta, \quad \delta = a/\Delta.\]

The number of the commutative substitutions is therefore \( (p^{2n} - 1)(p^{2n} - p^n) \), so that each substitution (7) is conjugate within \( SA(4, p^n) \) with exactly \( p^{3n}(p^{2n} + 1)(p^n + 1) \) substitutions.

The substitution (8) is transformed by \( P_{12} \) into a similar one with \( \kappa^{-1} \) in place of \( \kappa \). Hence there are \( \frac{1}{2} (p^n - 3) \) or \( \frac{1}{2} (2^n - 2) \) non-conjugate substitutions (8) with \( \kappa^2 \neq 1 \). A linear substitution commutative with (8) has the form

\[
\begin{bmatrix}
a & 0 & 0 & 0 \\
0 & a & b & 0 \\
0 & c & d & 0 \\
\gamma & 0 & 0 & \delta
\end{bmatrix}
\]

The abelian relations give

\[a\alpha - \beta b = 1, \quad a\gamma + \delta b = 0, \quad \gamma a + b\delta = 0, \quad \beta c + d = 1.\]

Letting \( \Delta = ad - bc \), we have, as the solution of these relations,

\[a = d/\Delta, \quad \beta = c/\Delta, \quad \gamma = b/\Delta, \quad \delta = a/\Delta.\]

The number of the commutative substitutions is therefore \( p^n(p^n - 1) \). Hence each substitution (8) is one of \( p^{3n}(p^{2n} - 1)(p^n + 1) \) conjugates.

\[\$ 5. \text{Roots in the field, two of them being } \pm 1.\]

Suppose next that the roots are \( \kappa, \kappa^{-1}, \pm 1, \pm 1 \), where \( \kappa \) is a mark \( \pm 0 \) or \( \pm 1 \) of the \( GF[p^n] \). The canonical form is
For $\beta = 0$ there are $p^n - 3$ or $\frac{1}{2}(2^n - 2)$ types each commutative with

\[
\begin{bmatrix}
  \kappa & 0 & 0 & 0 \\
  0 & \kappa^{-1} & 0 & 0 \\
  0 & 0 & \pm 1 & 0 \\
  0 & 0 & \beta & \pm 1
\end{bmatrix}.
\]

(9)

giving $(p^n - 1)p^n(p^{2n} - 1)$ substitutions. Hence each type yields a set of $p^{3n}(p^{2n} + 1)(p^n + 1)$ conjugate substitutions of $SA(4, p^n)$.

For $\beta \neq 0$, the substitutions with $\beta$ a square are transformed into each other by abelian substitutions $T_{2\sigma}$ and likewise those with $\beta$ a not-square. The two sets are seen to be not conjugate within $SA(4, p^n)$. The number of types is therefore $2(p^n - 3)$ or $\frac{1}{2}(2^n - 2)$ according as $p > 2$ or $p = 2$. A substitution commutative with (9) for $\beta \neq 0$, $\kappa^2 \neq 1$ has the form (10) with $b = 0$ and $a = d$. Each type is therefore commutative with $2p^n(p^n - 1)$ or $2^n(2^n - 1)$ substitutions and thus conjugate with exactly $p^{3n}(p^{4n} - 1)(p^n + 1)$ or $2^{3n}(2^{4n} - 1)(2^n + 1)$ substitutions within $SA(4, p^n)$.

§ 6. Two roots each $\pm 1$ and two roots each $\mp 1$.

If the roots are $\pm 1$, $\pm 1$, $\mp 1$, $\mp 1$, the canonical form is

\[
\begin{bmatrix}
  \pm 1 & 0 & 0 & 0 \\
  \mp 1 & 0 & 0 & 0 \\
  0 & 0 & \mp 1 & 0 \\
  0 & 0 & \beta & \mp 1
\end{bmatrix}.
\]

(11)

One may chose the lower sign, transforming if necessary by $P_{12}$.

For $a = \beta = 0$, the substitution becomes $T_{1-1}$ and, for $p > 2$, is commutative only with the $[p^n(p^{2n} - 1)]^2$ substitutions

\[
\begin{bmatrix}
  a & b & 0 & 0 \\
  c & d & 0 & 0 \\
  0 & 0 & a_1 & b_1 \\
  0 & 0 & c_1 & d_1
\end{bmatrix}.
\]

(12) $(ad - bc = 1, a_1d_1 - b_1c_1 = 1)$. 
For \( a \neq 0 \), we may suppose that \( a = 1 \) or \( \nu \), where \( \nu \) is a particular non-square in the \( GF[p^n] \); indeed, \( a \) is replaced by \( a\sigma^{-2} \) upon transforming (11) by \( T_1. \) Similarly, we may assume that \( \beta = 0, 1 \) or \( \nu \). The resulting eight types are:

\[
L_{1+T}, \quad L_{2+T}, \quad L_{1T}, \quad L_{2T}, \quad L_{1+T+L}, \quad L_{2+T+L},
\]

where \( \mu = 1 \) or \( \nu \). The number of conjugates to each may be determined directly or more simply by the method of §§ 9–10.

§ 7. Four equal roots each \( \pm 1 \).

If the roots be \( \pm 1, \pm 1, \pm 1, \pm 1 \), the canonical form is either

\[
L = \begin{bmatrix} \pm 1 & 0 & 0 & 0 \\ a & \pm 1 & 0 & 0 \\ 0 & 0 & \pm 1 & 0 \\ 0 & 0 & \beta & \pm 1 \end{bmatrix}
\]

or

\[
R = \begin{bmatrix} \beta_{11} & \pm 1 & \beta_{12} & \delta_{12} \\ \beta_{21} & 0 & \pm 1 & 0 \\ \beta_{21} & 0 & \beta_{22} & \pm 1 \end{bmatrix}
\]

according as the linear function \( \omega \), determined by the second root \( \pm 1 \) contains \( \eta \) or does not. If \( \beta_{12} = \delta_{12} = 0 \), \( R \) is of the form \( L \). If \( \delta_{12} = 0 \), \( \beta_{12} \neq 0 \), the transform of \( R \) by \( T_{2\beta_{12}} \) is of the form \( R \) with \( \beta_{12} = 1, \delta_{12} = 0 \). The abelian relations give \( \beta_{21} = 0, \beta_{21} = 1 \). Then, for \( \beta_{11} \neq 0 \), we transform by the abelian substitution

\[
\xi_1' = \xi_1 + \beta_{11}^{-1} \xi_2, \quad \eta_2 = \eta_2 - \beta_{11}^{-1} \eta_1,
\]

and reach a substitution of the form \( L \). A similar result follows if \( \beta_{11} = 0, \beta_{22} \neq 0 \), since the transform of \( R \) by \( P_{12} \) then has \( \beta_{11} \neq 0 \). Finally, if \( \beta_{11} = \beta_{22} = 0 \), we have the substitution

\[
(13)
\]

For \( p > 2 \), this is transformed into \( L \) (with \( a = 1, \beta = -1 \)) by

\[
\begin{bmatrix} 1 & 0 & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & 0 & 1 \\ -1 & 0 & \frac{1}{2} & 0 \\ 0 & -\frac{1}{2} & 0 & 1 \end{bmatrix}
\]
For \( p = 2 \), substitution (13) will be seen to furnish a new type. A substitution (1) commutative with (13) must have the form

\[
\begin{bmatrix}
    a_{11} & 0 & a_{12} & 0 \\
    \beta_{11} & \delta_{11} & \beta_{12} & \delta_{12} \\
    \delta_{12} & 0 & \delta_{11} & 0 \\
    \beta_{21} & a_{12} & \beta_{22} & a_{11}
\end{bmatrix}
\]

subject to the abelian conditions

\[
a_{11}\delta_{11} + a_{12}\delta_{12} = 1, \quad \beta_{11}a_{12} + \delta_{11}\beta_{21} + a_{11}\beta_{12} + \delta_{12}\beta_{22} = 0.
\]

By the former, \( a_{11} \) and \( a_{12} \) are not both zero, so that the latter determines one of the \( \beta_{ij} \) in terms of the other three, which may be chosen arbitrarily in the \( GF[2^n] \). Hence there are \( 2^n(2^{2n} - 1)2^{3n} \) substitutions of \( SA(4, 2^n) \) commutative with (13). A substitution \( L \) is conjugate with the identity or \( L_{11} \) or \( L_{11}L_{21} \). By \( \S \) 10, \( L_{11}L_{21} \) is commutative with exactly \( 2^{4n} \) substitutions of \( SA(4, 2^n) \), so that \( L_{11}L_{21} \) and (13) are not conjugate within the group. A different argument is necessary for the case of \( L_{11} \) and (13); but the latter are readily shown to be not conjugate under abelian transformation.

It remains to consider \( R \) when \( \delta_{12} \neq 0 \). The transformed of \( R \) by \( T_2 \delta_{12} \) is of the form \( R \) with \( \delta_{12} = 1 \). The latter is transformed by \( L_{2} \beta_{12} \) into the substitution

\[
R_1 = \begin{bmatrix}
    \pm 1 & 0 & 0 & 0 \\
    \beta_{11} & \pm 1 & 0 & 1 \\
    -1 & 0 & \pm 1 & 0 \\
    \mp a & 0 & a & \pm 1
\end{bmatrix}
\]

Suppose first that \( p = 2 \). If \( a = 0 \), the transform of \( R_1 \) by \( M_2 \) is of the form \( R \) with \( \delta_{12} = 0 \), a case previously considered. If \( a \neq 0 \), the transform of \( R_1 \) by \( T_1T_2k \) is of the form \( R_1 \) with \( \kappa^{-2} a \) in place of \( a \). Choosing \( \kappa = a^k \), we obtain a substitution

\[
R_\beta = \begin{bmatrix}
    1 & 0 & 0 & 0 \\
    \beta & 1 & 0 & 1 \\
    1 & 0 & 1 & 0 \\
    1 & 0 & 1 & 1
\end{bmatrix}
\]

of period 4. Transforming \( R_\beta \) by the abelian substitution

\[
\xi'_1 = \xi_1, \quad \eta'_1 = \eta_1 + \tau\eta_2 + \tau^2\xi_2, \quad \xi'_2 = \xi_2 - \tau\xi_1, \quad \eta'_2 = \eta_2 + \tau\xi_2,
\]

we obtain, for \( p = 2 \), the substitution \( R_\kappa \), where \( \beta = \beta + \tau + \tau^2 \). In order
that the $GF[2^n]$ shall contain a mark $\tau$ for which $b = 0$, it is necessary and sufficient that

$$B \equiv \beta + \beta^2 + \beta^4 + \ldots + \beta^{2n-1} = 0.$$  

Since $\beta$ belongs to the field, $B^2 = B$. Inversely, there are $2^{n-1}$ marks $\beta$ making $B = 0$ and as many making $B = 1$. The $2^{n-1}$ substitutions $R_\beta$ for which $B = 0$ are therefore conjugate within $SA(4, 2^n)$. Likewise the $2^{n-1}$ substitutions $R_\beta$ for which $B = 1$ are all conjugate; indeed, $R_\beta$ is conjugate with $R_b$ and $b \equiv \beta + \tau + \tau^2$ takes $2^{n-1}$ distinct values when $\tau$ runs through the series of $2^n$ marks, while

$$b + b^2 + b^4 + \ldots + b^{2n-1} \equiv \beta + \beta^2 + \beta^4 + \ldots + \beta^{2n-1} + \tau + \tau^2 \equiv B \pmod{2}.$$

That the substitutions $R_\beta$ for which $B = 1$ are not conjugate with $R_0$ may be shown by considering the condition $R_\beta S = SR_0$, $S$ being of the general form (1). We find that $S$ must have the form

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ \beta_{11} & 1 & \beta_{12} & \beta_{22} \\ \beta_{22} & 0 & 1 & 0 \\ \beta_{21} & 0 & \beta_{22} & 1 \end{pmatrix} \quad \begin{pmatrix} \beta_{21} = \beta_{12} + \beta_{22} + \beta \\ \beta_{21} = \beta_{12} + \beta_{22} \end{pmatrix}.$$

The latter conditions require that $\beta + \beta_{22} + \beta_{22}^2 \equiv 0 \pmod{2}$.

For $p = 2$, the only substitutions of $SA(4, 2^n)$ commutative with $R_\beta$ are of the form (14) subject, however, to the conditions

$$\beta_{21} = \beta_{12} + \beta_{22}^2 \quad \beta_{21} = \beta_{12} + \beta_{22}.$$

Hence $\beta_{22} = 0$ or $1$, while $\beta_{11}$ and $\beta_{12}$ are arbitrary; thus there are $2 \cdot 2^{2n}$ substitutions.

For $p > 2$, $R_\beta$ is transformed into a similar substitution $R'$ having $\beta_{11} = 0$ by the following abelian substitution

$$\eta'_1 = \eta_1 + \frac{1}{2} \beta_{11} \xi_2, \quad \eta'_2 = \eta_2 + \frac{1}{2} \beta_{11} \xi_1.$$

For $a = 0$, the transform of $R'$ by $M_2$ is of the form (13).

For $a \neq 0$, the transform of $R'$ by $T_{1+1}$ gives the substitutions

$$A_a = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ -1 & 0 & 1 & 0 \\ -a & 0 & a & 1 \end{pmatrix}, \quad A_{-a} T_{1+1} T_{2+1}.$$  

Transforming $A_a$ by $T_{1+1} T_{2+1}$ we obtain $A_{a-2}$. Hence, if $p > 2$, there are only four canonical types, $v$ being a particular not-square:
The substitutions $A_\mu$ and $A_\mu T_{1-1} T_{2-1}$ are not conjugate, if $p > 2$, their characteristic equations having different roots. But every substitution commutative with one is commutative with the other, $T_{1-1} T_{2-1}$ being commutative with every quaternary linear substitution. The period of $A_\mu$ is readily seen to be $p$ if $p > 3$, 9 if $p = 3$, or 4 if $p = 2$. Then $A_\mu T_{1-1} T_{2-1}$ is of period $2p$ if $p > 3$, 18 if $p = 3$, or 4 if $p = 2$.

If $S$ be the general substitution (1), the identity $A_a S = S A_a$, requires that

$$
\begin{align*}
\gamma_{11} &= \gamma_{22} = \gamma_{21} = \gamma_{12} = a_{12} = \delta_{21} = 0, \\
a_{22} &= \alpha_{11}, \\
\delta_{22} &= \delta_{11}, \\
\beta_{22} &= \alpha \delta_{12}, \\
\beta_{21} &= -\beta_{12} - \alpha \delta_{12}, \\
\alpha \delta_{22} &= \alpha \alpha_{22}, \\
-a\alpha_{11} + \alpha \alpha_{21} &= -\beta_{22} - \alpha \delta_{22}.
\end{align*}
$$

The second abelian relation (2) then gives $a_{22} \delta_{22} = 1$, whence

$$a \delta_{22}^2 = \alpha'.$$

Hence $A_a$ and $A_{a'}$ are conjugate within $SA(4, p^n)$ only when $a$ and $a'$ are both squares or both not-squares in the $GF[p^n]$. To determine the substitutions $S$ commutative with $A_a$, set $a' = a$. Then

$$S = \begin{bmatrix}
\alpha_{11} & 0 & 0 & 0 \\
\beta_{11} & \alpha_{11} & \beta_{12} & \delta_{12} \\
-\delta_{12} & 0 & \alpha_{11} & 0 \\
-\beta_{12} - \alpha \delta_{12} & 0 & \alpha \delta_{12} & \alpha_{11}
\end{bmatrix},$$

subject to the abelian relations

$$a_{11}^2 = 1, \quad 2a_{11} \beta_{12} + a \alpha_{11} \delta_{12} - a \delta_{12}^2 = 0.$$ 

For each of the two values of $a_{11}$, the second relation determines $\delta_{12}$. Hence there are $2p^{2n}$ substitutions commutative with $A_a$. Hence each of the substitutions (15) is conjugate with exactly $\frac{1}{2}p^{2n}(p^{2n} - 1)(p^{2n} - 1)$ substitutions within $SA(4, p^n)$, while no two of the four canonical types are conjugate.

§ 8. Study of the abelian substitutions of type $L$.

Upon transforming $L$ by $T_{1-1} T_{2-1}$, we obtain a substitution of the form $L$ with $\alpha, \beta$ replaced by $a \alpha^{-2}, \beta \alpha^{-2}$. Hence the substitutions $L$ are conjugate with one of the following:

* For example, by introducing the new indices

$$X = -\xi_1, \quad Y = \xi_2, \quad Z = \xi_2 - a^{-1} \eta_1, \quad W = -a^{-1} \eta_1 - \xi_2 + a^{-1} \eta_2,$$

$A_a$ takes the standard canonical form (not abelian):

$$X' = X, \quad Y' = Y + X, \quad Z' = Z + Y, \quad W' = W + Z.$$
Of these, \( L_{11}L_{2\nu} \) is transformed into \( L_{1\nu}L_{21} \) by \( P_{12} \), and \( L_{11}L_{21} \) is transformed into \( L_{1\nu}L_{2\nu} \) by the abelian substitution:

\[
\begin{pmatrix}

\nu\delta & 0 & \nu\sigma & 0 \\
0 & \delta & 0 & \sigma \\
-\nu\sigma & 0 & \nu\delta & 0 \\
0 & -\sigma & 0 & \delta
\end{pmatrix},
\]

subject only to the condition \( \nu(\delta^2 + \sigma^2) = 1 \), which has solutions in every \( GF[p^n] \). The identity and \( T_{1-1}T_{2-1} \) are conjugate only with themselves. Hence the types \( L \) remaining for consideration are:

\[
L_{1\mu}, \ L_{1\mu}T_{1-1}T_{2-1}, \ L_{1\mu}L_{21}, \ L_{1\mu}L_{21}T_{1-1}T_{2-1} \quad (\mu = 1, \nu).
\]

The characteristic equations for the second and fourth substitutions have the roots \(-1\) and hence are not conjugate with the first or third.

The substitutions \( L_{11} \) and \( L_{1\nu} \), \( \nu \) being a not-square in the \( GF[p^n] \), \( p > 2 \), are not conjugate within the \( SA(4, p^n) \). In fact, \( SL_{11} = L_{1\nu}S \) gives the conditions:

\[
\beta_{11} = 0, \quad \delta_{11} = \nu a_{11}, \quad \beta_{12} = \beta_{21} = a_{21} = \delta_{12} = 0.
\]

Thus \( S \) does not satisfy the abelian relation (2):

\[
1 = a_{11}\delta_{11} - \beta_{11}\gamma_{11} + a_{12}\delta_{12} - \beta_{12}\gamma_{12} \equiv \nu a_{11}^2.
\]

The fact that \( L_{11}L_{21} \) and \( L_{1\nu}L_{21} \) are not conjugate with each other and that neither is conjugate with either \( L_{11} \) or \( L_{1\nu} \) within \( SA(4, p^n) \) follows incidentally from the following determination of the number of abelian substitutions conjugate with each of the four. To determine the number of substitutions of \( SA(4, p^n) \) conjugate with \( L_{1\mu}L_{2\tau} \), let \( S \) denote the general substitution (1) commutative with it. The conditions for the identity

\[
SL_{1\mu}L_{2\tau} = L_{1\mu}L_{2\tau}S \quad (\mu \neq 0)
\]

are found at once to be the following:

\[
\beta_{11} = 0, \quad \beta_{12} = 0, \quad \beta_{21} = 0, \quad a_{11} = \delta_{11}, \quad \tau \beta_{22} = 0, \quad \mu a_{21} = \tau \delta_{21}, \quad \mu \delta_{12} = \tau a_{12}, \quad \tau a_{22} = \tau \delta_{22}.
\]

For \( \tau = 0 \), \( S \) has the form:

\[
\begin{pmatrix}
a_{11} & \gamma_{11} & a_{12} & \gamma_{12} \\
0 & a_{11} & 0 & 0 \\
0 & \gamma_{21} & a_{22} & \gamma_{22} \\
0 & \delta_{21} & \beta_{22} & \delta_{22}
\end{pmatrix}.
\]
In particular, an abelian relation gives $a_{11}^2 = 1$. Hence $S = Y$ or $T_{1-1} Y$, where $Y$ is the most general substitution of $SA(4, p^n)$ which leaves $\eta_1$ fixed. The number of substitutions $Y$ is $p^{3n} p^n (p^{2n} - 1)$, being equal to the number of substitutions of $SA(4, p^n)$ which leave fixed the index $\xi_1$.* According as $p > 2$ or $p = 2$, $L_{1\mu}$ is one of $\frac{1}{2}(p^{2n} - 1)$ or $2^n - 1$ conjugate substitutions within $SA(4, p^n)$.

For $\tau = 1$, a substitution $S$ commutative with $L_{1\mu} L_{21}$ has the form

$$
\begin{bmatrix}
    a_{11} & \gamma_{11} & \mu \delta_{12} & \gamma_{12} \\
    0 & a_{11} & 0 & \delta_{12} \\
    a_{21} & \gamma_{21} & a_{22} & \gamma_{22} \\
    0 & \mu a_{21} & 0 & a_{22}
\end{bmatrix}
$$

subject to the abelian relations

$$a_{11}^2 + \mu \delta_{12}^2 = 1, \quad a_{22}^2 + \mu a_{21}^2 = 1, \quad a_{11}^2 + \mu a_{21}^2 = 1,$$

$$a_{11} a_{21} + \delta_{12} a_{22} = 0, \quad a_{11} \gamma_{21} - \gamma_{11} a_{21} + \mu \delta_{12} \gamma_{22} - \gamma_{12} a_{22} = 0.$$ 

Hence

$$\delta_{12}^2 = a_{21}^2, \quad a_{22} = \pm a_{11}, \quad a_{11}(a_{21} \pm \delta_{12}) = 0.$$

Suppose first that $\mu$ is a not-square $\nu$ in the $GF[p^n], p \geq 2$. Then $a_{11} \neq 0$ and $a_{21} = \mp \delta_{12}, a_{22} = \pm a_{11}$. For any one of the $p^n + \epsilon$ sets of solutions of $a_{11}^2 + \nu \delta_{12}^2 = 1$, $\epsilon$ being $\pm 1$ according as $p^n = 4l \pm 1$, $a_{21}$ and $a_{22}$ are determined except in sign; while $\gamma_{21}$ is determined in terms of $\gamma_{11}, \gamma_{12}, \gamma_{22}$. Hence there are $2p^{3n}(p^n + \epsilon)$ substitutions of $SA(4, p^n)$ commutative with $L_{1\nu} L_{21}$.

Suppose next that $\mu = 1$. Whether $a_{11}$ be zero or not, we may set $a_{22} = \pm a_{11}, a_{21} = \mp \delta_{12}$. For any one of the $p^n - \epsilon$ sets of solutions of $a_{11}^2 + \delta_{12}^2 = 1$ in the $GF[p^n], p \geq 2$, $a_{22}$ and $a_{21}$ are determined except in sign, and one of the $\gamma_{ij}$ is determined in terms of the remaining three. Hence there are $2p^{3n}(p^n - \epsilon)$ substitutions of $SA(4, p^n), p \geq 2$, commutative with $L_{111} L_{21}$. For $p = 2$, we get $a_{22} = a_{11}, \delta_{12} = a_{21}, a_{11} + \delta_{12} = 1$, so that $SA(4, 2^n)$ contains exactly $2^n$ substitutions commutative with $L_{111} L_{21}$.

§ 9. Study of the substitutions $L_{1\mu} T_{1-1}$ and $L_{1\mu} T_{2-1}$ $(\mu = 1$ or $\nu$).

If $\nu$ be a not-square in the $GF[p^n], p \geq 2$, no two of the substitutions $L_{111} T_{1-1}, L_{1\nu} T_{1-1}, L_{111} T_{2-1}, L_{1\nu} T_{2-1}$ are conjugate within $SA(4, p^n)$. The first two are not conjugate and the last two are not conjugate since their $(p + 1)$-th powers are $L_{111}$ and $L_{1\nu}$, and are not conjugate by § 8. Finally, a relation $SL_{1\mu} T_{1-1} = L_{1\nu} T_{2-1} S$ is proved impossible by forming the respective products.
Within $SA(4, p^n), p > 2$, each of the four substitutions is one of a complete set of $\frac{1}{2}p^{2n}(p^n - 1)$ conjugate substitutions. In proof, let $S$ be an abelian substitution commutative with $L_{1, \mu} T_{1, -1}$. Then $S$ is commutative with the $p$-th and $(p + 1)$-th powers of the latter, which are $T_{1, -1}$ and $L_{1, \mu}$ respectively. Hence $S$ is at the same time of the forms (12) and (16). Hence

$$S = \begin{bmatrix} a_{11} & \gamma_{11} & 0 & 0 \\ 0 & a_{11} & 0 & 0 \\ 0 & 0 & a_{22} & \gamma_{22} \\ 0 & 0 & \beta_{22} & \delta_{22} \end{bmatrix},$$

subject to the abelian relations

$$a_{11}^2 = 1, \quad a_{22}\delta_{22} - \beta_{22}\gamma_{22} = 1.$$

The number of substitutions $S$ is therefore $2p^np^n(p^n - 1)$.

A substitution $S'$ commutative with $L_{1, \mu} L_{2, -1}$ will be commutative with $L_{1, \mu} T_{2, -1}, T_{1, -1} T_{2, -1} \equiv L_{1, \mu} T_{1, -1}$ and vice versa. Hence every $S'$ is an $S$ and vice versa. Hence the final theorem:

**Within $SA(4, p^n), p > 2$, the substitutions $L_{1, \mu} T_{1, -1}, L_{1, \mu} T_{2, -1}, L_{1, \nu} T_{1, -1}$ and $L_{1, \nu} T_{2, -1}$, where $\nu$ is a not-square in the field, are not conjugate and each gives rise to a complete set of $p^{2n}(p^n - 1)$ conjugate substitutions.**

§ 10. Study of the substitutions $L_{1, \mu} L_{1, -1} L_{2, \tau} (\mu, \tau = 1$ or $\nu)$.

The substitutions $L_{1, \mu} L_{1, -1} L_{2, 1}$ and $L_{1, \mu} L_{1, -1} L_{2, 1}$ are not conjugate within $SA(4, p^n), p > 2$. Indeed, their $p + 1$-th powers, $L_{1, \mu} L_{2, \nu}$ and $L_{1, \tau} L_{2, \nu}$ are not conjugate within $SA(4, p^n)$. Finally, $L_{1, \mu} L_{1, -1} L_{2, 1}$ is not conjugate with $L_{1, \tau} L_{1, -1} L_{2, \nu}$; for, if $S$ transform the former into the latter, it is seen that $S$ must replace $\xi_2$ by $v\delta_{22}\xi_2 + \gamma_2\eta_2$ and $\eta_2$ by $\delta_{22}\xi_2$, where $v\delta_{22}^2 = 1$. Combining the four non-conjugate substitutions into the single type $E \equiv L_{1, \mu} L_{1, -1} L_{2, \tau}$, where $\mu, \tau = 1, \nu$, it will be shown that each $E$ is commutative with exactly $4p^{2n}$ substitutions of $SA(4, p^n), p > 2$, and hence is one of a set of $\frac{1}{2}(p^n - 1)(p^{2n} - 1)p^{2n}$ conjugate substitutions. In proof, let $S$ be commutative with $E$. Then $S$ must be commutative with $E^\tau = T_{1, -1}$, so that $S$ must be of the form (12). Also $S$ must be commutative with $E^{\mu + 1} = L_{1, \mu} L_{2, \tau}$, and hence have $\beta_{11} = 0, \beta_{22} = 0, a_{11} = \delta_{11}, a_{22} = \delta_{22}$ (§ 8). Hence $S$ has the form

$$\begin{bmatrix} a & \gamma & 0 & 0 \\ 0 & a & 0 & 0 \\ 0 & 0 & a_{22} & \gamma_{22} \\ 0 & 0 & 0 & a_{22} \end{bmatrix},$$

$(a^2 = a_{22}^2 = 1)$.

Inversely, each of these substitutions is evidently commutative with $E$. 
In view of the number of the substitutions of $SA(4, p^n)$ commutative with the substitutions $E$ and the number commutative with the four of § 9, none of the latter are conjugate with a substitution $E$.

§ 11. Canonical form of a binary substitution of irreducible characteristic determinant.

Theorem. A binary linear substitution in the $GF[p^n]$

$$
\Sigma \equiv \begin{pmatrix} a & \gamma \\ \beta & \delta \end{pmatrix}
$$

whose characteristic determinant $D(\kappa) \equiv \kappa^2 - \kappa(a + \delta) + 1$ is irreducible in the field may be transformed into the canonical form

$$
\Sigma_1 \equiv \begin{pmatrix} 0 & 1 \\ -1 & a + \delta \end{pmatrix}
$$

by a linear substitution of determinant unity and belonging to the field.

If $\beta \gamma = 0$, then $D(\kappa) = (\kappa - a)(\kappa - \delta)$, contrary to hypothesis. Transforming $\Sigma$ by $\begin{pmatrix} 1 & 0 \\ \alpha/\gamma & 1 \end{pmatrix}$, we obtain $\Sigma \equiv \begin{pmatrix} 0 & \gamma \\ -\gamma^{-1} & a + \delta \end{pmatrix}$. If $\gamma$ be a square in the field, the transform of $\Sigma$ by $T_{1,\gamma^{1/2}}$ gives $\Sigma_1$. If $\gamma$ be a not-square, so that $p > 2$, the transform of $\Sigma$ by $\begin{pmatrix} 1 & \tau \\ 0 & 1 \end{pmatrix}$ is a substitution of the form $\Sigma$ with $c \equiv \gamma + \tau(a + \delta) + \tau^2\gamma^{-1}$ in place of the coefficient $\gamma$. Since

$$
c\gamma^{-1} = 1 + \tau\gamma^{-1}(a + \delta) + (\tau\gamma^{-1})^2
$$

is irreducible in the field, $c$ cannot vanish. Moreover, at most two values of $\tau$ give the same value to the expression $c$. Hence $c$ has at least $\frac{1}{2}(p^n + 1)$ values $\neq 0$, at least one of which is therefore a square in the field. By the earlier case, the substitution is conjugate with $\Sigma_1$.

By an analogous proof, $\Sigma$ may be transformed into

$$
\Sigma_1^{-1} \equiv \begin{pmatrix} a + \delta & -1 \\ 1 & 0 \end{pmatrix}
$$

§ 12. Substitutions whose characteristic determinant is the product of two linear factors and an irreducible quadratic factor.

Let the characteristic determinant $\Delta(\kappa)$ of the abelian substitution $S$ be the product of two linear factors and an irreducible quadratic factor each belonging to the $GF[p^n]$. Denote the roots of the former by $a$, $b$ and those of the latter by $\lambda$, $\lambda^{p^n}$. Then ($\S 3$), $b = a^{-1}$, $\lambda^{p^n} = \lambda^{-1}$; hence $\lambda^{p^n+1} = 1$, $\lambda^{p^n-1} \neq 1$, the latter excluding only the two roots $\pm 1$ of the former, so that $\lambda$ may have $p^n - 1$ or $2^n$ distinct values, according as $p > 2$ or $p = 2$. 

If \( a^{-1} \neq a \), \( S \) may be transformed by a substitution of \( SA(4, p^n) \) into a substitution \( S' \) which replaces \( \xi_1 \) by \( a\xi_1 \) and \( \eta_1 \) by \( a^{-1}\eta_1 \). On account of the abelian conditions, \( S' \) is seen to affect \( \xi_2, \eta_2 \) according to a substitution of the form

\[
\Sigma = \begin{pmatrix} a & \gamma \\ \beta & \delta \end{pmatrix} \quad (a\delta - \beta\gamma = 1).
\]

From the invariance of \( \Delta(\kappa) \), it follows that \( \lambda, \lambda^{-1} \) are the roots of

\[ \kappa^2 - \kappa(\alpha + \delta) + 1 = 0. \]

In particular, the latter is irreducible in the \( GF[p^n] \). By \( \S 11 \), there exists a substitution on \( \xi_2, \eta_2 \) with coefficients in the field and having determinant unity which transforms \( \Sigma \) into

\[
\Sigma_1 = \begin{pmatrix} 0 & 1 \\ -1 & a + \delta \end{pmatrix}.
\]

A substitution \( S \) of the group \( SA[4, p^n] \) whose characteristic determinant is the product of two distinct linear factors \( \kappa - a, \kappa - a^{-1} \) and an irreducible quadratic factor \( \kappa^2 - A\kappa + 1 \) is conjugate within the group with the canonical substitution

\[
\begin{pmatrix} a & 0 & 0 & 0 \\ 0 & a^{-1} & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & A \end{pmatrix}
\]

(18')

If \( a^{-1} = a \), \( S \) may be transformed by a substitution of the group into a substitution \( S_1 \) which replaces \( \xi_1 \) by \( a\xi_1 \) and \( \eta_1 \) by \( a\eta_1 + b\xi_1 \) and therefore \( \xi_2, \eta_2 \) by linear functions of \( \xi_2, \eta_2 \) only. If \( b \neq 0 \), we transform \( S_1 \) by \( T_1 \), and obtain a substitution of the form \( S_1 \) with \( e^{-2b} \) in place of \( b \), so that \( b \) may be restricted to unity and (for \( p > 2 \)) a particular not-square \( \nu \) of the field. The canonical forms within \( SA(4, p^n) \) of substitutions whose characteristic determinant is the product of two equal linear factors \( \kappa = 1 \) and an irreducible quadratic factor \( \kappa^2 - A\kappa + 1 \) are

\[
\begin{pmatrix} \pm 1 & 0 & 0 & 0 \\ b & \pm 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & A \end{pmatrix}
\]

(19') \quad (b = 0, 1 \) or \( \nu \).

To obtain ultimate canonical forms, we introduce the new indices, conjugate with respect to the \( GF[p^n] \),

\[
X = -\xi_2 + \lambda\eta_2, \quad Y = -\xi_2 + \lambda^{-1}\eta_2.
\]

Then (18') and (19') each replace \( X \) by
- $\lambda \xi_2 + (\lambda A - 1) \eta_2 = - \lambda \xi_2 + \lambda^2 \eta_2 = \lambda(- \xi_2 + \lambda \eta_2)$.

Hence (18') and (19') are reducible to the canonical forms

$$(18) \quad \xi' = a \xi_1, \quad \eta' = \alpha^{-1} \eta, \quad X' = \lambda X, \quad Y' = \lambda^{-1} Y$$

$$(a \pm 1),$$

$$(19) \quad \xi' = \pm \xi_1, \quad \eta' = \pm \eta_1 + b \xi_1, \quad X' = \lambda X, \quad Y' = \lambda^{-1} Y.$$

Two substitutions of $SA(4, p^n)$ reducible in this manner to the same canonical form (18) or (19) are conjugate within the group and inversely.

There are $(p^n - 1) (a + 1)$ or $2^{n-1} (a - 1)$ non-conjugate canonical types (18). Indeed, $M_1$ transforms (18) into a like substitution with $a$ and $a^{-1}$ interchanged; $M_2$ transforms (18) into a like substitution with $\lambda$ and $\lambda^{-1}$ interchanged. A substitution of $SA(4, p^n)$ commutative with one having the canonical form (18) has simultaneously the canonical form

$$(18) \quad \xi' = c \xi_1, \quad \eta' = c^{-1} \eta, \quad X' = \tau X, \quad Y' = \tau^{-1} Y,$$

where $c$ is any mark $\neq 0$ of the $GF[p^n]$ and $\tau$ any root of $\tau^{p^{n+1}} = 1$, giving $(p^n - 1)(p^n + 1)$ substitutions. Hence each type (18) represents a complete set of $p^n (p^n - 1)$ conjugate substitutions of $SA(4, p^n)$.

For $b = 0$, there are $p^n - 1$ or $2^{n-1}$ non-conjugate types (19). A substitution of $SA(4, p^n)$ commutative with one having the canonical form (19) with $b = 0$ has simultaneously the canonical form

$$(20) \quad \xi' = r \xi_1 + s \eta, \quad \eta' = t \xi_1 + u \eta, \quad X' = \tau X, \quad Y' = \tau^{-1} Y,$$

where $ru - st = 1$, giving $p^n (p^n - 1)(p^n + 1)$ substitutions. Each type thus represents $p^n (p^n - 1) (p^n + 1)$ conjugate substitutions of $SA(4, p^n)$.

For $b = 1$ or a not-square $\nu$, there are altogether $(p^n - 1) + 2^{n-1}$ non-conjugate types (19). The commutative substitutions have the canonical form (20) with $s = 0$, $r = u = \pm 1$, giving $2p^n (p^n + 1)$ or $2^{n-1} (2^n + 1)$ substitutions. Hence each type represents a set of $\frac{1}{2} p^n (p^n - 1)(p^n + 1)$ or $2^{n-1} (2^n - 1)(2^n + 1)$ conjugate substitutions.

§ 13. Substitutions whose characteristic equations have no root in the $GF[p^n]$.

**Theorem.** Within $SA(4, p^n)$ any substitution $S$, whose characteristic equation $\Delta(\kappa) = 0$ has no root in the $GF[p^n]$, is conjugate with a substitution replacing $\xi_1$ by $\gamma \eta_1$.

Let $S$ replace $\xi_1$ by $\omega = a_1 \xi_1 + \gamma_1 \eta_1 + a_2 \xi_2 + \gamma_2 \eta_2$. Suppose first that $\gamma_{11} \neq 0$. There exists in $SA(4, p^n)$ a substitution $T$ which replaces $\xi_1$ by $\gamma_{11}^{-1} \xi_1$ and $\eta_1$ by $\omega$ [compare § 4]. Then $T^{-1}ST$ replaces $\xi_1$ by $\gamma_{11}^{-1} \eta_1$. The same result will follow if $S$ be conjugate within $SA(4, p^n)$ with a substitution having $\gamma_{11} \neq 0$. In the contrary case $\gamma_{11} = \beta_{11} = \gamma_{22} = \beta_{22} = 0$ in $S$ and all its conjugates; indeed, by transforming $S$ by $M_1$, $P_{12}$ or $P_{12} M_1$, we may bring the
coefficient $\beta_{11}$, $\gamma_{22}$ or $\beta_{22}$ in the place of the former $\gamma_{11}$. By an earlier transformation, we can make $\beta_{12} = \gamma_{12} = 0$. The resulting substitution is

$$S' = \begin{bmatrix} a_{11} & a_{12} & 0 \\ 0 & \delta_{11} & \delta_{12} \\ a_{21} & \gamma_{21} & a_{22} \\ 0 & \delta_{21} & \delta_{22} \end{bmatrix}.$$  

The transform of $S'$ by $\eta'_1 = \eta_1 + \eta_2$, $\xi'_2 = \xi_2 - \xi_1$ has $\beta_{21}$ as the coefficient of $\xi_1$ in $\eta'_1$. Hence $\beta_{21} = 0$. Similarly $\gamma_{21} = 0$. Next $L_{11}$ transforms $S'$ into a substitution with $\delta_{11} = a_{11}$ and similarly $\delta_{22} = a_{22}$. The transform of $S'$ by $N_{12}$: $\xi'_1 = \xi_1 + \eta_2$, $\xi'_2 = \xi_2 + \eta_1$, has $\delta_{21} = a_{12}$ as the coefficient of $\eta_1$ in $\xi'_1$. Hence $a_{12} = \delta_{21}$ and similarly $a_{21} = \delta_{12}$. Now $a_{12}$ or $\delta_{12}$ is not zero, since otherwise the characteristic equation has a root $a_{11}$ or $\delta_{11}$ in the field. The transformed of $S'$ by

$$\xi'_1 = \xi_1 + \tau \xi_2, \quad \eta'_2 = \eta_2 - \tau \eta_1 \quad (a_{11} + \tau \delta_{12} = 0),$$

has the form

$$\begin{bmatrix} 0 & 0 & a'_{12} & 0 \\ 0 & 0 & 0 & \delta_{12} \\ \delta_{12} & 0 & 0 & 0 \\ 0 & a'_{12} & 0 & 0 \end{bmatrix}.$$  

It is transformed by $T_{2_{a_{12}}}$ into $P_{12}$ whose characteristic determinant is $(1 - \kappa^2)^2$, contrary to the hypothesis concerning the roots of $\Delta(\kappa) = 0$.

§14.

The further discussion of the resulting substitution

$$\begin{bmatrix} 0 & \gamma_{11} & 0 & 0 \\ \beta_{11} & \delta_{11} & \beta_{12} & \delta_{12} \\ 0 & \gamma_{21} & a_{22} & \gamma_{22} \\ 0 & \beta_{21} & \beta_{22} & \delta_{22} \end{bmatrix}$$

is separated into the cases $\beta_{12} = \delta_{12} = 0$, when the substitution has the form (12), and $\beta_{12}$, $\delta_{12}$ not both zero. In the latter case we may take $\beta_{12} = 0$, first transforming by $M_2$ if $\delta_{12} = 0$. Transforming by $T_{2\beta_{12}}$, we have a similar substitution with $\beta_{12} = 1$. Then the transform by $L_{2\delta_{12}}$ becomes

It has the characteristic determinant

\[
\kappa^4 - \kappa^3(\delta_{11} + a_{22} + \delta_{22}) + \kappa^2(2 + \delta_{11} a_{22} + \delta_{11} \delta_{22} - \gamma_{11} \gamma_{22}) - \kappa(\delta_{11} + a_{22} + \delta_{22}) + 1.
\]

It is the product of two factors \(\kappa^2 - \sigma \kappa + 1\) and \(\kappa^2 - \lambda \kappa + 1\) if, and only if,

\[
\sigma + \lambda = a_{22} + \delta_{22} + \delta_{11}, \quad \sigma \lambda = (a_{22} + \delta_{22}) \gamma_{11} - \gamma_{11} \gamma_{22}
\]

may be satisfied by marks \(\sigma, \lambda\) of the \(GF[p^n]\). For \(p > 2\), the necessary and sufficient condition is that \((a_{22} + \delta_{22} - \delta_{11})^2 + 4\gamma_{11} \gamma_{22}\) be zero or a square in the field, viz., \((\sigma - \lambda)^2\). In particular, if \(\gamma_{22} = 0\), we have

\[
\Delta(\kappa) \equiv (\kappa^2 - \delta_{11} \kappa + 1)[\kappa^2 - \kappa(a_{22} + \delta_{22}) + 1].
\]

§ 15.

We seek the conditions under which new indices

\[
X' = a' \xi_1 + b' \eta_1 + c' \xi_2 = d' \eta_2, \quad Y' = a' \xi_1 + b' \eta_1 + c' \xi_2 + d' \eta_2
\]

may be introduced so that \(S_1\) will replace \(X\) by \(Y\) and \(Y\) by \(-X + AY\), where \(A, a, b, c, d, a_1, \ldots\), are marks of the \(GF[p^n]\) satisfying the equation

\[
(23) \left| \begin{array}{cc} a & b \\ c_1 & d_1 \end{array} \right| = 1.
\]

In order that \(S_1\) shall replace \(X\) by \(Y\) and \(Y\) by \(-X + AY\), we must have

\[
\left\{ \begin{array}{l}
a_i = b \beta_{11}, \\
b_i = a \gamma_{11} + b \delta_{11} + c \gamma_{11} \gamma_{22} + d \gamma_{11} \delta_{22}, \\
c_i = b + c \gamma_{22} + d \beta_{22}, \\
d_i = c \gamma_{22} + d \delta_{22}, \\
a = -a_1 A + b_1 \beta_{11}, \\
b = a_1 \gamma_{11} + b_1 (\delta_{11} - A) + c_1 \gamma_{11} \gamma_{22} + d_1 \gamma_{11} \delta_{22}, \\
c = b_1 + c_1 (a_{22} - A) + d_1 \beta_{22}, \\
d = c_1 \gamma_{22} + d_1 (\delta_{22} - A).
\end{array} \right.
\]

On substitution of the values of \(a_i, b_i, c_i, d_i\) into the second set of equations, we have the following equations :

\[
(24) b \beta_{11} (\delta_{11} - A) - c \gamma_{22} - d \delta_{22} = 0,
\]

\[
(25) a (\delta_{11} - A) \gamma_{11} + b (\gamma_{11} \gamma_{22} + \delta_{11} - \delta_{11} A) + c \gamma_{11} \gamma_{22} (a_{22} + \delta_{22} + \delta_{11} - A)
+ d \gamma_{11} (\delta_{22}^2 + \beta_{22} \gamma_{22} + \delta_{11} \delta_{22} - A \delta_{22}) = 0,
\]

\[
(26) a \gamma_{11} + b (\delta_{11} + a_{22} - A) + c \{ \gamma_{11} \gamma_{22} + a_{22} (a_{22} + \delta_{22} - A) \}
+ d \{ \gamma_{11} \delta_{22} + \beta_{22} (a_{22} + \delta_{22} - A) \} = 0,
\]

\[
(27) b \gamma_{22} + c \gamma_{22} (a_{22} + \delta_{22} - A) + d \delta_{22} (a_{22} + \delta_{22} - A) = 0.
\]
Multiplying (24) by \( a_{22} + \delta_{22} - \lambda \) and adding to (27), we find

\begin{equation}
\gamma_{22} + \beta_{11}(\delta_{11} - \lambda)(a_{22} + \delta_{22} - \lambda) = 0 .
\end{equation}

Indeed, if \( \delta = 0 \), then \( a_1 = 0 , a = 0 \); then (24) and (26) require

\[ a_{22} + \delta_{22} - \lambda = 0 , \]

whence (24) and (25) require \( d = 0 , \gamma_{22}c = 0 \). Then \( d_1 = 0 \), so that (23) will not hold. If we calculate the determinant of the coefficients of (24), (25), (26), (27), we find \( \gamma_{22} \) times the square of the left member of (28). Hence the latter is the condition that these equations have solutions other than \( a = b = c = d = 0 \).

In order that \( \lambda \) determined by (28), viz.,

\[ \lambda^2 - \lambda(\delta_{11} + a_{22} + \delta_{22}) + \delta_{11}(a_{22} + \delta_{12}) - \gamma_{11} \gamma_{22} = 0 , \]

shall belong to the \( GF[p^n] \) it is necessary and sufficient that \( \Delta(\kappa) \) decomposes into quadratic factors \( \kappa^2 - \lambda \kappa + 1 , \kappa^2 - \lambda' \kappa + 1 \) [see § 14].

For the case of \( \gamma_{22} = 0 \), the decomposition is evident:

\[ \lambda = \delta_{11} , \lambda' = a_{22} + \delta_{22} . \]

If these roots be equal, we have

\[ a_{22}(a_{22} + \delta_{22} - \delta_{11}) = a_{22}^2 - \delta_{11} a_{22} + 1 = 0 , \]

since \( a_{22} \delta_{22} = 1 \), so that \( \kappa^2 - \delta_{11} \kappa + 1 \) would be reducible in the field. Hence if \( \Delta(\kappa) \) has equal irreducible quadratic factors, then \( \gamma_{22} \neq 0 \).

In case (28) is satisfied by a mark \( \lambda \), equation (27) may be dropped from consideration. Multiplying (24) by \( \gamma_{11} \) and adding to (26), we find

\[ \gamma_{11}a_{22} + ba_{22} + ca_{22}(a_{22} + \delta_{22} - \lambda) + d\beta_{22}(a_{22} + \delta_{22} - \lambda) = 0 . \]

Multiplying (24) by \( \gamma_{11} \delta_{11} \) and (27) by \( - \gamma_{11} \), and adding the resulting equations to (25), we find

\[ d = \alpha(\delta_{11} - \lambda) . \]

Using the relation \( 1 + \beta_{22} \gamma_{22} = a_{22} \delta_{22} \) and (28), we have from (26') and (24)

\[ a_{22}\{\gamma_{11} \delta_{22} + b + c(a_{22} + \delta_{22} - \lambda)\} = 0 , \]

\[ (\delta_{11} - \lambda)\{\gamma_{11} \delta_{22} + b + c(a_{22} + \delta_{22} - \lambda)\} = 0 . \]

If \( \delta_{11} - \lambda = 0 \), then \( \gamma_{22} = 0 \) and \( a_{22} \neq 0 \). Hence, in every case

\[ b = - \alpha \gamma_{11} \delta_{22} - c(a_{22} + \delta_{22} - \lambda) . \]

Hence, if (28) be satisfied, equations (24), (25), (26), (27) are equivalent to the two (25') and (29).
It remains to prove that the condition (23) may be satisfied. For \( \gamma_{22} = 0 \), we may take \( A = \delta_{11} \) so that \( d = 0, d_1 = 0 \). Then
\[
\begin{vmatrix}
  a & b \\
  a_1 & b_1
\end{vmatrix} = a\gamma_{11} + ab\delta_{11} - \delta^2\beta_{11} = 1.
\]
For \( p = 2 \), we may take \( b = 0, a = \gamma_{11}^2 \), every mark of the \( GF[2^n] \) being a square. For \( p > 2 \), the condition may be written
\[
\left(a - \frac{1}{2} b\beta_{11}\delta_{11}\right)^2 + b^2\beta_{11}^2(1 - \frac{1}{4} \delta_{11}^2) = -\beta_{11}.
\]
It has solutions \( a, b \) in the \( GF[p^n] \), unless \( \delta_{11} = \pm 2 \). In the latter case \( \kappa^2 - \delta_{11}\kappa + 1 = (\kappa \mp 1)^2 \), contrary to hypothesis. Then \( c \) is determined by (29) since \( a_{22} + \delta_{22} - \delta \neq 0 \).

For \( \gamma_{22} \neq 0 \), we may suppose \( \delta_{22} = 0 \). Indeed the transform of \( S_1 \) by \( L_{2, r} \), \( \delta_{22} + \tau \gamma_{22} = 0 \), is of the form \( S_1' \) with \( \delta_{22} = 0, \gamma_{22} = \mp 0 \). Then
\[
d = a(\delta_{11} - A), \quad b = -c(a_{22} - A), \quad a_1 = -c\beta_{11}(a_{22} - A),
\]
\[
b_1 = a\gamma_{11} - cA(a_{22} - A), \quad c_1 = a\beta_{22}(\delta_{11} - A) + cA, \quad d_1 = c\gamma_{22}.
\]
Hence the condition (23) becomes
\[
a^2\{\gamma_{11} - \beta_{22}(\delta_{11} - A)^2\} - acA(a_{22} + \delta_{11} - 2A) + c^2\{\gamma_{22} - \beta_{11}(a_{22} - A)^2\} = 1.
\]
Since \( \beta_{22}\gamma_{22} = -1, \gamma_{11}\gamma_{22} = (\delta_{11} - A)(a_{22} - A) \), the condition may be written
\[
(a_{22} + \delta_{11} - 2A)(a_{22} + \delta_{11} - 2A) + c^2(a_{22} - A)^2 = \gamma_{11}(a_{22} - A).
\]
Here \( a_{22} - A \neq 0 \). Hence the equation is impossible if \( 2A = a_{22} + \delta_{11} \), whence
\[
4\gamma_{11}\gamma_{22} + (a_{22} - \delta_{11})^2 = 0.
\]
In this case \( \Delta(\kappa) \) is the square of a quadratic factor (see §14).

This case being excluded here the above condition may be satisfied, when \( p > 2 \), unless \( 1 - \frac{1}{4} A^2 = 0 \) [cf. §1]. Then \( \gamma_{11}\gamma_{22} = (\delta_{11} \mp 2)(a_{22} \mp 2) \), so that
\[
4\gamma_{11}\gamma_{22} + (a_{22} - \delta_{11})^2 = (a_{22} + \delta_{11} \mp 4)^2,
\]
\[
\Delta(\kappa) \equiv [\kappa^2 - \kappa(a_{22} + \delta_{11} \mp 2) + 1][\kappa^2 - 2\kappa + 1],
\]
c contrary to the hypothesis concerning the roots of \( \Delta(\kappa) = 0 \). For \( p = 2 \), the condition is satisfied by the values
\[
a = \gamma_{11}^{-\frac{1}{2}}A(a_{22} - A)^{-\frac{1}{2}}(a_{22} + \delta_{11})^{-\frac{1}{2}}, \quad c = \gamma_{11}^{\frac{1}{2}}(a_{22} - A)^{-\frac{1}{2}}(a_{22} + \delta_{11})^{-\frac{1}{2}}.
\]
As a first conclusion of the preceding investigation it follows that if the characteristic determinant \( \Delta(\kappa) \) of a substitution \( S \) of \( SA(4, p^n) \) decomposes in the \( GF[p^n] \) into two distinct irreducible quadratic factors \( \kappa^2 - A\kappa + 1 \) and \( \kappa^2 - A'\kappa + 1 \), then \( S \) is conjugate within \( SA(4, p^n) \) with a substitution of the form (12) and therefore conjugate with
If \( \Delta(\kappa) \) be the square of an irreducible quadratic factor, then \( S \) is either conjugate with (21) for \( \beta_{12} = \delta_{12} = 0 \) and hence conjugate with (30), or else is conjugate with \( S_1 \) with \( \gamma_{22} \neq 0 \). In the latter case we transform by \( L'_2 \), and make \( \delta_{22} = 0 \), obtaining the substitution

\[
S_2 = \begin{pmatrix}
0 & \gamma_1 & 0 & 0 \\
-\gamma_1^{-1} & \delta & 1 & 0 \\
0 & \gamma_1 \gamma & a & \gamma \\
0 & 0 & -\gamma^{-1} & 0
\end{pmatrix}.
\]

The characteristic determinant of \( S_2 \) is

\[
\Delta(\kappa) \equiv \kappa^4 - \kappa^3(\delta + a) + \kappa^2(2 + \delta a - \gamma \gamma_1) - \kappa(\delta + a) + 1.
\]

In particular, \( \Delta(\kappa) \) is a perfect square * if, and only if,

\[
(a - \delta)^2.
\]

A second result of the investigation is that \( S \) is conjugate with a substitution of the form \( S_2 \) within \( SL(4, p^n) \) when \( \Delta(\kappa) \) is irreducible in the \( GF[p^n] \) or is the product of two factors \( \kappa^2 - \rho \kappa + \tau, \tau \neq 1 \), belonging to and irreducible in the \( GF[p^n] \). The latter cases are treated in § 17; the case in which (31) holds is considered in the next section.

\[\text{§16. Characteristic determinant the square of an irreducible quadratic.}\]

Consider the following substitution of the form \( S_2 \):

\[
\Sigma_2 = \begin{pmatrix}
0 & 1 & 0 & 0 \\
-1 & 0 & 1 & 0 \\
0 & c & a & c \\
0 & 0 & -c^{-1} & 0
\end{pmatrix}
\]

\[
(-4c = a^2).
\]

It has the characteristic determinant (whether \( p = 2 \) or \( p > 2 \))

\[
\kappa^4 - \kappa^3c + \kappa^2(2 - c) - \kappa a + 1 \equiv [\kappa^2 - (- c)^{1/2}\kappa + 1]^2.
\]

* If \( p > 2 \) and (31) is satisfied, \( \Delta(\kappa) = \frac{1}{4}(a + \delta)\kappa + 1 \).
A substitution \( S_2 \) satisfying (31) will have the same characteristic determinant as \( \Sigma_2 \) if, and only if, \( \alpha = \alpha + \delta \), and for \( p = 2 \), \( c = \alpha^2 - \gamma \gamma_1 \). The latter are consequently necessary conditions for the conjugacy of \( S_2 \) and \( \Sigma_2 \) under linear transformation. We proceed to prove that, if \( S_2 \) satisfy the condition (31) and if \( \kappa^2 - (-c)^{\frac{1}{2}} + 1 \) be irreducible in the \( GF[p^n] \), then \( \alpha = \alpha + \delta \), together with \( c = \alpha^2 - \gamma \gamma_1 \) if \( p = 2 \), are sufficient conditions for the conjugacy of \( S_2 \) and \( \Sigma_2 \) within \( SA(4, p^n) \). Assuming these conditions satisfied, we may determine a substitution \( S \) of \( SA(4, p^n) \) such that \( SS_2 = \Sigma_2 S \). We take for \( S \) the general substitution (1), the latter relation imposes a set of conditions which reduce to the following upon applying \( \alpha = \alpha + \delta \), \(-4c = \alpha^2 \) and (31):

\[
\begin{align*}
\gamma_{11} &= -\gamma_{1}\beta_{11}, \quad c\alpha_{12} = \gamma_{1}\delta_{12}, \quad \gamma_{22} = -\gamma c\beta_{22}, \quad \alpha_{21} = \gamma\delta_{21}, \\
ca_{12} &= -a_{11} + \gamma_{1}\delta_{11}, \quad c\gamma_{1}\beta_{12} = -a\alpha_{11} + \gamma\delta_{11} + c\gamma_{11} - \gamma_{12}, \\
a_{21} &= \gamma_{1}^{-1}a_{11} - c\delta_{11} - \delta\beta_{11}, \quad \gamma_{1}\gamma_{21} = a\gamma_{1}\delta_{11} + c\gamma_{11} - a\alpha_{11} - \gamma_{12}, \\
\gamma_{1}\gamma_{22} &= \delta a_{11} + \gamma_{12}, \quad \gamma_{1}\gamma_{21} = a\gamma_{1}\delta_{11} + c\gamma_{11} - a\gamma_{12}, \\
a_{22} &= \delta_{11} + a\beta_{12}, \quad \gamma_{1}\gamma_{22} = \delta a_{11} + \gamma_{12}.
\end{align*}
\]

It suffices to take \( a_{12} = 0 \). Setting \( \rho \equiv \gamma_{1}^{-1}\gamma_{12} \), we have \( S \) in the form

\[
\begin{pmatrix}
\gamma_{1}\delta_{11} & -\gamma_{1}\beta_{11} & 0 & \gamma_{1}\rho \\
\beta_{11} & \delta_{11} & -\beta_{11} - c^{-1}\rho & 0 \\
-\delta\beta_{11} & -\delta\delta_{11} - c\beta_{11} - \rho & \delta_{11} - a\beta_{11} - ac^{-1}\rho & -c\beta_{11} \\
\gamma_{1}^{-1}\delta\delta_{11} + \gamma_{1}^{-1}\rho & -\gamma_{1}^{-1}\delta\beta_{11} & \gamma_{1}^{-1}\beta_{11} & c\gamma_{1}^{-1}\delta_{11} - a\gamma_{1}^{-1}\rho
\end{pmatrix}.
\]

The abelian relations (2), (3), (4) here reduce to the two:

\[
\delta_{11}^2 + \beta_{11}^2 + \beta_{11}\rho + c^{-1}\rho^2 = \gamma_{1}^{-1},
\]

\[
-\delta\delta_{11}^2 - \delta\beta_{11}^2 - c\delta_{11}\beta_{11} - 2\delta_{11}\rho + a\beta_{11}\rho + ac^{-1}\rho^2 = 0.
\]

Multiplying the first by \( a \) and the second by \(-1\) and adding, we have

\[
(a + \delta) (\delta_{11}^2 + \beta_{11}^2) + c\delta_{11}\beta_{11} + 2\delta_{11}\rho = a\gamma_{1}^{-1}.
\]

If \( p > 2 \), we may eliminate \( \rho \) between (33) and (34) and find

\[
\delta_{11}^2 (-\beta_{11}(c + 4) + 8a^{-1}a\gamma_{1}^{-1} - 4\gamma_{1}^{-1}) = \{2\beta_{11}^2 - (-c)^{-\frac{1}{2}}a\gamma_{1}^{-1}\}^2.
\]

We prove that there exists a mark \( \beta_{11}^2 \) making the coefficient of \( \delta_{11}^2 \) a square and the right member not zero. Let

\[
\tau \equiv 8a^{-1}a\gamma_{1}^{-1} - 4\gamma_{1}^{-1}.
\]

For \( p > 2 \), \( \tau \neq 0 \); since \( 2a^{-1}a = 1 \) requires \( a = \delta \) and therefore \( \gamma \gamma_1 = 0 \). If \( \tau \) be square, we may take \( \beta_{11} = 0 \), when (35) determines \( \delta_{11} \neq 0 \) and (34) determines \( \rho \). Suppose finally that \( \tau \) is a not-square. Since \( \kappa^2 - (-c)^{\frac{1}{2}}+ 1 \)
is irreducible, \(-c - 4\) is a not-square. After we divide \((35)\) by \(\tau\), the question is the possibility of finding a mark \(\mu^2\) such that \(\mu^2 + 1\) is a not-square. There are \(\frac{1}{4}(p^n - 1)\) such squares \(\mu^2 \neq 0\), according as \(p^n = 4l \pm 1\).\(^*\) Hence for \(p^n > 5\), there are at least two marks \(\beta_{11}^2\) making the coefficient of \(\delta_{11}\) in \((35)\) a square, and hence at least one mark \(\beta_{11}^2\) making also the right member \(\neq 0\). Then \(\delta_{11}\) is determined different from zero, so that \((34)\) gives \(p\).

For \(p^n = 5\), the right member of \((35)\) vanishes only if

\[\beta_{11}^2 = \pm 1, \quad (\pm c)^{-\frac{1}{2}}a\gamma^{-1} = \pm 2.\]

Then \(\tau\) is a not-square only when \(\gamma^{-1}_1 = +1\) or \(-1\). Since \(\gamma_1\) is a square, it may be taken to be \(+1\) by an earlier transformation of \(S_2\) by \(T_1^\omega T_2^{\omega^{-1}}\), \(\omega\) being suitably chosen. With \(\gamma_1 = 1\), then \(a^{-1}a = \pm 1\). But \(a^{-1}a = 1\) makes \(\tau\) a square. Hence \(a^{-1}a = -1\), so that \(\delta = -2a\), \(a = -2\delta\). Since \(-c - 4\) is a not-square, and \(-c = \delta^2\), it follows that \(\delta^2 = 1\), \(a^2 = -1\). Since \(\beta_{11}^2\) was chosen to make the coefficient of \(\delta_{11}\) a square, and since \(\tau\) is now \(3\), it follows that \(\beta_{11}^2 = -1\), and \(\delta_{11} = 0\). Then \((34)\) is an identity and \((33)\) becomes \((2\rho - \beta_{11})^2 = 1\) and may be satisfied.

For \(p^n = 3\), \(c \equiv 0 \pmod{3}\), since \(-c - 4\) is to be a not-square, necessarily \(-1\). Hence the substitution \(\Sigma_2\) cannot be employed. Since \(a + \delta = 0\), \((31)\) gives \(\gamma\gamma_1 \equiv -a^2 \equiv -1 \pmod{3}\). Hence \(S_2\) takes the form

\[\begin{bmatrix} a, \gamma \end{bmatrix} \equiv \begin{bmatrix} 0 & -\gamma^{-1} & 0 & 0 \\ \gamma & -a & 1 & 0 \\ 0 & -1 & a & \gamma \\ 0 & 0 & -\gamma^{-1} & 0 \end{bmatrix}.\]

But \(P_{12}M_1M_2\) transforms \([a, \gamma]\) into \([-a, -\gamma]\). Hence \([a, \gamma]\) is conjugate either with \([1, -1]\) or with \([-1, -1]\). The latter is transformed into the former by the special abelian substitution

\[\begin{bmatrix} 1 & 0 & -1 & 0 \\ 0 & -1 & 1 & 1 \\ -1 & 0 & -1 & 0 \\ -1 & 1 & 0 & 1 \end{bmatrix}.\]

For \(p = 2\), we have \(a = 0\), \(a + \delta = 0\), \(c = a^2 - \gamma\gamma_1\), so that \((34)\) becomes \(c\delta_{11}\beta_{11} = a\gamma^{-1}\). The latter together with \((33)\) are to be satisfied by marks \(\beta_{11}\), \(\delta_{11}\), \(\rho\) of the \(GF[2^n]\). Letting \(\rho = c\beta_{11}\gamma^2\) in \((33)\), dividing by \(c\beta_{11}\) and extracting the square root, we find

\[r^2 + r \equiv c^{-\frac{1}{2}} + \gamma_{11}^{-\frac{1}{2}} + \delta_{11} \pmod{2}\]

\[= c^{-\frac{1}{2}} + g\delta_{11}(\gamma_{11}^{-\frac{1}{2}} + \delta_{11})\]

upon eliminating $\beta_{11}$ and denoting the constant $c^{\gamma}a^{-1}\gamma_i$ by $g$. It remains to prove that a mark $\delta_{11}$ may be founded for which this equation has a root $r$ belonging to the field. But, by § 7, $r^2 + r = \tau$ is irreducible if, and only if,

$$\tau + \tau^2 + \tau^4 + \cdots + \tau^{2n-1} = 1.$$ 

By hypothesis $\kappa^2 + c^{\gamma}\kappa + 1 = 0$ and therefore $\mu^2 + \mu + c^{-1} = 0$ is irreducible in the field, so that

$$c^{-1} + (c^{-1})^2 + (c^{-1})^4 + \cdots + (c^{-1})^{2n-1} = 1.$$ 

If, for every mark $\delta_{11}$, the equation in $r$ be irreducible, then

$$g\delta_{11}(\gamma_1^{\gamma} + \delta_{11}) + \{g\delta_{11}(\gamma_1^{\gamma} + \delta_{11})\}^2 + \cdots + \{g\delta_{11}(\gamma_1^{\gamma} + \delta_{11})\}^{2n-1} \equiv 0$$

must be an identity modulo 2 in the variable $\delta_{11}$. This will be the case if, and only if, $g = g^{\gamma}\gamma_{1}^{-1}$, whence $g = \gamma_{1}$. The latter requires $c = a^2$. But $c = a^2 - \gamma_{1}$. Hence $\gamma = 0$, which is impossible.

In addition to the determination of the canonical form (32) and for $p^n = 3$, [1, -1], we have derived the theorem:

If two substitutions $S_2$ have as (common) characteristic determinant the square of an irreducible quadratic, they are conjugate within the group $SA(4, p^n)$.

§17.

It remains to consider the cases in which $\Delta(\kappa)$ is irreducible in the $GF[p^n]$ or is the product of two irreducible quadratic factors of the form

$$\kappa^2 - \rho \kappa + \tau, \tau \neq 1.$$ 

In either case the roots of $\Delta(\kappa) = 0$ are $\sigma$, $\sigma^{-1}$, $\sigma^{p^n}$, $\sigma^{-p^n}$; in the former case $\sigma^{2n+1} = 1$, in the latter case $\sigma^{p^{2n}-1} = 1$. We may write $\Delta(\kappa) = 0$ in the form

$$\sigma^2 \gamma \gamma_1 = (\sigma^2 - \sigma \delta + 1)(\sigma^2 - \sigma \delta + 1).$$

The substitution $S_2$ given at the end of § 15, multiplies by $\sigma$ the function

$$X_1' = -\gamma \xi_1 + \sigma \gamma \gamma_1 \eta_1 + (\sigma^2 - \sigma \delta + 1)\xi_2 + \sigma^{-1}\gamma(\sigma^2 - \sigma \delta + 1)\eta_2.$$ 

Denote by $Y_1$, $Y_2$, $Y_2$ the linear functions derived from $X_1$ upon replacing $\sigma$ by $\sigma^{-1}$, $\sigma^{p^n}$, $\sigma^{-p^n}$ respectively. If $\Delta(\kappa)$ be irreducible, so that $\sigma$ belongs to the $GF[p^n]$, the functions $X_1$, $Y_1$, $X_2$, $Y_2$ are conjugate with respect to the $GF[p^n]$. In the second case, $\sigma$ belongs to the $GF[p^{2n}]$, so that $X_1$ and $X_2$, $Y_1$ and $Y_2$ are conjugate with respect to the $GF[p^n]$. Hence the four functions satisfy the requirements as to the conjugacy. In terms of these functions taken as new indices, the substitution $S_2$ takes the canonical form

$$X_1' = \sigma X_1, \quad Y_1' = \sigma^{-1} Y_1, \quad X_2' = \sigma^{p^n} X_2, \quad Y_2' = \sigma^{-p^n} Y_2.$$ 

*It may be verified by direct calculation that the determinant of the transformation of indices does not vanish; but the result follows from the abelian character of the transformation.
The transformation of indices satisfies those abelian conditions specified by formulæ (3) and (4). In fact,

\[
\begin{vmatrix}
-\gamma & \sigma\gamma_1 \\
-\gamma & \sigma\gamma_2
\end{vmatrix} + \begin{vmatrix}
\sigma^2 - \sigma\delta + 1 & \sigma^{-1}\gamma(\sigma^2 - \sigma\delta + 1) \\
\sigma^{-2}\gamma - \sigma^{-1}\delta & \sigma^{-1}\gamma(\sigma^{-2}\gamma - \sigma^{-1}\delta + 1)
\end{vmatrix} = \gamma(\sigma - \sigma^p)\{\gamma\gamma_1 + (\sigma^2 - \sigma\delta + 1)(\sigma^{-2}\gamma - \sigma^{-1}\delta + 1)\sigma^{-1}\}.
\]

On elimination of \(\gamma\gamma_1\) by (36), the quantity in brackets vanishes if

\[
\sigma^{p-1}(\sigma^2 - \sigma\delta + 1) + \sigma^{2\gamma} - \sigma\gamma = 0.
\]

The latter is derived by multiplying by \(\sigma\gamma\) the identity

\[
\sigma + \sigma^{-1} + \sigma\gamma + \sigma\gamma^{-1} = \sigma + \delta,
\]

which follows from the form of \(\Delta(\kappa) = 0\), with the roots \(\sigma, \sigma^{-1}, \ldots\). In a similar manner, we find that

\[
\begin{vmatrix}
-\gamma & \sigma\gamma_1 \\
-\gamma & \sigma^{-1}\gamma
\end{vmatrix} + \begin{vmatrix}
\sigma^2 - \sigma\delta + 1 & \sigma^{-1}\gamma(\sigma^2 - \sigma\delta + 1) \\
\sigma^{-2}\gamma - \sigma^{-1}\delta & \sigma^{-1}\gamma(\sigma^{-2}\gamma - \sigma^{-1}\delta + 1)
\end{vmatrix} = 0.
\]

Replacing \(\sigma\) by \(\sigma^{-1}\) in the two identities just established, we obtain two new identities. The four embrace the relations (3) and (4). Consider next the left member of the first abelian relation (2):

\[
\begin{vmatrix}
-\gamma & \sigma\gamma_1 \\
-\gamma & \sigma^{-1}\gamma
\end{vmatrix} + \begin{vmatrix}
\sigma^2 - \sigma\delta + 1 & \sigma^{-1}\gamma(\sigma^2 - \sigma\delta + 1) \\
\sigma^{-2} - \sigma^{-1}\delta + 1 & \sigma\gamma(\sigma^{-2} - \sigma^{-1}\delta + 1)
\end{vmatrix} = \gamma(\sigma - \sigma^{-1})\{\gamma\gamma_1 + \sigma^{-2}(\sigma^2 - \sigma\delta + 1)^2\}.
\]

Denoting, for the moment, the quantity in brackets by \(C\), we observe that \(C\sigma^2\) may be written

\[
2(\sigma^2 - \sigma\delta + 1)\left(\sigma^2 - \frac{\alpha + \delta}{2} - \sigma + 1\right)
\]

and hence does not vanish. If \(\sigma - \sigma^{-1} = 0\), then \(\sigma^2 - 1 = 0\), contrary to hypothesis. The left member of the second abelian relation (2) is seen in like manner to be

\[
\gamma(\sigma^{p\gamma} - \sigma^{-p\gamma})C\mu^n.
\]

If \(\sigma^{p\gamma} = \sigma\), it is only necessary that \(X_1\) and \(X_2\), \(Y_1\) and \(Y_2\) be conjugate with respect to the \(GF[\mu^n]\). When we take \(\mu X_1\) in place of \(X_1\) and \(\mu^{p\gamma}X_2\) in place of \(X_2\), the canonical form (37) is preserved, as well as the abelian relations (3) and (4) just established. In case \(\mu\) is the reciprocal of \(\gamma(\sigma - \sigma^{-1})C\), the resulting transformation of indices satisfies also the abelian relations (2) and is therefore an abelian substitution in the \(GF[\mu^{2\gamma}]\) on two pairs of conjugate indices. In this case it follows that two substitutions \(S_2\) having the same characteristic equation are conjugate within \(SA(4, \mu^n)\).
If $\Delta(c) = 0$ be irreducible, so that $c^{2n} = c^{-1}$, the replacement of $X_1$ by $\mu X_1$ requires the replacement of $Y_1$ by $\mu^{2n} Y_1$, $X_2$ by $\mu^{2n} X_2$, $Y_2$ by $\mu^{2n} Y_2$. The above expression $\gamma(c - c^{-1})C$ is then multiplied by $\mu^{2n+1}$, a mark of the $GF[p^{2n}]$; the product can not be made unity by choice of $\mu$, since $C$ belongs to the $GF[p^{2n}]$, while $c - c^{-1}$ does not. Hence $S_2$ is not reducible to the canonical form (37) by a special abelian substitution with conjugate indices. Nor is $S_2$ so reducible by a general abelian substitution; for the product

$$\mu^{2n+1} \gamma(c - c^{-1})C$$

differs from its $(p^n)$-th power; indeed, the product equals the negative of its $(p^{2n})$-th power. By a suitable choice of $\mu$, $\mu^{2n+1} \gamma C = 1$, so that the left members of (2) become $c - c^{-1}$ and $c^{2n} - c^{-2n}$. Hence if $T$ denote the transformation of indices reducing $S_2$ to the canonical form (37), then $T$ replaces $c$ by $c'$, where

$$\phi \equiv \left[ \xi_1 \eta_1 \right] + \left[ \xi_2 \eta_2 \right], \quad \phi' \equiv (c - c^{-1}) \left[ \xi_1 \eta_1 \right] + (c^{2n} - c^{-2n}) \left[ \xi_2 \eta_2 \right],$$

when $T$ operates cogrediently upon the indices $\xi_i$, $\eta_i$ and $\bar{\xi}_i$, $\bar{\eta}_i$. If $T'$ denote the transformation of indices which reduces a second substitution $S_2'$ to the canonical form (37), the product $A \equiv T' T^{-1}$ leaves $c$ absolutely invariant and transforms $S_2'$ into $S_2$. In view of the conjugacy of the indices $X_i$, $Y_i$ and the invariance of $c$ under $A$, the latter may be expressed as a special abelian substitution on $\xi_i$, $\eta_i$ with coefficients in the $GF[p^n]$. Hence, if two substitutions $S_2$ have the same characteristic determinant and if the latter be irreducible or the product of two irreducible quadratic factors $c^2 - \rho c + \tau$, $\tau \neq 1$, they are conjugate within the group $SA(4, p^n)$.

§18.

Let $S$ be an abelian substitution whose characteristic determinant is irreducible in the $GF[p^n]$, so that $S$ may be reduced to the canonical form (37), where $\sigma^{2n+1} = 1$. Of the solutions of the latter, only $\sigma = \pm 1$ satisfy also $\sigma^{2n-1} = 1$, so that there remain $p^{2n} - 1$ or $2^{2n}$ suitable values of $\sigma$. Replacing $\sigma$ by $\sigma^{-1}$, we obtain from (37) a substitution which is transformed into (37) by $M_1 M_2$; replacing $\sigma$ by $\sigma^{-p^n}$, we obtain the transform of (37) by $P_{12} M_1$. Replacing $\sigma$ by $\sigma^{p^n}$, we obtain the transform of (37) by $P_{12} M_2$. Any new replacement of $\sigma$ leads to a substitution not conjugate with (37). Hence there are $\frac{1}{4}(p^{2n} - 1)$ or $\frac{3}{4} 2^{2n}$ non-conjugate types (37). An abelian substitution $S_1$ commutative with an abelian substitution $S$ having the canonical form (37) has simultaneously the canonical form

$$X_1' = \rho X_1, \quad Y_1' = \rho^{-1} Y_1, \quad X_2' = \rho^{p^n} X_2, \quad Y_2' = \rho^{-p^n} Y_2 \quad (\rho^{2n+1} = 1),$$

so that there are $p^{2n} + 1$ such substitutions $S_1$. Hence $S$ is conjugate with $p^{4n}(p^{2n} - 1)^2$ substitutions within $SA(4, p^n)$.
§ 19.

An abelian substitution $S$ whose characteristic determinant is the product of two irreducible quadratic factors $\kappa^2 - \rho \kappa + \tau$, $\tau \neq 1$, is reducible to the canonical form (37), where $\sigma^{2n-1} = 1$, $\sigma^n \neq \sigma$, $\sigma^{n-1} \neq \sigma^{-1}$. The $(p^n - 1)^2$ or $2^{2n-2}$ suitable values of $\sigma$ give, in sets of four, conjugate substitutions. Hence there are $\frac{1}{4}(p^n - 1)^2$ or $\frac{1}{4}2^{2n}(2^n - 2)$ non-conjugate types. Each is commutative with $p^{2n} - 1$ substitutions and therefore conjugate with exactly $p^{2n}(p^n - 1)$ substitutions of $SA(4, p^n)$.

§ 20.

An abelian substitution $S$ whose characteristic determinant is the product of two distinct irreducible factors of the form $\kappa^2 - A\kappa + 1$ is conjugate within $SA(4, p^n)$ with a substitution (30) and therefore is reducible to the canonical form

\[
(38) \quad X'_1 = \lambda X_1, \quad Y'_1 = \lambda^{-1} Y_1, \quad X'_2 = \mu X_2, \quad Y'_2 = \mu^{-1} Y_2,
\]

where $\lambda^{p^n + 1} = 1$, $\mu^{p^n + 1} = 1$, $\lambda^{p^n - 1} \neq 1$, $\mu^{p^n - 1} \neq 1$, $\mu \neq \lambda$, $\mu \neq \lambda^{-1}$. Of the $p^n + 1$ solutions of $\lambda^{p^n + 1} = 1$, $\lambda = \pm 1$ are to be excluded; then of the $p^n + 1$ solutions of $\mu^{p^n + 1} = 1$, $\mu = \pm 1$ and $\mu = \lambda$, $\lambda^{-1}$ are to be excluded. Hence there are $(p^n - 1)(p^n - 3)$ or $2^n(2^n - 2)$ pairs of suitable values $\lambda, \mu$. But $\lambda$ and $\lambda^{-1}$ are interchanged upon transforming (38) by $M_1$; $\mu$ and $\mu^{-1}$ upon transforming by $M_2$; $\lambda$ and $\mu$, $\lambda^{-1}$ and $\mu^{-1}$ upon transforming by $P_1$. Hence eight of the pairs of values $\lambda, \mu$ lead to conjugate types, so that there are exactly $\frac{1}{8}(p^n - 1)(p^n - 3)$ or $\frac{1}{8}2^n(2^n - 2)$ non-conjugate types (38). Each is commutative with exactly $(p^n + 1)^2$ substitutions having the canonical form

\[
X'_1 = \tau l X_1, \quad Y'_1 = \tau^{-1} Y_1, \quad X'_2 = \tau m X_2, \quad Y'_2 = \tau^{-m} Y_2,
\]

$\tau$ being a primitive root of the equation $\tau^{p^n + 1} = 1$ and $l$ and $m$ being arbitrary integers. Each type represents a set of $p^{2n}(p^{2n} + 1)(p^n - 1)^2$ conjugate substitutions of $SA(4, p^n)$.

§ 21.

An abelian substitution $S$ whose characteristic determinant is the square of an irreducible quadratic is either conjugate within $SA(4, p^n)$ with a substitution (30) having $A' = A$ or else with a substitution $S_2$ satisfying (31). In the former case, $S$ has the canonical form

\[
(39) \quad X'_1 = \lambda X_1, \quad Y'_1 = \lambda^{-1} Y_1, \quad X'_2 = \lambda Y_2, \quad Y'_2 = \lambda^{-1} Y_2,
\]

where $\lambda^{p^n + 1} = 1$, $\lambda \neq \pm 1$. There are $\frac{1}{2}(p^n - 1)$ or $2^{n-1}$ types not conjugate within $SA(4, p^n)$. An abelian substitution $S_1$, commutative with $S$ has simultaneously the canonical form
\[ X'_1 = aX_1 + \beta X_2, \quad X'_2 = \gamma X_1 + \delta X_2, \]
\[ Y'_1 = a^{p^n} Y_1 + \beta^{p^n} X_2, \quad Y'_2 = \gamma^{p^n} Y_1 + \delta^{p^n} Y_2, \]
subject to the abelian conditions *
\[ a^{p^n+1} + \beta^{p^n+1} = 1, \quad \gamma^{p^n+1} + \delta^{p^n+1} = 1, \quad a\gamma^{p^n} + \beta\delta^{p^n} = 0. \]

But these are the conditions that \( \left( \begin{array}{cc} a & \beta \\ \gamma & \delta \end{array} \right) \) shall be a binary hyperorthogonal substitution, the number of which is \( (p^n + 1)p^n(p^{2n} - 1) \). Hence each canonical form (39) represents a set of \( p^{3n}(p^{2n} + 1)(p^n - 1) \) conjugate substitutions of \( SA(4, p^n) \).

§22.

A substitution \( S_2 \) satisfying (31) has the canonical form
\[ (40) \quad X'_1 = \sigma X_1, \quad Y'_1 = \sigma^{-1} Y_1 + \sigma^{-1} X_2, \quad X'_2 = \sigma^{-1} X_2, \quad Y'_2 = \sigma Y_2 + \sigma X_1, \]
\( \sigma \) being a root of \( \Delta(\kappa) = 0 \). As in §17, we employ new indices
\[ X_1 \equiv -\gamma \xi_1 + \sigma \gamma \eta_1 + (\sigma^2 - \sigma \delta + 1) \xi_2 + \sigma^{-1} \gamma (\sigma^2 - \sigma \delta + 1) \eta_2, \]
and \( X_2 \) obtained from \( X_1 \) by replacing \( \sigma \) by \( \sigma^{p^n} \equiv \sigma^{-1} \); but for \( Y_1 \) and \( Y_2 \) we now take the functions
\[ Y_1 \equiv \gamma \xi_1 + (\sigma^2 - 1) \xi_2 + \gamma (\delta - 2\sigma) \eta_2, \quad Y_2 \equiv \gamma \xi_1 + (\sigma^2 - 1) \xi_2 + \gamma (\delta - 2\sigma^{-1}) \eta_2. \]
The determinant of the transformation of indices is seen to be
\[ -\gamma^2 \gamma_1 (\sigma - \sigma^{-1})^4 \neq 0. \]
Upon replacing \( \sigma \) by \( \sigma^{-1} \) in (40), we obtain the transform of (40) by \( P_{12} \). Hence there are \( \frac{1}{2}(p^n - 1) \) or \( 2^{n-1} \) non-conjugate types (40). Each is commutative only with the substitutions
\[ X'_1 = aX_1, \quad Y'_1 = a^{p^n} Y_1 + d^{p^n} X_2, \quad X'_2 = a^{p^n} X_2, \quad Y'_2 = a Y_2 + d X_1, \]
where \( a^{p^{n+1}} = 1 \), \( a^{p^n} d = ad^{p^n} \), so that \( d = \alpha \kappa \), \( \kappa \) a mark of the \( GF[p^n] \), giving \( p^n(p^n + 1) \) commutative substitutions. Hence each type represents a set of \( p^{3n}(p^{4n} - 1)(p^n - 1) \) conjugate substitutions within \( SA(4, p^n) \).

§23. Summary of the preceding results.

The numerical results obtained in the preceding investigation are collected into the following table. The mark \( \mu \) denotes 1 or a particular not-square \( \nu \) when \( p > 2 \); while \( \mu = 1 \), if \( p = 2 \). Also, \( \theta \) denotes \( \frac{1}{2} \) or 1 according as \( p > 2 \) or \( p = 2 \). Finally, for \( p > 2 \), \( \epsilon = \pm 1 \) according as \( p^n = 4l \pm 1 \). By the “number of types” is meant the number of non-conjugate types of the speci-

* Indeed, \( S \) given by (30) with \( A' = A \) may be reduced to its canonical form by an abelian substitution (not necessarily special), so that the canonical form of \( S \) satisfies the conditions (2), (3), (4).
fied form within $SA(4, p^n)$. As a check upon the enumeration it was verified that the sum of the products of the number of conjugate substitutions of each type (fourth column) by the number of types (second or third column) gives the order $N \equiv p^{4n}(p^{4n} - 1)(p^{2n} - 1)$ of the group.

Table of the non-conjugate types of operators of the group $SA(4, p^n)$ of order $N$.

<table>
<thead>
<tr>
<th>Type</th>
<th>Number of types.</th>
<th>$p &gt; 2$</th>
<th>$p = 2$</th>
<th>Number of conjugate substitutions of each type.</th>
</tr>
</thead>
<tbody>
<tr>
<td>(6)</td>
<td>$\frac{1}{3}(p^n - 3)(p^n - 5)$</td>
<td>$(2^{n-1} - 1)(2^{n-2} - 1)$</td>
<td>$p^{4n}(p^{2n} + 1)(p^n + 1)^2$</td>
<td></td>
</tr>
<tr>
<td>(7)</td>
<td>$\frac{1}{3}(p^n - 3)$</td>
<td>$2^{n-1} - 1$</td>
<td>$p^{3n}(p^{2n} + 1)(p^{n} + 1)$</td>
<td></td>
</tr>
<tr>
<td>(8)</td>
<td>$\frac{1}{3}(p^n - 3)$</td>
<td>$2^{n-1} - 1$</td>
<td>$p^{3n}(p^{2n} - 1)(p^{n} + 1)$</td>
<td></td>
</tr>
<tr>
<td>(9), $\beta = 0$</td>
<td>$p^n - 3$</td>
<td>$2^{n-1} - 1$</td>
<td>$p^{2n}(p^{2n} + 1)(p^{n} + 1)$</td>
<td></td>
</tr>
<tr>
<td>(9), $\beta = \mu$</td>
<td>$2(p^n - 3)$</td>
<td>$2^{n-1} - 1$</td>
<td>$\theta p^{3n}(p^{4n} - 1)(p^{n} + 1)$</td>
<td></td>
</tr>
<tr>
<td>$T_{1,1}T_{2,1}$</td>
<td>2</td>
<td>1</td>
<td>$\theta p^{4n} - (p^n - 1)$</td>
<td></td>
</tr>
<tr>
<td>$L_{1,1}L_{2,1}T_{1,1}T_{2,1}$</td>
<td>4</td>
<td>1</td>
<td>$\frac{1}{2} p^n(p^{4n} - 1)(p^n + \epsilon)$</td>
<td></td>
</tr>
<tr>
<td>$L_{1,1}L_{2,1}T_{1,1}T_{2,1}$</td>
<td>2</td>
<td>1</td>
<td>$(2^{n-1} - 1)(2^{n-2} - 1)$</td>
<td></td>
</tr>
<tr>
<td>$L_{1,1}L_{2,1}T_{1,1}T_{2,1}$</td>
<td>2</td>
<td>1</td>
<td>$\frac{1}{2} p^n(p^{4n} - 1)(p^n - \epsilon)$</td>
<td></td>
</tr>
<tr>
<td>$R_\beta$, $R_0$</td>
<td>4</td>
<td>1</td>
<td>$2^{n-1}$</td>
<td></td>
</tr>
<tr>
<td>$A_{\mu}T_{1,1}T_{2,1}$</td>
<td>$\frac{1}{4}(p^n - 1)(p^n - 3)$</td>
<td>$2^{n-1}(2^{n-1} - 1)$</td>
<td>$p^{2n}(p^{2n} + 1)(p^n - \epsilon)$</td>
<td></td>
</tr>
<tr>
<td>(18)</td>
<td></td>
<td></td>
<td>$p^{3n}(p^{2n} + 1)(p^n - 1)$</td>
<td></td>
</tr>
<tr>
<td>(19), $b = 0$</td>
<td>$p^n - 1$</td>
<td>$2^{n-1}$</td>
<td>$\theta p^{3n}(p^{4n} - 1)(p^{n} - 1)$</td>
<td></td>
</tr>
<tr>
<td>(19), $b = \mu$</td>
<td>$2(p^n - 1)$</td>
<td>$2^{n-1}$</td>
<td>$p^{4n}(p^{2n} - 1)(p^{n} - 1)$</td>
<td></td>
</tr>
<tr>
<td>(37), $\sigma_{p^{2n+1}} = 1$</td>
<td>$\frac{1}{4}(p^{2n} - 1)$</td>
<td>$2^{n-2}$</td>
<td>$p^{2n}(p^{2n} + 1)(p^n - \epsilon)$</td>
<td></td>
</tr>
<tr>
<td>(37), $\sigma_{p^{2n-1}} = 1$</td>
<td>$\frac{1}{4}(p^n - 1)^2$</td>
<td>$2^{n-1}(2^{n-1} - 1)$</td>
<td>$p^{4n}(p^{2n} + 1)(p^{n} - 1)$</td>
<td></td>
</tr>
<tr>
<td>(38)</td>
<td>$\frac{1}{3}(p^n - 1)(p^n - 3)$</td>
<td>$2^{n-1}(2^{n-1} - 1)$</td>
<td>$p^{3n}(p^{2n} + 1)(p^n - 1)$</td>
<td></td>
</tr>
<tr>
<td>(39)</td>
<td>$\frac{1}{2}(p^n - 1)$</td>
<td>$2^{n-1}$</td>
<td>$p^{3n}(p^{4n} - 1)(p^n - 1)$</td>
<td></td>
</tr>
<tr>
<td>(40)</td>
<td>$\frac{1}{2}(p^n - 1)$</td>
<td>$2^{n-1}$</td>
<td>$p^{2n}(p^{2n} + 1)$</td>
<td></td>
</tr>
<tr>
<td>$T_{1,1}$</td>
<td>1</td>
<td></td>
<td>$\frac{1}{2} p^{2n}(p^{4n} - 1)$</td>
<td></td>
</tr>
<tr>
<td>$L_{1,1}T_{1,1}$</td>
<td>4</td>
<td></td>
<td>$\frac{1}{2} p^{2n}(p^{4n} - 1)(p^{2n} - 1)$</td>
<td></td>
</tr>
<tr>
<td>$L_{1,1}T_{1,1}L_{2,1}$</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
§ 24. The group $SA(4,2)$ and the symmetric group on six letters.

A second check upon the above results is furnished by a consideration of the case $p^n = 2$, when the group $SA(4,2)$ is holoedrically isomorphic with the symmetric group on six letters.* The isomorphism may be established by the correspondence of generators:

$$(12) \sim M_1, \quad (23) \sim L_{11}, \quad (34) \sim S, \quad (45) \sim L_{21}, \quad (56) \sim M_2,$$

where

$$S = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}, \quad S' = L_{11}L_{21}S L_{21}L_{11} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{bmatrix} \sim (25).$$

Since $M_1$ transforms $L_{i1}$ into $L'_{i1}$, $L'_{11} \sim (13)$, $L'_{21} \sim (46)$. Then †

$$R_1 = L_{21}M_2 S' M_2 L'_{21} \sim (2456), \quad R_0 = M_2 L'_{11} S' L_{21} \sim (13)(2456),$$


By § 12, there is a single type $L_{21}M_2$ given by (19') for $b = 0$ and a single type $L'_{21}L_{21}M_2$ given by (19') for $b = 1$. The single type (39) may be represented by $L_{11}M_1 L_{21}M_2$. The single types (40) and (37), $\sigma^{p^{n+1}} = 1$, may be represented respectively by

$$[40] = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = M_1[13]M_2,$$

$$[37] = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = L'_{21}M_1[13]M_2.$$

For $p^n = 2$ the above table gives the following types of abelian substitutions:

† The abelian substitution numbered (13) is now referred to as [13].
The third column gives every type of substitution on six letters and the number of conjugates to each type is given by the second column. In view of the independence of the two determinations of the types of substitutions of $SA(4, 2)$, the check is a complete one.


For $p = 2$, $n > 1$, the group $SA(4, p^n)$ is simple; for $p > 2$, it has the maximal invariant subgroup composed of the identity and $T = T_1 T_2$, the quotient-group $A(4, p^n)$ being simple.* In view of the importance of the latter group, we proceed to determine, by means of the earlier results, the distribution of its operators into complete sets of conjugate operators.

In the table (§ 23) of the non-conjugate types of substitutions within $SA(4, p^n)$, $p > 2$, the types are grouped into sets (each set being exhibited in a single line of the table, except the last two sets) such that types $S$ and $ST$ always belong to the same set. If $S$ be not conjugate with $ST$ within $SA(4, p^n)$, the number of conjugates with $S$ within $SA(4, p^n)$ equals the number of conjugates with $S$ within $A(4, p^n)$.† If, however, there exists a substitution $V$ in $SA(4, p^n)$ which transforms $S$ into $ST$, the number of conjugates with $S$ in $A(4, p^n)$ equals one-half the number of conjugates with $S$ in $SA(4, p^n)$; indeed, if $W$ transforms $S_i$ into $S$, then $W V W^{-1}$ will transform $S_i$ into $S_i T$.

A type $S$ of the group $SA(4, p^n), p > 2$, will be called special and denoted


† In the quotient-group, $S$ and $ST$ become the same operator. It is convenient to denote the latter by $S$, the context sufficing to avoid confusion.
$S$, if $S$ be conjugate with $ST$ within the group. For example, there is a single special type (7),

$$\xi_1 = i\xi_1', \quad \eta_1 = -i\eta_1', \quad \xi_2 = -i\xi_2', \quad \eta_2 = i\eta_2$$

$(i^2 = -1)$, occurring if and only if $-1$ be a square in the $GF[p^n]$, viz., if $p^n = 4l + 1$.

In general, a type can be special only when the negative of each root of the characteristic equation is also a root.

For special types (6), three cases are to be examined. First, if $-\kappa = \kappa^{-1}$, so that $-\kappa^{-1} = \kappa$, then must $-\lambda = \lambda^{-1}$; hence $\kappa^2 = -1$, $\lambda^2 = -1$, so that $\lambda = \kappa$ or $\kappa^{-1}$, contrary to the hypothesis for type (6). Second, if $-\kappa = \lambda$, we have the special type

(6),

$$\xi_1 = \kappa\xi_1', \quad \eta_1 = \kappa^{-1}\eta_1', \quad \xi_2 = -\kappa\xi_2', \quad \eta_2 = -\kappa^{-1}\eta_2,'$$

which may be transformed into (6), $T$ by $P_{12}$. By the hypotheses for a type (6), $\kappa \neq 0$, $\kappa^2 \neq 1$, $\kappa^2 \neq -1$, the latter having solutions in the $GF[p^n]$ if, and only if, $p^n = 4l + 1$. Hence there are $\frac{1}{4}(p^n - 5)$ non-conjugate special types (6), if $p^n = 4l + 1$ and $\frac{1}{4}(p^n - 3)$ such types if $p^n = 4l - 1$. Third, if $-\kappa = \lambda^{-1}$, the resulting special type is transformed into (6), by $M_2$.

There is no special type (18), since $\alpha^2 = -1$, $\lambda^2 = -1$ require that $\alpha$ and $\lambda$ belong to the same field, contrary to hypothesis.

To show that type (37), $\sigma^{p_{n+1}} = 1$, is never special, we consider three cases. If $-\sigma = \sigma^{-1}$, then $\sigma^2 = -1$, while $p_{n+1}$ is not divisible by 4. If $-\sigma = \sigma^{p^n}$, then $\sigma^{p_{n+1}} = -\sigma^{p_n} = \sigma \neq \sigma^{-1}$. Similarly, for $-\sigma = \sigma^{-p_n}$, $\sigma^{p_{n+1}} = -\sigma^{-p_n} = \sigma \neq \sigma^{-1}$.

To determine the special types (37), $\sigma^{p_{n-1}} = 1$, $\sigma^{p_{n-1}} \neq 1$, $\sigma^{p_{n+1}} \neq 1$, we examine the three cases. If $-\sigma = \sigma^{-1}$, either $\sigma^{p_{n+1}} = 1$ or $\sigma^{p_{n-1}} = 1$, contrary to hypothesis. If $-\sigma = \sigma^{p_n}$, each solution of $\sigma^{p_{n-1}} = -1$, such that $\sigma^2 \neq -1$ and therefore $\sigma^{p_{n+1}} \neq 1$, furnishes a special type; there are $p^n - 1$ or $p^n - 3$ such values of $\sigma$ according as $p^n = 4l \pm 1$. If $-\sigma = \sigma^{-p_n}$, each solution of $\sigma^{p_{n-1}} = -1$, such that $\sigma^2 \neq -1$ and therefore $\sigma^{p_{n+1}} \neq 1$, furnishes a special type; there are $p^n \neq 1$ such values of $\sigma$ according as $p^n = 4l \pm 1$. The two sets of values for $\sigma$ are wholly distinct since $\sigma^2 \neq 1$. Hence there are $2p^n - 2$ values $\sigma$, whatever be the form of $p^n$, $p > 2$. Hence there are $\frac{1}{2}(p^n - 1)$ special types (37) when $\sigma^{p_{n-1}} = 1$.

Type (38) is not special for $-\lambda = \lambda^{-1}$, $-\mu = \mu^{-1}$, since then $\mu = \lambda$ or $\lambda^{-1}$, but is special for $\mu = -\lambda$, viz.:

(38),

$$X_1 = \lambda X_1', \quad Y_1 = \lambda^{-1}Y_1', \quad X_2 = -\lambda X_2', \quad Y_2 = -\lambda^{-1}Y_2,'$$

since $P_{12}$ transforms it into (38), $T$. The number of solutions of $\lambda^{p^{n+1}} = 1$, $\lambda^2 \neq 1$, $\lambda^2 \neq -1$, is $p^n - 1$ or $p^n - 3$, according as $p^n = 4l \pm 1$.

Of the remaining types in the table of § 23, it may be determined by inspection what special types, if any, exist. Our results may be combined in the following table:

Trans. Am. Math. Soc. 10
TABLE OF THE NON-CONJUGATE TYPES*  
of operators of the simple group $A(4, p^n)$, $p > 2$,  
of order $\frac{1}{2} p^n(p^{4n} - 1)(p^{2n} - 1)$.

<table>
<thead>
<tr>
<th>Type.</th>
<th>Number of distinct types.</th>
<th>Number of operators conjugate with each type.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$p^n = 4l + 1$, $p^n = 4l - 1$</td>
<td></td>
</tr>
<tr>
<td>(6)$^*$</td>
<td>$\frac{1}{2} (p^n - 5)$, $\frac{1}{2} (p^n - 3)$</td>
<td>$\frac{1}{2} p^n(p^{2n} + 1)(p^n + 1)^2$</td>
</tr>
<tr>
<td>(6)</td>
<td>$\frac{1}{6}(p^n - 5)^2$, $\frac{1}{16}(p^n - 3)(p^n - 7)$</td>
<td>$p^n(p^{2n} + 1)(p^n + 1)^2$</td>
</tr>
<tr>
<td>(7)$^*$</td>
<td>$1$</td>
<td>$\frac{1}{2} p^{3n}(p^{2n} + 1)(p^n + 1)$</td>
</tr>
<tr>
<td>(7)</td>
<td>$\frac{1}{2}(p^n - 5)$, $\frac{1}{4}(p^n - 3)$</td>
<td>$p^{3n}(p^{2n} + 1)(p^n + 1)$</td>
</tr>
<tr>
<td>(8)$^*$</td>
<td>$1$</td>
<td>$\frac{1}{2} p^{3n}(p^{4n} - 1)(p^n + 1)$</td>
</tr>
<tr>
<td>(8)</td>
<td>$\frac{1}{2}(p^n - 5)$, $\frac{1}{4}(p^n - 3)$</td>
<td>$p^{3n}(p^{2n} + 1)(p^n + 1)$</td>
</tr>
<tr>
<td>(9), $\beta = 0$</td>
<td>$\frac{1}{2}(p^n - 3)$</td>
<td>$\frac{1}{2} p^{3n}(p^{4n} - 1)(p^n + 1)$</td>
</tr>
<tr>
<td>(9), $\beta = \mu$</td>
<td>$p^n - 3$</td>
<td>$1$</td>
</tr>
<tr>
<td>identity</td>
<td>$1$</td>
<td>$\frac{1}{2}(p^n - 1)$</td>
</tr>
<tr>
<td>$L_{1,\mu}$</td>
<td>$2$</td>
<td>$p^n - 1$</td>
</tr>
<tr>
<td>$L_{1,\mu}L_{2,1}$</td>
<td>$1$</td>
<td>$\frac{1}{2}(p^{2n} - 1)$</td>
</tr>
<tr>
<td>$L_{1,\nu}L_{2,1}$</td>
<td>$1$</td>
<td>$\frac{1}{2}(p^n - 1)$</td>
</tr>
<tr>
<td>$A_1$</td>
<td>$2$</td>
<td>$p^n - 1$</td>
</tr>
<tr>
<td>(18)</td>
<td>$\frac{1}{8}(p^n - 1)(p^n - 3)$</td>
<td>$p^{3n}(p^{4n} - 1)(p^n + 1)$</td>
</tr>
<tr>
<td>(19), $b = 0$</td>
<td>$\frac{1}{2}(p^n - 1)$</td>
<td>$\frac{1}{2} p^{3n}(p^{4n} - 1)(p^n + 1)$</td>
</tr>
<tr>
<td>(19), $b = \mu$</td>
<td>$p^n - 1$</td>
<td>$\frac{1}{2} p^{3n}(p^{4n} - 1)(p^n + 1)$</td>
</tr>
<tr>
<td>(37), $\sigma^{2n+1}$</td>
<td>$1$</td>
<td>$\frac{1}{2} p^{4n}(p^{4n} - 1)$</td>
</tr>
<tr>
<td>(37)$^*$, $\sigma^{2n-1}$</td>
<td>$1$</td>
<td>$p^{4n}(p^{4n} - 1)$</td>
</tr>
<tr>
<td>(37)$^*$, $\sigma^{2n-1}$</td>
<td>$\frac{1}{8}(p^n - 1)(p^n - 3)$</td>
<td>$\frac{1}{2} p^{4n}(p^{4n} - 1)$</td>
</tr>
<tr>
<td>(38)$^*$</td>
<td>$\frac{1}{2}(p^{2n} - 1)$</td>
<td>$\frac{1}{2} p^{4n}(p^{2n} + 1)(p^n - 1)^2$</td>
</tr>
<tr>
<td>(38)</td>
<td>$\frac{1}{16}(p^{2n} - 1)(p^n - 5)$, $\frac{1}{16}(p^n - 3)^2$</td>
<td>$p^n(p^{2n} + 1)(p^n - 1)^2$</td>
</tr>
<tr>
<td>(39)$^*$</td>
<td>$0$</td>
<td>$\frac{1}{2} p^{3n}(p^{2n} + 1)(p^n - 1)$</td>
</tr>
<tr>
<td>(39)</td>
<td>$\frac{1}{2}(p^{2n} - 1)$, $\frac{1}{4}(p^n - 3)$</td>
<td>$p^{3n}(p^{2n} + 1)(p^n - 1)$</td>
</tr>
<tr>
<td>(40)$^*$</td>
<td>$0$</td>
<td>$\frac{1}{2} p^{3n}(p^{4n} - 1)(p^n - 1)$</td>
</tr>
<tr>
<td>(40)</td>
<td>$\frac{1}{4}(p^{2n} - 1)$, $\frac{1}{4}(p^n - 3)$</td>
<td>$p^{3n}(p^{4n} - 1)(p^n - 1)$</td>
</tr>
<tr>
<td>$T_{1,-1}$</td>
<td>$1$</td>
<td>$\frac{1}{2} p^{2n}(p^{2n} + 1)$</td>
</tr>
<tr>
<td>$L_{1,\mu}T_{1,-1}$</td>
<td>$2$</td>
<td>$\frac{1}{2} p^{2n}(p^{2n} + 1)$</td>
</tr>
<tr>
<td>$L_{1,\mu}L_{2,\mu}T_{1,-1}$</td>
<td>$1$</td>
<td>$\frac{1}{2} p^{2n}(p^{4n} - 1)$</td>
</tr>
<tr>
<td>$L_{1,\mu}L_{2,\mu}T_{1,-1}$</td>
<td>$2$</td>
<td>$\frac{1}{2} p^{2n}(p^{4n} - 1)$</td>
</tr>
</tbody>
</table>

* A type marked $s$ is special, otherwise a type is not special except for $T_{1,-1}$ and $L_{1,\mu}L_{2,\mu}T_{1,-1}$. 
In the table \( p \) denotes 1 or a particular not-square \( \nu \); \( \epsilon \) denotes \( \pm 1 \) according as \( p^\nu = 4l \pm 1 \). The total number of non-conjugate types in the simple group \( A(4, p^\nu) \), \( p > 2 \), is the same function of \( p^\nu \) in the two cases \( p^\nu = 4l \pm 1 \), viz.:
\[
\frac{1}{2} (p^{2n} + 1) + 3p^n + 6.
\]

§26. The operators of the simple group \( A(4, 3) \) of order 25920.

As proved by Jordan, \( SA(4, 3) \) is the group of the equation for the trisection of the periods of a hyperelliptic function of four periods. Moreover, the group of the equation for the determination of the 27 lines on a general cubic surface of the third order is of the same order 51840 as \( SA(4, 3) \). After a certain square root has been adjoined to the realm of rationality, the group reduces to the quotient-group \( A(4, 3) \) of order 25920. Hence the above two problems are essentially the same. In view of the importance of the group \( A(4, 3) \), it is desirable to know the distribution of its operators into complete sets of conjugates and likewise for its cyclic subgroups. By §25, there are exactly twenty types of non-conjugate operators in the group. It is desirable to have simple representatives in the group for each type. Type (39) may be represented by \( M_1M_2 \); type (19), \( b = 0 \), by \( M_2 \); type (19), \( b = 1 \), by \( M_2L_{11} \); type (19), \( b = -1 \), by \( M_2L_{-1} \); type (37), \( \sigma^4 = -1 \), by \( P_{12}M_1 \); type (40) by \( P_{12}L_{-1}T_{-1} \); type (37), \( \sigma^8 = 1 \), by \( S_2 \) for \( \gamma_1 = 1 \), \( \gamma = a = \delta = -1 \), viz.,
\[
K = \begin{bmatrix}
0 & 1 & 0 & 0 \\
-1 & -1 & 1 & 0 \\
0 & -1 & -1 & -1 \\
0 & 0 & 1 & 0
\end{bmatrix},
\]
of characteristic determinant \( \kappa^4 - \kappa^3 + \kappa^2 - \kappa + 1 \). Of the preceding statements, the only ones requiring further proof are those concerning the representatives \( P_{12}M_1 \) and \( P_{12}L_{-1}T_{-1} \); but the former has the characteristic determinant \( (\kappa^2 + \kappa - 1)(\kappa^2 - \kappa - 1) \), each factor being irreducible modulo 3, and hence has the canonical form (37), \( \sigma^8 = 1 \); while the latter is reduced to the canonical form (40) by the abelian transformation
\[
X_1 = \eta_1 + \sigma\eta_2, \quad Y_1 = \xi_1 - \sigma\xi_2 - \sigma\eta_2, \quad X_2 = \eta_1 - \sigma\eta_2, \quad Y_2 = \xi_1 + \sigma\xi_2 + \sigma\eta_2,
\]
where \( \sigma^2 \equiv -1 \pmod{3} \). We have therefore, by §25, the complete list of types of operators of \( A(4, 3) \) together with their periods and the number of their conjugates within \( A(4, 3) \), as given on the following page.

§27. Cyclic subgroups of the simple group \( A(4, 3) \).

To determine the distinct types of cyclic subgroups of \( A(4, 3) \), it is necessary to find what powers of each type of substitution are conjugate with
that type. Thus, \( L_{11} \) is not conjugate with its square \( L_{1-1} \); \( L_{11}L_{21} \) is con-
jugate with its square. \( A_{-1} \) is transformed into \( A_{1}^{-1} \) by \( T_{2-1}L_{2-1}' \). Since \( A_{1}^{3} = L_{1-1}^{3} \) and \( A_{1}^{6} = L_{11}^{6} \) are not conjugate, \( A_{1} \) is not conjugate with either \( A_{1}^{2} \) or \( A_{1}^{3} \), so that the latter are conjugate with \( A_{1}^{-1} \). Hence their squares \( A_{1}^{4} \), \( A_{1} \) and \( A_{1}^{7} \) are conjugate. Hence \( A_{1} \) generates a cyclic group self-conjugate
only under a \( G_{27} \). Again, \( M_{2} \) is transformed into \( M_{2}^{3} \) by the abelian substitution
(modulo 3) \( \xi_{2}' = \xi_{2} + \eta_{2}, \eta_{2}' = \xi_{2} - \eta_{2} \). Hence \( M_{2}L_{11} \) is conjugate with its
seventh power \( M_{2}^{3}L_{11} \), so that the fifth and eleventh powers are conjugate. The
latter is \( M_{2}^{3}L_{1-1} \) and is consequently conjugate with \( M_{2}L_{1-1} \) and hence (by the
above table) not conjugate with \( M_{2}L_{11} \) itself. Hence \( M_{2}L_{11} \) is conjugate only
with one other generator of the same cyclic group. The fact that \( P_{12}L_{1-1}T_{1-1} \) is conjugate with its reciprocal within \( A(4, 3) \) may be simply verified by observing
that the canonical form (40) is transformed into its reciprocal by the abelian
substitution \( P_{12}T_{2-1} \) on the indices \( X_{i}, Y_{i} \). In a similar way, \( P_{12}M_{1} \) is shown
to be conjugate with its reciprocal. Finally, there being but a single type of
substitutions of period 5, \( K \) must be conjugate with \( K^{2}, K^{3}, K^{4} \). We have
therefore the following complete list of the distinct types of cyclic subgroups
of \( A(4, 3) \), together with the number of conjugates to each cyclic group.

<table>
<thead>
<tr>
<th>Type of generator</th>
<th>Conjugate cyclic groups.</th>
<th>Generator</th>
<th>Groups.</th>
</tr>
</thead>
<tbody>
<tr>
<td>( L_{11} )</td>
<td>40</td>
<td>( A_{1} )</td>
<td>960</td>
</tr>
<tr>
<td>( L_{11}L_{21} )</td>
<td>120</td>
<td>( M_{2} )</td>
<td>270</td>
</tr>
<tr>
<td>( L_{1-1}L_{21} )</td>
<td>240</td>
<td>( M_{2}L_{11} )</td>
<td>1080</td>
</tr>
<tr>
<td>( T_{1-1} )</td>
<td>45</td>
<td>( K )</td>
<td>1296</td>
</tr>
<tr>
<td>( L_{11}T_{1-1} )</td>
<td>360</td>
<td>( P_{12}M_{1} )</td>
<td>1620</td>
</tr>
<tr>
<td>( L_{11}L_{2-1}T_{1-1} )</td>
<td>720</td>
<td>( M_{2} )</td>
<td>270</td>
</tr>
<tr>
<td>( L_{11}L_{21}T_{1-1} )</td>
<td>720</td>
<td>( P_{12}L_{1-1}T_{1-1} )</td>
<td>1080</td>
</tr>
</tbody>
</table>

**The University of Chicago, January 3, 1901.**