CANONICAL FORMS OF QUATERNARY ABELIAN SUBSTITUTIONS IN AN ARBITRARY GALOIS FIELD*

BY

LEONARD EUGENE DICKSON

§ 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.

‡ DICKSON, American Journal of Mathematics, vol. 22, p. 231, 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

$$a\xi^2 + \beta\eta^2 = 1$$

has in the $GF[p^n]$ $(p > 2)$, $p^n - \nu$ solutions (ξ, η), where ν 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

$$(1) \qquad S: \quad \begin{array}{r|cccc} & \xi_1 & \eta_1 & \xi_2 & \eta_2 \\ \hline \xi_1' = & \alpha_{11} & \gamma_{11} & \alpha_{12} & \gamma_{12} \\ \eta_1' = & \beta_{11} & \delta_{11} & \beta_{12} & \delta_{12} \\ \xi_2' = & \alpha_{21} & \gamma_{21} & \alpha_{22} & \gamma_{22} \\ \eta_2' = & \beta_{21} & \delta_{21} & \beta_{22} & \delta_{22} \end{array}$$

with coefficients in the $GF[p^n]$ which satisfy the relations ‡

$$(2) \qquad \begin{vmatrix} \alpha_{11} & \gamma_{11} \\ \beta_{11} & \delta_{11} \end{vmatrix} + \begin{vmatrix} \alpha_{12} & \gamma_{12} \\ \beta_{12} & \delta_{12} \end{vmatrix} = 1, \quad \begin{vmatrix} \alpha_{21} & \gamma_{21} \\ \beta_{21} & \delta_{21} \end{vmatrix} + \begin{vmatrix} \alpha_{22} & \gamma_{22} \\ \beta_{22} & \delta_{22} \end{vmatrix} = 1,$$

$$(3) \qquad \begin{vmatrix} \alpha_{11} & \gamma_{11} \\ \alpha_{21} & \gamma_{21} \end{vmatrix} + \begin{vmatrix} \alpha_{12} & \gamma_{12} \\ \alpha_{22} & \gamma_{22} \end{vmatrix} = 0, \quad \begin{vmatrix} \beta_{11} & \delta_{11} \\ \beta_{21} & \delta_{21} \end{vmatrix} + \begin{vmatrix} \beta_{12} & \delta_{12} \\ \beta_{22} & \delta_{22} \end{vmatrix} = 0,$$

$$(4) \qquad \begin{vmatrix} \alpha_{11} & \gamma_{11} \\ \beta_{21} & \delta_{21} \end{vmatrix} + \begin{vmatrix} \alpha_{12} & \gamma_{12} \\ \beta_{22} & \delta_{22} \end{vmatrix} = 0, \quad \begin{vmatrix} \beta_{11} & \delta_{11} \\ \alpha_{21} & \gamma_{21} \end{vmatrix} + \begin{vmatrix} \beta_{12} & \delta_{12} \\ \alpha_{22} & \gamma_{22} \end{vmatrix} = 0,$$

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.

† Compare American Journal of Mathematics, vol. 21, p. 195, 1899.

‡ 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: †

$$
\begin{aligned}
M_i &: \quad \xi_i' = \eta_i, \quad \eta_i' = -\xi_i;\\
L_{i\lambda} &: \quad \xi_i' = \xi_i + \lambda\eta_i;\\
L_{i\lambda}' &: \quad \eta_i' = \eta_i + \lambda\xi_i;\\
T_{i\lambda} &: \quad \xi_i' = \lambda\xi_i, \quad \eta_i' = \lambda^{-1}\eta_i;\\
P_{12} &: \quad \xi_1' = \xi_2, \quad \eta_1' = \eta_2, \quad \xi_2' = \xi_1, \quad \eta_2' = \eta_1;\\
N_{ij\lambda} &: \quad \xi_i' = \xi_i + \lambda\eta_j, \quad \xi_j' = \xi_j + \lambda\eta_i.
\end{aligned}
$$

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 $N_{ij\lambda}$, its determinant is unity.

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

$$
(5) \qquad S^{-1}: \quad \begin{vmatrix} \delta_{11} & -\gamma_{11} & \delta_{21} & -\gamma_{21} \\ -\beta_{11} & \alpha_{11} & -\beta_{21} & \alpha_{21} \\ \delta_{12} & -\gamma_{12} & \delta_{22} & -\gamma_{22} \\ -\beta_{12} & \alpha_{12} & -\beta_{22} & \alpha_{22} \end{vmatrix}.
$$

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

§ 3. *Characteristic equation of an abelian substitution.*

By definition, the characteristic determinant of S is

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

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

$$
\begin{vmatrix} \delta_{11} & \beta_{12} & \delta_{12} \\ \gamma_{21} & \alpha_{22} & \gamma_{22} \\ \delta_{21} & \beta_{22} & \delta_{22} \end{vmatrix} + \begin{vmatrix} \alpha_{11} & \alpha_{12} & \gamma_{12} \\ \alpha_{21} & \alpha_{22} & \gamma_{22} \\ \beta_{21} & \beta_{22} & \delta_{22} \end{vmatrix} + \begin{vmatrix} \alpha_{11} & \gamma_{11} & \gamma_{12} \\ \beta_{11} & \delta_{11} & \delta_{12} \\ \beta_{21} & \delta_{21} & \delta_{22} \end{vmatrix} + \begin{vmatrix} \alpha_{11} & \gamma_{11} & \alpha_{12} \\ \beta_{11} & \delta_{11} & \beta_{12} \\ \alpha_{21} & \gamma_{21} & \alpha_{22} \end{vmatrix}
$$

$$
= \delta_{11} + \alpha_{11} + \delta_{22} + \alpha_{22}:
$$

† If an index is not altered, it is not written in the formula.

The coefficient of κ^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 ± 1.*

Suppose first that all the roots of $\Delta(\kappa) = 0$ belong to the $GF[p^n]$. Designate them by κ, κ^{-1}, λ, λ^{-1} and consider first the case in which no root is ± 1. The root κ leads to a linear function $\omega \equiv a\xi_1 + b\eta_1 + c\xi_2 + d\eta_2$ which S multiplies by κ. But $SA(4, p^n)$ contains a substitution V which replaces ξ_1 by ω. Then $V^{-1}SV \equiv S_1$ replaces ξ_1 by $\kappa\xi_1$. Likewise the root κ^{-1}, which is also a root of the characteristic equation for S_1, leads to a linear function

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

which S_1 multiplies by κ^{-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

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

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

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

has as its roots the distinct marks λ, λ^{-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 $2m > 4$.

$$(6) \qquad \xi' = \kappa\xi_1, \quad \eta_1' = \kappa^{-1}\eta_1, \quad \xi_2' = \lambda\xi_2, \quad \eta_2' = \lambda^{-1}\eta_2.$$

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

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

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

$$\xi_1' = a\xi_1, \quad \eta_1' = a^{-1}\eta_1, \quad \xi_2' = b\xi_2, \quad \eta_2' = b^{-1}\eta_2.$$

Their number being $(p^n - 1)^2$, it follows that each substitution (6) is one of $N \div (p^n - 1)^2 \equiv p^{4n}(p^{2n} + 1)(p^n + 1)^2$ conjugates within $SA(4, p^n)$.

If, however, $b_1 = 0$ in ω_1, we may suppose that $c_1 \neq 0$. For, if $c_1 = 0$, $d_1 \neq 0$, then $M_2^{-1}S_1M_2$ multiplies $a_1\xi_1 + d_1\xi_2$ by κ^{-1}. With $c_1 \neq 0$, the group contains the abelian substitution

$$V = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -a_1c_1^{-1} \\ a_1 & 0 & c_1 & d_1 \\ 0 & 0 & 0 & c_1^{-1} \end{bmatrix}.$$

Hence $V^{-1}S_1V$ belongs to the group and has the form

$$\begin{bmatrix} \kappa & 0 & 0 & 0 \\ \beta_{11} & \kappa^{-1} & \beta_{12} & 0 \\ 0 & 0 & \kappa^{-1} & 0 \\ \beta_{21} & 0 & \beta_{22} & \kappa \end{bmatrix} \qquad (\beta_{21} = \kappa^2\beta_{12}).$$

Transforming by $L_{1\tau}'L_{2\sigma}'$ 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

$$(7) \qquad \xi_1' = \kappa\xi_1, \quad \eta_1' = \kappa^{-1}\eta_1, \quad \xi_2' = \kappa^{-1}\xi_2, \quad \eta_2' = \kappa\eta_2.$$

If $\beta_{12} \neq 0$, we transform by $T_{2\beta_{12}\kappa}$ and obtain the type

$$(8) \qquad \begin{bmatrix} \kappa & 0 & 0 & 0 \\ 0 & \kappa^{-1} & \kappa^{-1} & 0 \\ 0 & 0 & \kappa^{-1} & 0 \\ \kappa & 0 & 0 & \kappa \end{bmatrix}.$$

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

$$\begin{bmatrix} a & 0 & 0 & \beta \\ 0 & a & b & 0 \\ 0 & c & d & 0 \\ \gamma & 0 & 0 & \delta \end{bmatrix}.$$

The abelian relations give

$$aa - \beta b = 1, \quad ac - \beta d = 0, \quad -\gamma a + \delta b = 0, \quad -\gamma c + \delta d = 1.$$

Letting $\Delta \equiv ad - bc$, 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 κ^{-1} in place of κ. 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

$$\begin{bmatrix} a & 0 & 0 & 0 \\ 0 & c & d & 0 \\ 0 & 0 & c & 0 \\ b & 0 & 0 & a \end{bmatrix}.$$

The abelian relations give $ac = 1$, $-bc + ad = 0$, whence

$$c = a^{-1}, \quad d = bc^2.$$

The number of such substitutions is therefore $p^n(p^n - 1)$. Hence each substitution (8) is one of $p^{3n}(p^{4n} - 1)(p^n + 1)$ conjugates.

§ 5. *Roots in the field, two of them being* ± 1.

Suppose next that the roots are κ, κ^{-1}, ± 1, ± 1, where κ is a mark $\neq 0$ or ± 1 of the $GF[p^n]$. The canonical form is

$$(9) \qquad \begin{pmatrix} \kappa & 0 & 0 & 0 \\ 0 & \kappa^{-1} & 0 & 0 \\ 0 & 0 & \pm 1 & 0 \\ 0 & 0 & \beta & \pm 1 \end{pmatrix}.$$

For $\beta = 0$ there are $p^n - 3$ or $\frac{1}{2}(2^n - 2)$ types each commutative with

$$(10) \qquad \begin{pmatrix} t & 0 & 0 & 0 \\ 0 & t^{-1} & 0 & 0 \\ 0 & 0 & a & b \\ 0 & 0 & c & d \end{pmatrix} \qquad (ad - bc = 1),$$

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 β a square are transformed into each other by abelian substitutions $T_{2\sigma}$ and likewise those with β 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 $\frac{1}{2}p^{3n}(p^{4n} - 1)(p^n + 1)$ or $2^{3n}(2^{4n} - 1)(2^n + 1)$ substitutions within $SA(4, p^n)$.

§ 6. *Two roots each* ± 1 *and two roots each* ∓ 1.

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

$$(11) \qquad \begin{pmatrix} \pm 1 & 0 & 0 & 0 \\ a & \pm 1 & 0 & 0 \\ 0 & 0 & \mp 1 & 0 \\ 0 & 0 & \beta & \mp 1 \end{pmatrix}.$$

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

$$(12) \qquad \begin{pmatrix} a & b & 0 & 0 \\ c & d & 0 & 0 \\ 0 & 0 & a_1 & b_1 \\ 0 & 0 & c_1 & d_1 \end{pmatrix} \qquad (ad - bc = 1,\ a_1 d_1 - b_1 c_1 = 1).$$

For $a \neq 0$, we may suppose that $a = 1$ or ν, where ν is a particular not-square in the $GF[p^n]$; indeed, a is replaced by $a\sigma^{-2}$ upon transforming (11) by $T_{1\sigma}$. Similarly, we may assume that $\beta = 0$, 1 or ν. The resulting eight types are:

$$L_{1\mu}T_{1-1}, \quad L_{2\mu}T_{1-1}, \quad L_{11}T_{1-1}, \quad L_{2\mu}, \quad L_{1\nu}T_{1-1}L_{2\mu}$$

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

§ 7. *Four equal roots each* ± 1.

If the roots be ± 1, ± 1, ± 1, ± 1, the canonical form is either

$$L \equiv \begin{bmatrix} \pm 1 & 0 & 0 & 0 \\ a & \pm 1 & 0 & 0 \\ 0 & 0 & \pm 1 & 0 \\ 0 & 0 & \beta & \pm 1 \end{bmatrix} \quad \text{or} \quad R \equiv \begin{bmatrix} \pm 1 & 0 & 0 & 0 \\ \beta_{11} & \pm 1 & \beta_{12} & \delta_{12} \\ a_{21} & 0 & \pm 1 & 0 \\ \beta_{21} & 0 & a_{22} & \pm 1 \end{bmatrix}$$

according as the linear function ω_1 determined by the second root ± 1 contains η_1 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 $a_{21} = 0$, $\beta_{21} = 1$. 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 $\beta_{11} = 0$, $a_{22} \neq 0$, since the transform of R by P_{12} then has $\beta_{11} \neq 0$. Finally, if $\beta_{11} = a_{22} = 0$, we have the substitution

$$\begin{bmatrix} \pm 1 & 0 & 0 & 0 \\ 0 & \pm 1 & 1 & 0 \\ 0 & 0 & \pm 1 & 0 \\ 1 & 0 & 0 & \pm 1 \end{bmatrix}. \tag{13}$$

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

$$\begin{bmatrix} \alpha_{11} & 0 & \alpha_{12} & 0 \\ \beta_{11} & \delta_{11} & \beta_{12} & \delta_{12} \\ \delta_{12} & 0 & \delta_{11} & 0 \\ \beta_{21} & \alpha_{12} & \beta_{22} & \alpha_{11} \end{bmatrix},$$

subject to the abelian conditions

$$\alpha_{11}\delta_{11} + \alpha_{12}\delta_{12} = 1, \quad \beta_{11}\alpha_{12} + \delta_{11}\beta_{21} + \alpha_{11}\beta_{12} + \delta_{12}\beta_{22} = 0.$$

By the former, α_{11} and α_{12} are not both zero, so that the latter determines one of the β_{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 §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 $T_{2\,\delta_{12}^{-1}}$ 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 $T_{1\kappa}T_{2\kappa}$ is of the form R_1 with $\kappa^{-2}a$ in place of a. Choosing $\kappa = a^{\frac{1}{2}}$, 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_β 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_b, where $b \equiv \beta + \tau + \tau^2$. In order

that the $GF[2^n]$ shall contain a mark τ for which $b = 0$, it is necessary and sufficient that

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

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

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

That the substitutions R_β 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

$$(14) \qquad \begin{bmatrix} 1 & 0 & 0 & 0 \\ \beta_{11} & 1 & \beta_{12} & \beta_{22} \\ \beta_{22} & 0 & 1 & 0 \\ \beta_{21} & 0 & \beta_{22} & 1 \end{bmatrix} \qquad \begin{pmatrix} \beta_{21} = \beta_{12} + \beta_{22} + \beta \\ \beta_{21} = \beta_{12} + \beta_{22}^2 \end{pmatrix}.$$

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_β 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 β_{11} and β_{12} are arbitrary; thus there are $2 \cdot 2^{2n}$ substitutions.

For $p > 2$, R_1 is transformed into a similar substitution R' having $\beta_{11} = 0$ by the following abelian substitution

$$\eta_1' = \eta_1 + \tfrac{1}{2}\beta_{11}\xi_2, \quad \eta_2' = \eta_2 + \tfrac{1}{2}\beta_{11}\xi_1.$$

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

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

$$A_a = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ -1 & 0 & 1 & 0 \\ -a & 0 & a & 1 \end{bmatrix}, \qquad A_{-a} T_{1\,-1} T_{2\,-1}.$$

Transforming A_a by $T_{1\,\kappa} T_{2\,\kappa}$ we obtain $A_{a\kappa^{-2}}$. Hence, if $p > 2$, there are only four canonical types, ν being a particular not-square:

$$A_1,\quad A_\nu,\quad A_1T_{1,-1}T_{2,-1},\quad A_\nu T_{1,-1}T_{2,-1}. \tag{15}$$

The substitutions A_μ 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_μ 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 $A_\alpha S = SA_{\alpha'}$ requires that

$$\gamma_{11}=\gamma_{12}=\gamma_{21}=\gamma_{22}=\alpha_{12}=\delta_{21}=0,\quad \alpha_{22}=\alpha_{11},\quad \delta_{22}=\delta_{11},\quad \beta_{22}=\alpha\delta_{12},$$
$$\beta_{21}=-\beta_{12}-\alpha\delta_{12},\quad \alpha\delta_{22}=\alpha'\alpha_{22},\quad -\alpha'\alpha_{11}+\alpha'\alpha_{21}=-\beta_{22}-\alpha\delta_{22}.$$

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

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

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

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

For each of the two values of α_{11}, the second relation determines δ_{12}. Hence there are $2p^{2n}$ substitutions commutative with A_α. Hence each of the substitutions (15) is conjugate with exactly $\frac{1}{2}p^{2n}(p^{4n}-1)(p^{2n}-1)$ 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 $T_{1\sigma}T_{2\kappa}$, we obtain a substitution of the form L with α, β replaced by $\alpha\sigma^{-2}$, $\beta\kappa^{-2}$. Hence the substitutions L are conjugate with one of the following:

* For example, by introducing the new indices

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

A_α takes the standard canonical form (not abelian):

$$X'=X,\quad Y'=Y+X,\quad Z'=Z+Y,\quad W'=W+Z.$$

$$L_{1\mu}L_{2\tau}, \quad L_{1\mu}L_{2\tau}T_{1-1}T_{2-1} \qquad (\mu, \tau = 0, 1, \nu).$$

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

$$\begin{bmatrix} \nu\delta & 0 & \nu\sigma & 0 \\ 0 & \delta & 0 & \sigma \\ -\nu\sigma & 0 & \nu\delta & 0 \\ 0 & -\sigma & 0 & \delta \end{bmatrix},$$

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:

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

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 $L_{1\nu}$, ν 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:

$$\beta_{11} = 0, \quad \delta_{11} = \nu\alpha_{11}, \quad \beta_{12} = \beta_{21} = \alpha_{21} = \delta_{12} = 0.$$

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

$$1 = \alpha_{11}\delta_{11} - \beta_{11}\gamma_{11} + \alpha_{12}\delta_{12} - \beta_{12}\gamma_{12} \equiv \nu\alpha_{11}^2.$$

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

$$SL_{1\mu}L_{2\tau} = L_{1\mu}L_{2\tau}S \qquad (\mu \neq 0)$$

are found at once to be the following:

$$\beta_{11} = 0, \quad \beta_{12} = 0, \quad \beta_{21} = 0, \quad \alpha_{11} = \delta_{11}, \quad \tau\beta_{22} = 0,$$
$$\mu\alpha_{21} = \tau\delta_{21}, \quad \mu\delta_{12} = \tau\alpha_{12}, \quad \tau\alpha_{22} = \tau\delta_{22}.$$

For $\tau = 0$, S has the form

$$(16) \qquad \begin{bmatrix} \alpha_{11} & \gamma_{11} & \alpha_{12} & \gamma_{12} \\ 0 & \alpha_{11} & 0 & 0 \\ 0 & \gamma_{21} & \alpha_{22} & \gamma_{22} \\ 0 & \delta_{21} & \beta_{22} & \delta_{22} \end{bmatrix}.$$

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 η_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 ξ_1.* According as $p > 2$ or $p = 2$, $L_{1\mu}$ is one of $\frac{1}{2}(p^{4n}-1)$ or $2^{4n}-1$ conjugate substitutions within $SA(4, p^n)$.

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

$$(17) \qquad \begin{bmatrix} a_{11} & \gamma_{11} & \mu\delta_{12} & \gamma_{12} \\ 0 & a_{11} & 0 & \delta_{12} \\ a_{21} & \gamma_{21} & a_{22} & \gamma_{22} \\ 0 & \mu a_{21} & 0 & a_{22} \end{bmatrix},$$

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 μ is a not-square ν in the $GF[p^n]$, $p > 2$. 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 $a_{11}^2 + \nu\delta_{12}^2 = 1$, ϵ being ± 1 according as $p^n = 4l \pm 1$, a_{21} and a_{22} are determined except in sign; while γ_{21} is determined in terms of γ_{11}, γ_{12}, γ_{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 $GF[p^n]$, $p > 2$, a_{22} and a_{21} are determined except in sign, and one of the γ_{ij} is determined in terms of the remaining three. Hence there are $2p^{3n}(p^n - \epsilon)$ substitutions of $SA(4, p^n)$, $p > 2$, commutative with $L_{11}L_{21}$. 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^{4n} substitutions commutative with $L_{11}L_{21}$.

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

If ν be a not-square in the $GF[p^n]$, $p > 2$, no two of the substitutions $L_{11}T_{1-1}$, $L_{1\nu}T_{1-1}$, $L_{11}T_{2-1}$, $L_{1\nu}T_{2-1}$ 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_{11} and $L_{1\nu}$ and are not conjugate by § 8. Finally, a relation $SL_{1\mu}T_{1-1} = L_{1\tau}T_{2-1}S$ is proved impossible by forming the respective products.

*Quarterly Journal of Mathematics, vol. 29, pp. 171–173, 1897.

Within $SA(4, p^n)$, $p > 2$, each of the four substitutions is one of a complete set of $\frac{1}{2}p^{2n}(p^{4n} - 1)$ 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

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

subject to the abelian relations

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

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

A substitution S' commutative with $L_{1\mu}T_{2-1}$ will be commutative with $L_{1\mu}T_{2-1} \cdot T_{1-1}T_{2-1} \equiv L_{1\mu}T_{1-1}$ 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 $L_{11}T_{1-1}$, $L_{11}T_{2-1}$, $L_{1\nu}T_{1-1}$ and $L_{1\nu}T_{2-1}$, where ν is a not-square in the field, are not conjugate and each gives rise to a complete set of $\frac{1}{2}p^{2n}(p^{4n} - 1)$ conjugate substitutions.

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

The substitutions $L_{11}T_{1-1}L_{21}$ and $L_{1\nu}T_{1-1}L_{21}$ are not conjugate within $SA(4, p^n)$, $p > 2$. Indeed, their $p+1$-th powers, $L_{11}L_{21}$ and $L_{1\nu}L_{21}$ are not conjugate by § 8. Likewise $L_{11}T_{1-1}L_{2\nu}$ and $L_{1\nu}T_{1-1}L_{2\nu}$ are not conjugate within $SA(4, p^n)$. Finally, $L_{1\mu}T_{1-1}L_{21}$ is not conjugate with $L_{1\kappa}T_{1-1}L_{2\nu}$; for, if S transform the former into the latter, it is seen that S must replace ξ_2 by $\nu\delta_{22}\xi_2 + \gamma_{22}\eta_2$ and η_2 by $\delta_{22}\xi_2$, where $\nu\delta_{22}^2 = 1$. Combining the four non-conjugate substitutions into the single type $E \equiv L_{1\mu}T_{1-1}L_{2\tau}$, 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 $\frac{1}{4}(p^{4n} - 1)(p^{2n} - 1)p^{2n}$ conjugate substitutions. In proof, let S be commutative with E. Then S must be commutative with $E^p = T_{1-1}$, so that S must be of the form (12). Also S must be commutative with $E^{p+1} = L_{1\mu}L_{2\tau}$ and hence have $\beta_{11} = 0$, $\beta_{22} = 0$, $\alpha_{11} = \delta_{11}$, $\alpha_{22} = \delta_{22}$ (§ 8). Hence S has the form

$$\begin{bmatrix} \alpha & \gamma & 0 & 0 \\ 0 & \alpha & 0 & 0 \\ 0 & 0 & \alpha_{22} & \gamma_{22} \\ 0 & 0 & 0 & \alpha_{22} \end{bmatrix} \qquad (\alpha^2 = \alpha_{22}^2 = 1).$$

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* $GF[p^n]$

$$\Sigma \equiv \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \qquad (\alpha\delta - \beta\gamma = 1)$$

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

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

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

If $\beta\gamma = 0$, then $D(\kappa) = (\kappa - \alpha)(\kappa - \delta)$, contrary to hypothesis. Transforming Σ by $\begin{pmatrix} 1 & 0 \\ \alpha/\gamma & 1 \end{pmatrix}$, we obtain $S \equiv \begin{pmatrix} 0 & \gamma \\ -\gamma^{-1} & \alpha + \delta \end{pmatrix}$. If γ be a square in the field, the transform of S by $T_{1\gamma^{\frac{1}{2}}}$ gives Σ_1. If γ be a not-square, so that $p > 2$, the transform of S by $\begin{pmatrix} 1 & \tau \\ 0 & 1 \end{pmatrix}$ is a substitution of the form Σ with $c \equiv \gamma + \tau(\alpha + \delta) + \tau^2\gamma^{-1}$ in place of the coefficient γ. Since

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

is irreducible in the field, c cannot vanish. Moreover, at most two values of τ 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 Σ_1.

By an analogous proof, Σ may be transformed into

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

§ 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 λ, λ^{p^n}. Then (§ 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 ± 1 of the former, so that λ 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 ξ_1 by $a\xi_1$ and η_1 by $a^{-1}\eta_1$. On account of the abelian conditions, S' is seen to affect ξ_2, η_2 according to a substitution of the form

$$\Sigma \equiv \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \qquad (\alpha\delta - \beta\gamma = 1).$$

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

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

In particular, the latter is irreducible in the $GF[p^n]$. By §11, there exists a substitution on ξ_2, η_2 with coefficients in the field and having determinant unity which transforms Σ into

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

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

$$(18') \qquad \begin{bmatrix} a & 0 & 0 & 0 \\ 0 & a^{-1} & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & A \end{bmatrix}.$$

If $a^{-1} = a$, S may be transformed by a substitution of the group into a substitution S_1 which replaces ξ_1 by $a\xi_1$ and η_1 by $a\eta_1 + b\xi_1$ and therefore ξ_2, η_2 by linear functions of ξ_2, η_2 only. If $b \neq 0$, we transform S_1 by T_{1c} and obtain a substitution of the form S_1 with $c^{-2}b$ in place of b, so that b may be restricted to unity and (for $p > 2$) a particular not-square ν of the field. *The canonical forms within $SA(4, p^n)$ of substitutions whose characteristic determinant is the product of two equal linear factors $\kappa \mp 1$ and an irreducible quadratic factor $\kappa^2 - A\kappa + 1$ are*

$$(19') \qquad \begin{bmatrix} \pm 1 & 0 & 0 & 0 \\ b & \pm 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & A \end{bmatrix} \qquad (b = 0, 1 \text{ or } \nu).$$

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

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

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

$$(18) \qquad \xi_1' = a\xi_1, \quad \eta_1' = a^{-1}\eta_1, \quad X' = \lambda X, \quad Y' = \lambda^{-1}Y \qquad (a \neq \pm 1),$$

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

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 $\frac{1}{4}(p^n - 1)(p^n - 3)$ or $\frac{1}{4}2^n(2^n - 2)$ 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 λ and λ^{-1} interchanged. A substitution of $SA(4, p^n)$ commutative with one having the canonical form (18) has simultaneously the canonical form

$$\xi_1' = c\xi_1, \quad \eta_1' = c^{-1}\eta_1, \quad X' = \tau X, \quad Y' = \tau^{-1}Y,$$

where c is any mark $\neq 0$ of the $GF[p^n]$ and τ 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 $p^{4n}(p^{4n} - 1)$ 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

$$(20) \qquad \xi_1' = r\xi_1 + s\eta_1, \quad \eta_1' = t\xi_1 + u\eta_1, \quad X' = \tau X, \quad Y' = \tau^{-1}Y,$$

where $ru - st = 1$, giving $p^n(p^{2n} - 1)(p^n + 1)$ substitutions. Each type thus represents $p^{3n}(p^{2n} + 1)(p^n - 1)$ conjugate substitutions of $SA(4, p^n)$.

For $b = 1$ or a not-square ν, there are altogether $2(p^n - 1)$ or 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 $2^n(2^n + 1)$ substitutions. Hence each type represents a set of $\frac{1}{2}p^{3n}(p^{4n} - 1)(p^n - 1)$ or $2^{3n}(2^{4n} - 1)(2^n - 1)$ 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* ξ_1 *by* $\gamma\eta_1$.

Let S replace ξ_1 by $\omega \equiv a_{11}\xi_1 + \gamma_{11}\eta_1 + a_{12}\xi_2 + \gamma_{12}\eta_2$. Suppose first that $\gamma_{11} \neq 0$. There exists in $SA(4, p^n)$ a substitution T which replaces ξ_1 by $\gamma_{11}^{-1}\xi_1$ and η_1 by ω [compare § 4]. Then $T^{-1}ST$ replaces ξ_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 β_{11}, γ_{22} or β_{22} in the place of the former γ_{11}. By an earlier transformation, we can make $\beta_{12} = \gamma_{12} = 0$.* The resulting substitution is

$$S' \equiv \begin{pmatrix} a_{11} & 0 & a_{12} & 0 \\ 0 & \delta_{11} & 0 & \delta_{12} \\ a_{21} & \gamma_{21} & a_{22} & 0 \\ \beta_{21} & \delta_{21} & 0 & \delta_{22} \end{pmatrix}.$$

The transform of S' by $\eta_1' = \eta_1 + \eta_2$, $\xi_2' = \xi_2 - \xi_1$ has β_{21} as the coefficient of ξ_1 in η_1'. Hence $\beta_{21} = 0$. Similarly $\gamma_{21} = 0$. Next L_{11} transforms S' into a substitution with $\delta_{11} - a_{11}$ as the coefficient of η_1 in ξ_1'. Hence $\delta_{11} = a_{11}$ and similarly $\delta_{22} = a_{22}$. The transform of S' by $N_{121}: \xi_1' = \xi_1 + \eta_2$, $\xi_2' = \xi_2 + \eta_1$, has $\delta_{21} - a_{12}$ as the coefficient of η_1 in ξ_1'. Hence $a_{12} = \delta_{21}$ and similarly $a_{21} = \delta_{12}$. Now a_{12} or δ_{12} is not zero, since otherwise the characteristic equation has a root a_{11} or δ_{11} in the field. The transformed of S' by

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

has the form

$$\begin{pmatrix} 0 & 0 & a_{12}' & 0 \\ 0 & 0 & 0 & \delta_{12} \\ \delta_{12} & 0 & 0 & 0 \\ 0 & a_{12}' & 0 & 0 \end{pmatrix}.$$

It is transformed by $T_{2a_{12}'}$ 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

$$(21) \qquad \begin{pmatrix} 0 & \gamma_{11} & 0 & 0 \\ \beta_{11} & \delta_{11} & \beta_{12} & \delta_{12} \\ 0 & \gamma_{21} & a_{22} & \gamma_{22} \\ 0 & \beta_{21} & \beta_{22} & \delta_{22} \end{pmatrix}$$

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

* Quarterly Journal of Mathematics, vol. 32, pp. 42–63, § 5, 1900.

$$S_1 \equiv \begin{Vmatrix} 0 & \gamma_{11} & 0 & 0 \\ \beta_{11} & \delta_{11} & 1 & 0 \\ 0 & \gamma_{11}\gamma_{22} & \alpha_{22} & \gamma_{22} \\ 0 & \gamma_{11}\delta_{22} & \beta_{22} & \delta_{22} \end{Vmatrix} \qquad (\beta_{11}\gamma_{11} = -1, \quad \alpha_{22}\delta_{22} - \beta_{22}\gamma_{22} = 1).$$

It has the characteristic determinant

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

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

$$\sigma + \lambda = \alpha_{22} + \delta_{22} + \delta_{11}, \quad \sigma\lambda = (\alpha_{22} + \delta_{22})\delta_{11} - \gamma_{11}\gamma_{22}$$

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

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

§ 15.

We seek the conditions under which new indices

$$X \equiv a\xi_1 + b\eta_1 + c\xi_2 = d\eta_2, \quad Y \equiv a_1\xi_1 + b_1\eta_1 + c_1\xi_2 + d_1\eta_2$$

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, $\cdots$, are marks of the $GF[p^n]$ satisfying the equation

$$(23) \qquad \begin{vmatrix} a & b \\ a_1 & b_1 \end{vmatrix} + \begin{vmatrix} c & d \\ c_1 & d_1 \end{vmatrix} = 1.$$

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

$$\begin{cases} a_1 = b\beta_{11}, & b_1 = a\gamma_{11} + b\delta_{11} + c\gamma_{11}\gamma_{22} + d\gamma_{11}\delta_{22}, \\ c_1 = b + c\alpha_{22} + d\beta_{22}, & d_1 = c\gamma_{22} + d\delta_{22}, \end{cases}$$

$$\begin{cases} -a = -a_1A + b_1\beta_{11}, & -b = a_1\gamma_{11} + b_1(\delta_{11} - A) + c_1\gamma_{11}\gamma_{22} + d_1\gamma_{11}\delta_{22}, \\ -c = b_1 + c_1(\alpha_{22} - A) + d_1\beta_{22}, & -d = c_1\gamma_{22} + d_1(\delta_{22} - A). \end{cases}$$

On substitution of the values of a_1, b_1, c_1, d_1 into the second set of equations, we have the following equations:

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

$$(25) \quad a(\delta_{11} - A)\gamma_{11} + b(\gamma_{11}\gamma_{22} + \delta_{11}^2 - \delta_{11}A) + c\gamma_{11}\gamma_{22}(\alpha_{22} + \delta_{22} + \delta_{11} - A) + d\gamma_{11}(\delta_{22}^2 + \beta_{22}\gamma_{22} + \delta_{11}\delta_{22} - A\delta_{22}) = 0,$$

$$(26) \quad a\gamma_{11} + b(\delta_{11} + \alpha_{22} - A) + c\{\gamma_{11}\gamma_{22} + \alpha_{22}(\alpha_{22} + \delta_{22} - A)\} + d\{\gamma_{11}\delta_{22} + \beta_{22}(\alpha_{22} + \delta_{22} - A)\} = 0,$$

$$(27) \qquad b\gamma_{22} + c\gamma_{22}(\alpha_{22} + \delta_{22} - A) + d\delta_{22}(\alpha_{22} + \delta_{22} - A) = 0.$$

Multiplying (24) by $a_{22}+\delta_{22}-A$ and adding to (27), we find

$$\gamma_{22}+\beta_{11}(\delta_{11}-A)(a_{22}+\delta_{22}-A)=0\,. \tag{28}$$

Indeed, if $b=0$, then $a_1=0$, $a=0$; then (24) and (26) require

$$a_{22}+\delta_{22}-A=0\,,$$

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 γ_{11}^2 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 A determined by (28), viz.,

$$A^2-A(\delta_{11}+a_{22}+\delta_{22})+\delta_{11}(a_{22}+\delta_{12})-\gamma_{11}\gamma_{22}=0\,,$$

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

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

$$A=\delta_{11}\,,\quad A'=a_{22}+\delta_{22}\,.$$

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 A, equation (27) may be dropped from consideration. Multiplying (24) by γ_{11} and adding to (26), we find

$$a\gamma_{11}+ba_{22}+ca_{22}(a_{22}+\delta_{22}-A)+d\beta_{22}(a_{22}+\delta_{22}-A)=0\,. \tag{26'}$$

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

$$d=a(\delta_{11}-A)\,. \tag{25'}$$

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

$$a_{22}\{a\gamma_{11}\delta_{22}+b+c(a_{22}+\delta_{22}-A)\}=0\,,$$

$$(\delta_{11}-A)\{a\gamma_{11}\delta_{22}+b+c(a_{22}+\delta_{22}-A)\}=0\,.$$

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

$$b=-a\gamma_{11}\delta_{22}-c(a_{22}+\delta_{22}-A)\,. \tag{29}$$

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

$$\begin{vmatrix} a & b \\ a_1 & b_1 \end{vmatrix} \equiv a^2\gamma_{11} + ab\delta_{11} - \delta^2\beta_{11} = 1.$$

For $p = 2$, we may take $b = 0$, $a = \gamma_{11}^{\frac{1}{2}}$, every mark of the $GF[2^n]$ being a square. For $p > 2$, the condition may be written

$$(a - \tfrac{1}{2} b\beta_{11}\delta_{11})^2 + b^2\beta_{11}^2(1 - \tfrac{1}{4}\delta_{11}^2) = -\beta_{11}.$$

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 $L'_{2\tau}$, $\delta_{22} + \tau\gamma_{22} = 0$, is of the form S_1 with $\delta_{22} = 0$, $\gamma_{22} \neq 0$. 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

$$(a_{22} + \delta_{11} - 2A)\{a^2\gamma_{11}^2 - ac\gamma_{11}A(a_{22} - A) + c^2(a_{22} - A)^2\} = \gamma_{11}(a_{22} - A).$$

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

$$4\gamma_{11}\gamma_{22} + (a_{22} - \delta_{11})^2 \equiv (a_{22} + \delta_{11} \mp 4)^2,$$

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

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

$$(30) \qquad \begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & A & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & A' \end{bmatrix}.$$

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 $L'_{2\tau}$ and make $\delta_{22} = 0$, obtaining the substitution

$$S_2 \equiv \begin{bmatrix} 0 & \gamma_1 & 0 & 0 \\ -\gamma_1^{-1} & \delta & 1 & 0 \\ 0 & \gamma_1\gamma & a & \gamma \\ 0 & 0 & -\gamma^{-1} & 0 \end{bmatrix}.$$

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,

$$(31) \qquad -4\gamma\gamma_1 = (a - \delta)^2.$$

A second result of the investigation is that S is conjugate with a substitution of the form S_2 within $SA(4, p^n)$ 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.

§16. *Characteristic determinant the square of an irreducible quadratic.*

Consider the following substitution of the form S_2:

$$(32) \qquad \Sigma_2 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ 0 & c & a & c \\ 0 & 0 & -c^{-1} & 0 \end{bmatrix} \qquad (-4c = a^2).$$

It has the characteristictic determinant (whether $p = 2$ or $p > 2$)

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

* If $p > 2$ and (31) is satisfied, $\Delta(\kappa) = \{\kappa^2 - \frac{1}{2}(a + \delta)\kappa + 1\}^2$.

A substitution S_2 satisfying (31) will have the same characteristic determinant as Σ_2 if, and only if, $\alpha = \alpha + \delta$, and for $p = 2$, $c = a^2 - \gamma\gamma_1$. The latter are consequently necessary conditions for the conjugacy of S_2 and Σ_2 under linear transformation. We proceed to prove that, if S_2 satisfy the condition (31) and if $\kappa^2 - (-c)^{\frac{1}{2}}\kappa + 1$ be irreducible in the $GF[p^n]$, then $\alpha = \alpha + \delta$, together with $c = a^2 - \gamma\gamma_1$ if $p = 2$, are sufficient conditions for the conjugacy of S_2 and Σ_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 $\alpha = \alpha + \delta$, $-4c = a^2$ and (31):

$$\gamma_{11} = -\gamma_1\beta_{11}, \quad ca_{12} = \gamma_1\delta_{12}, \quad \gamma_{22} = -\gamma c\beta_{22}, \quad a_{21} = \gamma\delta_{21},$$
$$ca_{12} = -a_{11} + \gamma_1\delta_{11}, \qquad c\gamma_1\beta_{12} = -aa_{11} + a\gamma_1\delta_{11} + c\gamma_{11} - \gamma_{12},$$
$$a_{21} = \gamma_1^{-1}a_{11} - \delta_{11} - \delta\beta_{11}, \qquad \gamma_1\gamma_{21} = a\gamma_1\delta_{11} + c\gamma_{11} - aa_{11} - \gamma_{12},$$
$$\gamma_1\gamma\beta_{21} = \delta a_{11} + \gamma_{12}, \qquad \gamma\gamma_1 c\beta_{22} = aa_{11} - c\gamma_{11} - a\gamma_1\delta_{11},$$
$$a_{22} = \delta_{11} + a\beta_{12}, \qquad \gamma\gamma_1\delta_{22} = ca_{11} - a\gamma_{12}.$$

It suffices to take $a_{12} = 0$. Setting $\rho \equiv \gamma_1^{-1}\gamma_{12}$, we have S in the form

$$\begin{bmatrix} \gamma_1\delta_{11} & -\gamma_1\beta_{11} & 0 & \gamma_1\rho \\ \beta_{11} & \delta_{11} & -\beta_{11} - c^{-1}\rho & 0 \\ -\delta\beta_{11} & -\delta\delta_{11} - c\beta_{11} - \rho & \delta_{11} - a\beta_{11} - ac^{-1}\rho & -c\beta_{11} \\ \gamma^{-1}\delta\delta_{11} + \gamma^{-1}\rho & -\gamma^{-1}\delta\beta_{11} & \gamma^{-1}\beta_{11} & c\gamma^{-1}\delta_{11} - a\gamma^{-1}\rho \end{bmatrix}.$$

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

$$\delta_{11}^2 + \beta_{11}^2 + \beta_{11}\rho + c^{-1}\rho^2 = \gamma_1^{-1},$$
$$-\delta\delta_{11}^2 - \delta\beta_{11}^2 - c\delta_{11}\beta_{11} - 2\delta_{11}\rho + a\beta_{11}\rho + ac^{-1}\rho^2 = 0. \tag{33}$$

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

$$(a + \delta)(\delta_{11}^2 + \beta_{11}^2) + c\delta_{11}\beta_{11} + 2\delta_{11}\rho = a\gamma_1^{-1}. \tag{34}$$

If $p > 2$, we may eliminate ρ between (33) and (34) and find

$$\delta_{11}^2\{-\beta_{11}^2(c + 4) + 8a^{-1}a\gamma_1^{-1} - 4\gamma_1^{-1}\} = \{2\beta_{11}^2 - (-c)^{-\frac{1}{2}}a\gamma_1^{-1}\}^2. \tag{35}$$

We prove that there exists a mark β_{11}^2 making the coefficient of δ_{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 τ be square, we may take $\beta_{11} = 0$, when (35) determines $\delta_{11} \neq 0$ and (34) determines ρ. Suppose finally that τ is a not-square. Since $\kappa^2 - (-c)^{\frac{1}{2}}\kappa + 1$

is irreducible, $-c-4$ is a not-square. After we divide (35) by τ, the question is the possibility of finding a mark μ^2 such that μ^2+1 is a not-square. There are $\frac{1}{4}(p^n \mp 1)$ such squares $\mu^2 \neq 0$, according as $p^n = 4l \pm 1$.* Hence for $p^n > 5$, there are at least two marks β_{11}^2 making the coefficient of δ_{11}^2 in (35) a square, and hence at least one mark β_{11}^2 making also the right member $\neq 0$. Then δ_{11} is determined different from zero, so that (34) gives ρ.

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

$$\beta_{11}^2 = \pm 1, \quad (-c)^{-\frac{1}{2}} a\gamma_1^{-1} = \pm 2.$$

Then τ is a not-square only when $\gamma_1^{-1} = +1$ or -1. Since γ_1 is a square, it may be taken to be $+1$ by an earlier transformation of S_2 by $T_{1\omega}T_{2\omega^{-1}}$, ω being suitably chosen. With $\gamma_1 = 1$, then $a^{-1}a = \pm 1$. But $a^{-1}a = 1$ makes τ 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 β_{11}^2 was chosen to make the coefficient of δ_{11}^2 a square, and since τ 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 Σ_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

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

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 $c\delta_{11}\beta_{11} = a\gamma_1^{-1}$. The latter together with (33) are to be satisfied by marks β_{11}, δ_{11}, ρ of the $GF[2^n]$. Letting $\rho = c\beta_{11}r^2$ in (33), dividing by $c\beta_{11}^2$ and extracting the square root, we find

$$r^2 + r \equiv c^{-\frac{1}{2}} + \frac{\gamma_1^{-\frac{1}{2}} + \delta_{11}}{c^{\frac{1}{2}}\beta_{11}} \pmod 2$$

$$= c^{-\frac{1}{2}} + g\delta_{11}(\gamma_1^{-\frac{1}{2}} + \delta_{11})$$

*American Journal of Mathematics, vol. 21, p. 196.

upon eliminating β_{11} and denoting the constant $c^{\frac{1}{2}}a^{-1}\gamma_1$ by g. It remains to prove that a mark δ_{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,

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

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

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

If, for every mark δ_{11}, the equation in r be irreducible, then

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

must be an identity modulo 2 in the variable δ_{11}. This will be the case if, and only if, $g = g^2\gamma_1^{-1}$, whence $g = \gamma_1$. The latter requires $c = a^2$. But $c = a^2 - \gamma\gamma_1$. 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 σ, σ^{-1}, σ^{p^n}, σ^{-p^n}; in the former case $\sigma^{p^{2n}+1} = 1$, in the latter case $\sigma^{p^{2n}-1} = 1$. We may write $\Delta(\kappa) = 0$ in the form

$$\sigma^2\gamma\gamma_1 = (\sigma^2 - \sigma a + 1)(\sigma^2 - \sigma\delta + 1) . \tag{36}$$

The substitution S_2 given at the end of § 15, multiplies by σ the function

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

Denote by Y_1, X_2, Y_2 the linear functions derived from X_1 upon replacing σ by σ^{-1}, σ^{p^n}, σ^{-p^n} respectively. If $\Delta(\kappa)$ be irreducible, so that σ belongs to the $GF[p^{4n}]$, the functions X_1, Y_1, X_2, Y_2 are conjugate with respect to the $GF[p^n]$. In the second case, σ 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

$$X_1' = \sigma X_1 , \quad Y_1' = \sigma^{-1}Y_1 , \quad X_2' = \sigma^{p^n}X_2 , \quad Y_2' = \sigma^{-p^n}Y_2 . \tag{37}$$

* 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,

$$\begin{vmatrix} -\gamma & \sigma\gamma\gamma_1 \\ -\gamma & \sigma^{p^n}\gamma\gamma_1 \end{vmatrix} + \begin{vmatrix} \sigma^2 - \sigma\delta + 1 & \sigma^{-1}\gamma(\sigma^2 - \sigma\delta + 1) \\ \sigma^{2p^n} - \sigma^{p^n}\delta + 1 & \sigma^{-p^n}\gamma(\sigma^{2p^n} - \sigma^{p^n}\delta + 1) \end{vmatrix}$$

$$= \gamma(\sigma - \sigma^{p^n})\{\gamma\gamma_1 + (\sigma^2 - \sigma\delta + 1)(\sigma^{2p^n} - \sigma^{p^n}\delta + 1)\sigma^{-p^n-1}\}.$$

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

$$\sigma^{p^n-1}(\sigma^2 - \sigma a + 1) + \sigma^{2p^n} - \sigma^{p^n}\delta + 1 = 0.$$

The latter is derived by multiplying by σ^{p^n} the identity

$$\sigma + \sigma^{-1} + \sigma^{p^n} + \sigma^{-p^n} = a + \delta,$$

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

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

Replacing σ by σ^{-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):

$$\begin{vmatrix} -\gamma & \sigma\gamma\gamma_1 \\ -\gamma & \sigma^{-1}\gamma\gamma_1 \end{vmatrix} + \begin{vmatrix} \sigma^2 - \sigma\delta + 1 & \sigma^{-1}\gamma(\sigma^2 - \sigma\delta + 1) \\ \sigma^{-2} - \sigma^{-1}\delta + 1 & \sigma\gamma(\sigma^{-2} - \sigma^{-1}\delta + 1) \end{vmatrix}$$

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

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

$$2(\sigma^2 - \sigma\delta + 1)\left(\sigma^2 - \frac{a+\delta}{2}\sigma + 1\right)$$

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

$$\gamma(\sigma^{p^n} - \sigma^{-p^n})C^{p^n}.$$

If $\sigma^{p^{2n}} = \sigma$, it is only necesary that X_1 and X_2, Y_1 and Y_2 be conjugate with respect to the $GF[p^n]$. When we take μX_1 in place of X_1 and $\mu^{p^n}X_2$ in place of X_2, the canonical form (37) is preserved, as well as the abelian relations (3) and (4) just established. In case μ 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 $GF[p^{2n}]$ on two pairs of conjugate indices. In this case it follows that two substitutions S_2 having the same characteristic equation are conjugate within $SA(4, p^n)$.

If $\Delta(\kappa) = 0$ be irreducible, so that $\sigma^{p^{2n}} = \sigma^{-1}$, the replacement of X_1 by μX_1 requires the replacement of Y_1 by $\mu^{p^{2n}} Y_1$, X_2 by $\mu^{p^n} X_2$, Y_2 by $\mu^{p^{3n}} Y_2$. The above expression $\gamma(\sigma - \sigma^{-1})C$ is then multiplied by $\mu^{p^{2n}+1}$, a mark of the $GF[p^{2n}]$; the product can not be made unity by choice of μ, since C belongs to the $GF[p^{2n}]$, while $\sigma - \sigma^{-1}$ 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

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

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

$$\phi \equiv \begin{vmatrix} \xi_1 & \eta_1 \\ \bar{\xi}_1 & \bar{\eta}_1 \end{vmatrix} + \begin{vmatrix} \xi_2 & \eta_2 \\ \bar{\xi}_2 & \bar{\eta}_2 \end{vmatrix}, \quad \phi' \equiv (\sigma - \sigma^{-1}) \begin{vmatrix} \xi_1 & \eta_1 \\ \bar{\xi}_1 & \bar{\eta}_1 \end{vmatrix} + (\sigma^{p^n} - \sigma^{-p^n}) \begin{vmatrix} \xi_2 & \eta_2 \\ \bar{\xi}_2 & \bar{\eta}_2 \end{vmatrix},$$

when T operates cogrediently upon the indices ξ_i, η_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 ϕ 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 ϕ under A, the latter may be expressed as a special abelian substitution on ξ_i, η_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 $\kappa^2 - \rho\kappa + \tau$, $\tau \neq 1$, 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 $\sigma^{p^{2n}+1} = 1$. Of the solutions of the latter, only $\sigma = \pm 1$ satisfy also $\sigma^{p^{2n}-1} = 1$, so that there remain $p^{2n} - 1$ or 2^{2n} suitable values of σ. Replacing σ by σ^{-1}, we obtain from (37) a substitution which is transformed into (37) by M_1M_2; replacing σ by σ^{-p^n}, we obtain the transform of (37) by $P_{12}M_1$. Replacing σ by σ^{p^n}, we obtain the transform of (37) by $P_{12}M_2$. Any new replacement of σ leads to a substitution not conjugate with (37). Hence there are $\frac{1}{4}(p^{2n} - 1)$ or $\frac{1}{4}2^{2n}$ 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

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

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 $\sigma^{p^{2n}-1} = 1$, $\sigma^{p^n} \neq \sigma$, $\sigma^{p^n} \neq \sigma^{-1}$. The $(p^n-1)^2$ or $2^{2n} - 2 \cdot 2^n$ suitable values of σ give, in sets of four, conjugate substitutions. Hence there are $\frac{1}{4}(p^n-1)^2$ or $\frac{1}{4}2^n(2^n-2)$ non-conjugate types. Each is commutative with $p^{2n}-1$ substitutions and therefore conjugate with exactly $p^{4n}(p^{4n}-1)$ 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

$$(38) \qquad X_1' = \lambda X_1, \quad Y_1' = \lambda^{-1} Y_1, \quad X_2' = \mu X_2, \quad Y_2' = \mu^{-1} Y_2,$$

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 $\mu = \lambda$, λ^{-1} are to be excluded. Hence there are $(p^n-1)(p^n-3)$ or $2^n(2^n-2)$ pairs of suitable values λ, μ. But λ and λ^{-1} are interchanged upon transforming (38) by M_1; μ and μ^{-1} upon transforming by M_2; λ and μ, λ^{-1} and μ^{-1} upon transforming by P_{12}. Hence eight of the pairs of values λ, μ 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

$$X_1' = \tau^l X_1, \quad Y_1' = \tau^{-l} Y_1, \quad X_2' = \tau^m X_2, \quad Y_2' = \tau^{-m} Y_2,$$

τ 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 $p^{4n}(p^{2n}+1)(p^n-1)^2$ 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

$$(39) \qquad X_1' = \lambda X_1, \quad Y_1' = \lambda^{-1} Y_1, \quad X_2' = \lambda Y_2, \quad Y_2' = \lambda^{-1} Y_2,$$

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

$$X_1' = aX_1 + \beta X_2, \qquad X_2' = \gamma X_1 + \delta X_2,$$
$$Y_1' = a^{p^n} Y_1 + \beta^{p^n} Y_2, \quad Y_2' = \gamma^{p^n} Y_1 + \delta^{p^n} Y_2,$$

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 $\begin{pmatrix} a & \beta \\ \gamma & \delta \end{pmatrix}$ 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) $X_1' = \sigma X_1, \quad Y_1' = \sigma^{-1} Y_1 + \sigma^{-1} X_2, \quad X_2' = \sigma^{-1} X_2, \quad Y_2' = \sigma Y_2 + \sigma X_1,$

σ being a root of $\Delta(\kappa) = 0$. As in § 17, we employ new indices

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

and X_2 obtained from X_1 by replacing σ 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

$$-\gamma^3\gamma_1(\sigma - \sigma^{-1})^4 \neq 0.$$

Upon replacing σ by σ^{-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

$$X_1' = aX_1, \quad Y_1' = a^{p^n} Y_1 + d^{p^n} X_2, \quad X_2' = a^{p^n} X_2, \quad Y_2' = aY_2 + dX_1,$$

where $a^{p^n+1} = 1$, $a^{p^n} d = ad^{p^n}$, so that $d = a\kappa$, κ 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 μ denotes 1 or a particular not-square ν when $p > 2$; while $\mu = 1$, if $p = 2$. Also, θ 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_1 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.

Type.	Number of types.		Number of conjugate substitutions of each type.
	$p>2$	$p=2$	
(6)	$\frac{1}{8}(p^n-3)(p^n-5)$	$(2^{n-1}-1)(2^{n-2}-1)$	$p^{4n}(p^{2n}+1)(p^n+1)^2$
(7)	$\frac{1}{2}(p^n-3)$	$2^{n-1}-1$	$p^{3n}(p^{2n}+1)(p^n+1)$
(8)	$\frac{1}{2}(p^n-3)$	$2^{n-1}-1$	$p^{3n}(p^{4n}-1)(p^n+1)$
(9), $\beta=0$	p^n-3	$2^{n-1}-1$	$p^{3n}(p^{2n}+1)(p^n+1)$
(9), $\beta=\mu$	$2(p^n-3)$	$2^{n-1}-1$	$\theta p^{3n}(p^{4n}-1)(p^n+1)$
$T_{1\,\pm1}T_{2\,\pm1}$	2	1	1
$L_{1\,\mu}T_{1\,\pm1}T_{2\,\pm1}$	4	1	$\theta(p^{4n}-1)$
$L_{1\,1}L_{2\,1}T_{1\,\pm1}T_{2\,\pm1}$	2		$\frac{1}{2}p^n(p^{4n}-1)(p^n+\epsilon)$
		1	$(2^{4n}-1)(2^{2n}-1)$
$L_{1\,\nu}L_{2\,1}T_{1\,\pm1}T_{2\,\pm1}$	2		$\frac{1}{2}p^n(p^{4n}-1)(p^n-\epsilon)$
(13)		1	$2^{4n}-1$
R_β, R_0		2	$\frac{1}{2}2^{2n}(2^{4n}-1)(2^{2n}-1)$
$A_\mu T_{1\,\pm1}T_{2\,\pm1}$	4		$\frac{1}{2}p^{2n}(p^{4n}-1)(p^{2n}-1)$
(18)	$\frac{1}{4}(p^n-1)(p^n-3)$	$2^{n-1}(2^{n-1}-1)$	$p^{4n}(p^{4n}-1)$
(19), $b=0$	p^n-1	2^{n-1}	$p^{3n}(p^{2n}+1)(p^n-1)$
(19), $b=\mu$	$2(p^n-1)$	2^{n-1}	$\theta p^{3n}(p^{4n}-1)(p^n-1)$
(37), $\sigma^{p^{2n}+1}=1$	$\frac{1}{4}(p^{2n}-1)$	2^{2n-2}	$p^{4n}(p^{2n}-1)^2$
(37), $\sigma^{p^{2n}-1}=1$	$\frac{1}{4}(p^n-1)^2$	$2^{n-1}(2^{n-1}-1)$	$p^{4n}(p^{4n}-1)$
(38)	$\frac{1}{8}(p^n-1)(p^n-3)$	$2^{n-2}(2^{n-1}-1)$	$p^{4n}(p^{2n}+1)(p^n-1)^2$
(39)	$\frac{1}{2}(p^n-1)$	2^{n-1}	$p^{3n}(p^{2n}+1)(p^n-1)$
(40)	$\frac{1}{2}(p^n-1)$	2^{n-1}	$p^{3n}(p^{4n}-1)(p^n-1)$
$T_{1\,-1}$	1		$p^{2n}(p^{2n}+1)$
$L_{1\,\mu}T_{1\,-1}$ $L_{2\,\mu}T_{1\,-1}$	4		$\frac{1}{2}p^{2n}(p^{4n}-1)$
$L_{1\,1}T_{1\,-1}L_{2\,\mu}$ $L_{1\,\nu}T_{1\,-1}L_{2\,\mu}$	4		$\frac{1}{4}p^{2n}(p^{4n}-1)(p^{2n}-1)$

§ 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

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

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

$$R_1 \equiv L_{21}M_2S'M_2L'_{21} \sim (2456), \quad R_0 \equiv M_2L'_{11}S'L_{21} \sim (13)(2456),$$

$$[13] \equiv L'_{11}L'_{21}S' \sim (13)(46)(25).$$

By § 12, there is a single type $L_{21}M_2$ given by (19′) for $b = 0$ and a single type $L'_{11}\,L_{21}\,M_2$ given by (19′) for $b = 1$, The single type (39) may be represented by $L_{11}\,M_1L_{21}M_2$. The single types (40) and (37), $\sigma^{p^{2n}+1} = 1$, may be represented respectively by

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

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

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

* Proceedings of the London Mathematical Society, vol. 31, p. 40, 1899.

† The abelian substitution numbered (13) is now referred to as [13].

Type.	Number of conjugates.	Corresponding substitution on six letters.
identity	1	identity
L_{11}	15	(23)
$L_{11}L_{21}$	45	(23)(45)
[13]	15	(13)(25)(46)
R_1	90	(2456)
R_0	90	(13)(2456)
$L_{21}M_2$	40	(465)
$L'_{11}L_{21}M_2$	120	(13)(465)
[37]	144	(16523)
$L_{11}M_1L_{21}M_2$	40	(123)(465)
[40]	120	(164523)

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.

§ 25. *Operators of the simple group* $A(4, p^n)$, $p > 2$.

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 $T \equiv T_{1-1}T_{2-1}$, 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_1 into S, then WVW^{-1} will transform S_1 into S_1T.

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

*Quarterly Journal of Mathematics, vol. 29, pp. 169-178, 1897; vol. 31, pp. 383-4, 1899.

† 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_s if S be conjugate with ST within the group. For example, there is a single special type $(7)_s$,

$$\xi_1' = i\xi_1, \quad \eta_1' = -i\eta_1, \quad \xi_2' = -i\xi_2, \quad \eta_2' = i\eta_2 \qquad (i^2 = -1),$$

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 κ^{-1}, contrary to the hypothesis for type (6). Second, if $-\kappa = \lambda$, we have the special type

$$(6)_s \qquad \xi_1' = \kappa\xi_1, \quad \eta_1' = \kappa^{-1}\eta_1, \quad \xi_2' = -\kappa\xi_2, \quad \eta_2' = -\kappa^{-1}\eta_2,$$

which may be transformed into $(6)_s T$ 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 $(6)_s$ 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 $(6)_s$ by M_2.

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

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

To determine the special types (37), $\sigma^{p^{2n}-1} = 1$, $\sigma^{p^n-1} \neq 1$, $\sigma^{p^n+1} \neq 1$, 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 σ 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 $p^n \mp 1$ such values of σ according as $p^n = 4l \pm 1$. The two sets of values for σ are wholly distinct since $\sigma^2 \neq 1$. Hence there are $2p^n - 2$ values σ, whatever be the form of p^n, $p > 2$. Hence there are $\frac{1}{2}(p^n - 1)$ special types (37) when $\sigma^{p^{2n}-1} = 1$.

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

$$(38)_s \qquad X_1' = \lambda X_1, \quad Y_1' = \lambda^{-1} Y_1, \quad X_2' = -\lambda X_2, \quad Y_2' = -\lambda^{-1} Y_2,$$

since P_{12} transforms it into $(38)_s T$. 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:

TABLE OF THE NON-CONJUGATE TYPES*
OF OPERATORS OF THE SIMPLE GROUP $A(4, p^n)$, $p > 2$,
OF ORDER $\frac{1}{2}p^{4n}(p^{4n}-1)(p^{2n}-1)$.

Type.	Number of distinct types.	
	$p^n = 4l+1$,	$p^n = 4l-1$
$(6)_s$	$\frac{1}{4}(p^n-5)$,	$\frac{1}{4}(p^n-3)$
(6)	$\frac{1}{16}(p^n-5)^2$,	$\frac{1}{16}(p^n-3)(p^n-7)$
$(7)_s$	1,	0
(7)	$\frac{1}{4}(p^n-5)$,	$\frac{1}{4}(p^n-3)$
$(8)_s$	1,	0
(8)	$\frac{1}{4}(p^n-5)$,	$\frac{1}{4}(p^n-3)$
(9), $\beta = 0$	$\frac{1}{2}(p^n-3)$	
(9), $\beta = \mu$	p^n-3	
identity	1	
$L_{1\mu}$	2	
$L_{11}L_{21}$	1	
$L_{1\nu}L_{21}$	1	
A_μ	2	
(18)	$\frac{1}{8}(p^n-1)(p^n-3)$	
(19), $b = 0$	$\frac{1}{2}(p^n-1)$	
(19), $b = \mu$	p^n-1	
(37), $\sigma^{p^{2n}+1} = 1$	$\frac{1}{8}(p^{2n}-1)$	
$(37)_s$, $\sigma^{p^{2n}-1} = 1$	$\frac{1}{2}(p^n-1)$	
(37), $\sigma^{p^{2n}-1} = 1$	$\frac{1}{8}(p^n-1)(p^n-3)$	
$(38)_s$	$\frac{1}{4}(p^n-1)$,	$\frac{1}{4}(p^n-3)$
(38)	$\frac{1}{16}(p^n-1)(p^n-5)$,	$\frac{1}{16}(p^n-3)^2$
$(39)_s$	0,	1
(39)	$\frac{1}{4}(p^n-1)$,	$\frac{1}{4}(p^n-3)$
$(40)_s$	0,	1
(40)	$\frac{1}{4}(p^n-1)$,	$\frac{1}{4}(p^n-3)$
T_{1-1}	1	
$L_{1\mu}T_{1-1}$	2	
$L_{11}L_{2\nu}T_{1-1}$	1	
$L_{1\mu}L_{2\mu}T_{1-1}$	2	

Number of operators conjugate with each type.
$\frac{1}{2}p^{4n}(p^{2n}+1)(p^n+1)^2$
$p^{4n}(p^{2n}+1)(p^n+1)^2$
$\frac{1}{2}p^{3n}(p^{2n}+1)(p^n+1)$
$p^{3n}(p^{2n}+1)(p^n+1)$
$\frac{1}{2}p^{3n}(p^{4n}-1)(p^n+1)$
$p^{3n}(p^{4n}-1)(p^n+1)$
$p^{3n}(p^{2n}+1)(p^n+1)$
$\frac{1}{2}p^{3n}(p^{4n}-1)(p^n+1)$
1
$\frac{1}{2}(p^{4n}-1)$
$\frac{1}{2}p^n(p^{4n}-1)(p^n+\epsilon)$
$\frac{1}{2}p^n(p^{4n}-1)(p^n-\epsilon)$
$\frac{1}{2}p^{2n}(p^{4n}-1)(p^{2n}-1)$
$p^{4n}(p^{4n}-1)$
$p^{3n}(p^{2n}+1)(p^n-1)$
$\frac{1}{2}p^{3n}(p^{4n}-1)(p^n-1)$
$p^{4n}(p^{2n}-1)^2$
$\frac{1}{2}p^{4n}(p^{4n}-1)$
$p^{4n}(p^{4n}-1)$
$\frac{1}{2}p^{4n}(p^{2n}+1)(p^n-1)^2$
$p^{4n}(p^{2n}+1)(p^n-1)^2$
$\frac{1}{2}p^{3n}(p^{2n}+1)(p^n-1)$
$p^{3n}(p^{2n}+1)(p^n-1)$
$\frac{1}{2}p^{3n}(p^{4n}-1)(p^n-1)$
$p^{3n}(p^{4n}-1)(p^n-1)$
$\frac{1}{2}p^{2n}(p^{2n}+1)$
$\frac{1}{2}p^{2n}(p^{4n}-1)$
$\frac{1}{4}p^{2n}(p^{4n}-1)(p^{2n}-1)$
$\frac{1}{8}p^{2n}(p^{4n}-1)(p^{2n}-1)$

*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 μ denotes 1 or a particular not-square ν; ϵ denotes ± 1 according as $p^n = 4l \pm 1$. The total number of non-conjugate types in the simple group $A(4, p^n)$, $p > 2$, is the same function of p^n in the two cases $p^n = 4l \pm 1$, viz.:

$$\tfrac{1}{2}(p^{2n} + 1) + 3p^n + 6.$$

§ 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_{1-1}; type (37), $\sigma^4 = -1$, by $P_{12}M_1$; type (40) by $P_{12}L_{1-1}T_{1-1}$; type (37), $\sigma^{10} = 1$, by S_2 for $\gamma_1 = 1$, $\gamma = a = \delta = -1$, viz.,

$$K \equiv \begin{Vmatrix} 0 & 1 & 0 & 0 \\ -1 & -1 & 1 & 0 \\ 0 & -1 & -1 & -1 \\ 0 & 0 & 1 & 0 \end{Vmatrix},$$

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 $P_{12}L_{1-1}T_{1-1}$; 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

Type.	Period.	Conjugates.	Type.	Period.	Conjugates.
L_{11}	3	40	identity	1	1
L_{1-1}	3	40	A_1	9	2880
$L_{11}L_{21}$	3	240	A_{-1}	9	2880
$L_{1-1}L_{21}$	3	480	M_2	4	540
T_{1-1}	2	45	M_2L_{11}	12	2160
$L_{11}T_{1-1}$	6	360	M_2L_{1-1}	12	2160
$L_{1-1}T_{1-1}$	6	360	K	5	5184
$L_{11}L_{2-1}T_{1-1}$	6	1440	$P_{12}M_1$	4	3240
$L_{11}L_{21}T_{1-1}$	6	720	M_1M_2	2	270
$L_{1-1}L_{2-1}T_{1-1}$	6	720	$P_{12}L_{1-1}T_{1-1}$	6	2160

that type. Thus, L_{11} is not conjugate with its square L_{1-1}; $L_{11}L_{21}$ is conjugate with its square. A_{-1} is transformed into A_1^{-1} by $T_{2-1}L'_{21}$. Since $A_1^3 = L'_{1-1}$ and $A_1^6 = L'_{11}$ are not conjugate, A_1 is not conjugate with either A_1^2 or A_1^5, 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_2L_{11} is conjugate with its seventh power $M_2^3L_{11}$, so that the fifth and eleventh powers are conjugate. The latter is $M_2^3L_{1-1}$ and is consequently conjugate with M_2L_{1-1} and hence (by the above table) not conjugate with M_2L_{11} itself. Hence M_2L_{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.

Type of generator.	Conjugate cyclic groups.	Generator.	Groups.
L_{11}	40	A_1	960
$L_{11}L_{21}$	120	M_2	270
$L_{1-1}L_{21}$	240	M_2L_{11}	1080
T_{1-1}	45	K	1296
$L_{11}T_{1-1}$	360	$P_{12}M_1$	1620
$L_{11}L_{2-1}T_{1-1}$	720	M_1M_2	270
$L_{11}L_{21}T_{1-1}$	720	$P_{12}L_{1-1}T_{1-1}$	1080

THE UNIVERSITY OF CHICAGO, *January* 3, 1901.