The necessary condition that (1) and (2) have two integrals in common is that, in the following matrix obtained by successive differentiation,

\[
\begin{bmatrix}
\alpha_0 & \alpha'_0 + \alpha_1 & \alpha'_1 + \alpha_2 & \alpha'_2 + \alpha_3 & \alpha'_3 + \alpha_4 & \alpha'_4 \\
0 & \alpha_0 & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\
0 & \beta_0 + 2\beta'_0 + \beta_1 & \beta'_1 + 2\beta'_2 + \beta_2 & \beta'_2 + 2\beta'_3 + \beta_3 & \beta'_3 \\
0 & \beta_0 & \beta'_0 + \beta_1 & \beta'_1 + \beta_2 & \beta'_2 + \beta_3 & \beta'_3 \\
0 & 0 & \beta_0 & \beta_1 & \beta_2 & \beta_3
\end{bmatrix}
\]

the determinant consisting of the first five columns, and also that consisting of the first four columns and the sixth, shall vanish identically.

COLUMBIA UNIVERSITY.

F. N. COLE.

TWO SYSTEMS OF SUBGROUPS OF THE QUATERNARY ABELIAN GROUP IN A GENERAL GALOIS FIELD.

BY PROFESSOR L. E. DICKSON.

(Read before the American Mathematical Society, August 31, 1903.)

1. CONSIDER first the group \( G_{\omega} \) composed of the

\[
\omega = p^{2n}(p^{2n} - 1)(p^n - 1)
\]

operators of the homogeneous quaternion abelian group in the \( GF[p^n] \), \( p > 2 \), which multiply the variable \( \eta \) by a constant. Those of its operators which leave \( \xi_1 \) and \( \eta_1 \) unaltered are given the notation

\[
\begin{bmatrix}
a & \gamma \\
\beta & \delta
\end{bmatrix} : \xi'_2 = a\xi_2 + \gamma\eta_2, \quad \eta'_2 = \beta\xi_2 + \delta\eta_2, \quad (a\delta - \beta\gamma = 1).
\]

Certain other operators of \( G_{\omega} \) are given the notation

\[
[k, a, c, \gamma] =
\begin{bmatrix}
1 & k & a & c \\
0 & 1 & 0 & 0 \\
0 & c - \gamma a & 1 & \gamma \\
0 & -a & 0 & 1
\end{bmatrix}
\]
They form a group of order $p^3n$, as shown elsewhere by the writer.* The general operator of $G_w$ may now be exhibited as either of the products

$$T_{1,1}[k, a, c, 0] \left[\begin{array}{c|c} a & \gamma \\ \hline \beta & \delta \end{array}\right], \quad T_{1,1}[k, -\beta c + \delta a, ac - \gamma a, 0].$$

Now $T_{1,1}T_{2,1}$ transforms $[k, a, c, 7]$ into $[kt^2, \alpha t\sigma^{-1}, \sigma t\sigma, \gamma t\sigma^2]$. The operators $[k', a', c', 0]$ are seen to form a group $G_{p^3n}$. The $T_{1,1}$ extend the latter to $G_{p^3n}$. Hence the groups $G_{p^3n}$ and $G_{p^3n}^{(p^n - 1)}$ are self-conjugate under $G_w$.

The quotient group $G_w/G_{p^3n}^{(p^n - 1)}$ may be taken concretely as the group $\Gamma^{p^n(p^n - 1)}$ of the binary substitutions $[\sigma, \gamma]$. To a subgroup of order $\mu$ of the latter corresponds a subgroup of order $\mu p^3n(p^n - 1)$ of $G_w$. We obtain subgroups of order $d\mu p^3n$ of $G_w$, where $d$ is any divisor of $p^n - 1$, by restricting $T$ in $T_{1,1}$ to marks which define a cyclic subgroup of order $d$ of the cyclic group of all the $p^n - 1$ operators $T_{1,1}$. If the subgroup of order $\mu$ is self-conjugate under $\Gamma$, the corresponding subgroup is self-conjugate under $G_w$. This follows from the theory of isomorphism, or directly, since $[k, a, c, 0]$ transforms $[\sigma, \gamma]$, into

$$[\gamma a^2 - \beta c^2 + \delta ac - aac, \beta c + aa - \alpha, \gamma a + \delta c - c, 0] \left[\begin{array}{c|c} a & \gamma \\ \hline \beta & \delta \end{array}\right].$$

2. As the first example, let $p^n = 3$. Then $\Gamma$ is of order 24. Now $\Gamma_{24}$ contains a self-conjugate $\Gamma_{24}$, a self-conjugate $\Gamma_{8}$, one set of 3 conjugate cyclic $\Gamma_{9}$, one set of 4 conjugate cyclic $\Gamma_{9}$, one set of 4 conjugate cyclic $\Gamma_{9}$, but no further subgroups.|† Hence $G_w$ contains subgroups $G_{54n}$, $\mu = 1, 2, 3, 4, 6, 8$. Within $G_w$, $G_{54}$, $G_{54.2}$ and $G_{54.8}$ are, therefore, self-conjugate, while $G_{54.3}$ and $G_{54.6}$ are self-conjugate only under $G_{54.6}$ and $G_{54.4}$ only under $G_{54.8}$.

3. Let next $p^n = 5$. Denote the general substitution of $\Gamma_{120}$ by

$$S = \left[\begin{array}{c|c} a & \gamma \\ \hline \beta & \delta \end{array}\right], \quad a\delta - \beta \gamma \equiv 1 \pmod{5}. \quad (1)$$

If the characteristic determinant $D(k) \equiv k^2 - (a + \delta)k + 1$ of $S$ is irreducible modulo 5, $S$ is conjugate within $\Gamma_{120}$ with one of the canonical forms ‡

‡ Dickson, Transactions, vol. 2 (1901), p. 117. Instead of $S_l = \left[\begin{array}{c} 0 \\ -1 \end{array}\right]$, we employ its transform $S_l$ by $\left[\begin{array}{c} 1 \\ -1 \end{array}\right]$. In the $GF(5^5)$, $S_l$ and $S_0$ may both be given ultimate canonical forms of the type $\left[\begin{array}{c} 0 \\ 1 \end{array}\right]$. $k^3 = 1.
The only substitutions of $\Gamma_{120}$ commutative with $S_9$ are its powers

\[
S_3 = \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix}, \quad S_6 = \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix}.
\]

(2)

The only ones commutative with $S_3$ are (3). If $D(k)$ is reducible modulo 5, $S$ is conjugate within $\Gamma_{120}$ with one of the canonical forms

\[
S = \begin{bmatrix} a & \gamma \\ -\gamma & a + \gamma \end{bmatrix}, \quad (a^2 + a\gamma + \gamma^2 \equiv 1).
\]

(3)

Indeed, $S_3$ is commutative only with its powers, and

\[
S_9 = \begin{bmatrix} \pm 1 & 0 \\ \pm t & \pm 1 \end{bmatrix} \text{ only with } \begin{bmatrix} a & 0 \\ \beta & a \end{bmatrix}, \quad (a^2 \equiv 1).
\]

4

\[
S_2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \quad S_4 = \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix}, \quad S_5 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix},
\]

\[
S_{10} = \begin{bmatrix} -1 & 0 \\ -1 & -1 \end{bmatrix}, \quad S'_{10} = \begin{bmatrix} -1 & 0 \\ -2 & -1 \end{bmatrix}, \quad S'_5 = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}.
\]

(4)

Theorem: The group $\Gamma_{120}$ of all binary substitutions of determinant unity modulo 5 contains, in addition to the identity and the self-conjugate substitution $S_9$, one set of 20 conjugate substitutions of period 3, one set of 20 of period 6, one set of 30 of period 4, two sets each of 12 of period 5, and two sets each of 12 of period 10.

The only substitutions of $\Gamma_{120}$ which transform $S_9$ into its inverse are

\[
S_9^2 = S'_9, \quad S_9^6 = S_9, \quad S_9^7 = S'_9, \quad S_9^{10} = S'_9,
\]

(5)

Now $S_4$ is commutative only with its powers, and

\[
S_4 = \begin{bmatrix} \alpha & \gamma \\ \alpha + \gamma & -\alpha \end{bmatrix}, \quad (-\alpha^2 - \alpha\gamma - \gamma^2 \equiv 1),
\]

(6)

Denote by $\Gamma_{120}'$ the group formed by the substitutions (3) and (6). Denote by $\Gamma_{20}'$ the group formed by the powers of $S_9$ and the 10 substitutions $[\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}]$ of period 4 which transform $S_{10}$ into its inverse. Denote by $\Gamma_4'$ the group of the powers of $S_4$ and the substitutions $[\begin{smallmatrix} 0 & \alpha \\ -\alpha & 0 \end{smallmatrix}]$ of period 4 which
transform $S_i$ into its inverse. Since $\Gamma_8$ contains 3 groups of order 4 conjugate within $\Gamma_{120}$, it is self-conjugate under a subgroup $\Gamma_{24}$. Finally, denote by $C_i$ the cyclic group generated by $S_i$.

We proceed to show that every subgroup of $\Gamma_{120}$ is conjugate with one of the preceding. This has already been shown for the cyclic groups, and is evident for groups of orders 8, 20 and 40. A subgroup of order 10 is necessarily cyclic. A subgroup of order 12 contains 3 conjugate cyclic groups of order 4 and hence a single cyclic group of order 3, so that it is conjugate with $\Gamma_{12}$. A group of order 15 is cyclic and hence cannot be a subgroup. A subgroup of order 24 has 1 or 3 conjugate groups of order 8; if 1, it is conjugate with $\Gamma_{24}$; if 3, the group transforming each into itself is a self-conjugate subgroup of order 4 of the group of order 24, contrary to the above. There is no subgroup of order 30, since it would contain 6 cyclic $G_5$, 10 cyclic $G_3$, and 15 $G_{2\times}$. There is no subgroup of order 60, since it would contain 6 cyclic $G_5$, 10 cyclic $G_3$, and 15 cyclic $G_{2\times}$.

**Theorem.** The subgroups of $\Gamma_{120}$ aside from itself and identity, are conjugate with $C_2$, $C_3$, $C_4$, $C_5$, $C_6$, $C_{10}$, $C_{12}$, $C_{20}$, $C_{24}$, $\Gamma_{24}$. Within $\Gamma_{120}$ the largest groups in which these are self-conjugate are $\Gamma_{120}$, $\Gamma_{12}$, $\Gamma_{20}$, $\Gamma_{12}$, $\Gamma_{24}$, $\Gamma_{20}$, $\Gamma_{20}$, $\Gamma_{20}$, $\Gamma_{20}$, $\Gamma_{20}$, respectively.

We may derive from §1 the following subgroups of $G_w$:

$$G_{50\mu}(\mu = 1, 2, 3, 4, 5, 6, 8, 10, 12, 20, 24).$$

Within $G_w$, $G_{50\mu}$ and $G_{50\mu.2}$ are self-conjugate, while the others are self-conjugate only under the respective groups $G_{50\lambda}(\lambda = 12, 8, 20, 12, 24, 20, 12, 20, 24)$.

4. Consider next the group $H_w$ of homogeneous quaternary abelian substitutions † in the $GF[p^n], p > 2$, subject to the condition that two variables $\eta_1$ and $\eta_2$ are replaced by linear functions of themselves

$$\begin{bmatrix}
\alpha_{11} & \gamma_{11} & \alpha_{12} & \gamma_{12} \\
0 & \delta_{11} & 0 & \delta_{12} \\
\alpha_{21} & \gamma_{21} & \alpha_{22} & \gamma_{22} \\
0 & \delta_{21} & 0 & \delta_{22}
\end{bmatrix}.$$

† By way of check, we note that the simple $G_{50}=\Gamma_{120}/C_5$ has subgroups only of the orders 2, 3, 4, 5, 6, 10 and 12, those of orders 6 and 10 being dihedral.

† Given by formula (19), without the sign $\pm$, page 380, Transactions, vol. 4 (1903).
If each \( y_j = 0 \), (7) becomes, in view of the abelian conditions,

\[
\begin{bmatrix}
\frac{\delta_{22}}{\Delta} & 0 & -\frac{\delta_{21}}{\Delta} & 0 \\
0 & \delta_{11} & 0 & \delta_{12} \\
-\frac{\delta_{12}}{\Delta} & 0 & \frac{\delta_{11}}{\Delta} & 0 \\
0 & \delta_{21} & 0 & \delta_{22}
\end{bmatrix}, \quad (\Delta = \delta_{11} \delta_{22} - \delta_{12} \delta_{21}).
\]

The substitutions (8) form a group \( H_p \) of order

\[ \rho = (p^{2n} - 1) (p^{2n} - p^n), \]

simply isomorphic with the group of all binary substitutions (of general determinant) in the \( GF[p^n] \). Giving therefore to (8) the notation \( (\delta_1, \delta_2) \), we find that \( (\delta_1, \delta_2) \) is identical with (7) if

\[
\gamma_{11} = k \delta_{11} + c \delta_{21}, \quad \gamma_{21} = c \delta_{11} + \gamma \delta_{21},
\]
\[
\gamma_{12} = k \delta_{12} + c \delta_{22}, \quad \gamma_{22} = c \delta_{12} + \gamma \delta_{22}.
\]

Inversely, every operator (7) may be obtained as such a product. Indeed, the four last conditions may be written

\[
k \Delta = \begin{vmatrix} \gamma_{11} & \delta_{21} \\ \gamma_{12} & \delta_{22} \end{vmatrix}, \quad c \Delta = \begin{vmatrix} \delta_{11} & \gamma_{11} \\ \delta_{12} & \gamma_{12} \end{vmatrix}, \quad c \Delta = \begin{vmatrix} \gamma_{21} & \delta_{21} \\ \gamma_{22} & \delta_{22} \end{vmatrix}, \quad \gamma \Delta = \begin{vmatrix} \delta_{11} & \gamma_{21} \\ \delta_{12} & \gamma_{22} \end{vmatrix}.
\]

These determine \( k \), \( c \) and \( \gamma \) uniquely, the two values for \( c \) being equal in view of the abelian relation \( \gamma \Delta = \gamma (\Delta) \gamma^{-1} \). By bringing the \( \alpha_{ij} \) to the foreground in place of the \( \delta_{ij} \), we may reverse the order of the factors and give (7) the form

\[
[k', 0, c', \gamma'] \begin{pmatrix} \delta_{11} & \delta_{12} \\ \delta_{21} & \delta_{22} \end{pmatrix}, \quad \gamma_{11} = k' \alpha_{11} + c' \alpha_{12}, \text{ etc.}
\]

Hence the commutative * group \( K_p^{\alpha} \) of the substitutions \( [k, 0, c, \gamma] \) is self-conjugate under \( H_p \). The quotient group may be taken concretely as \( H_p^{\alpha} \). To a subgroup \( H_r \) of \( H_p^{\alpha} \) corre-
sponds a subgroup $H_{p^n}$ of $H_w$. For the cases $p^n = 3$ and $p^n = 5$, we may apply at once the results of §§ 2 and 3.

5. The results thus far obtained may be applied to the simple group given as the quotient group of the homogeneous abelian group by the group composed of the identity and the substitution $C$ which changes the sign of each variable. From $G^*_w$ and $H_w$, we obtain $G'_{3w}$ and $H'_{3w}$, respectively. For $p^n = 3$, $G'_{3w}$, namely $G'_{6w}$, has subgroups $G'_{27w}$, $\mu = 1, 2, 3, 4, 6, 8$ (§ 2). For $p^n = 5$, $G'_{50000}$ has subgroups $G'_{20000}$, $\mu = 1, 2, 3, 4, 5, 6, 8, 10, 12, 20, 24$ (§ 3).

Let $H_p$ correspond to $H_{3p'}$. For $p^n = 3$, $H'_{34}$ is simply isomorphic with the group of all linear fractional substitutions (§ 2) modulo 3. But the latter is simply isomorphic with the symmetric group $G_{24}$ on four letters. The latter has the following non-conjugate subgroups, in addition to identity, itself, and the alternating group $G_{12}$:

$G_2 = \{I, (13)\}$; $G_3 = \{I, (123), (132)\}$;
$G_6 = \{I, (123), (132), (12), (13), (23)\}$;
$G'_2 = \{I, (13)(24)\}$; $G_4 = \{I, (13), (24), (13)(24)\}$;
$G'_4 = \{I, (12)(34), (13)(24), (14)(23)\}$;
$G''_4 = \{I, (1234), (13)(24), (1432)\}$;
$G_8 = \{I, (1234), (1432), (13)(24), (12)(34), (14)(23), (13)(24)\}$;

every subgroup being conjugate within $G_{24}$ with one of the foregoing. Then $G_3$ is self-conjugate only under $G_4$, $G_3$ only under $G_6'$, $G_6$ only under $G_3'$, $G'_2$ only under $G_3$, $G_4$ only under $G'_3$, $G'_4$ only under $G_{24}$, $G''_4$ only under $G_8$, $G_8$ only under $G_3$, $G_{12}$ only under $G_{24}$.

In passing to the subgroups of $H'_{24}$, it is convenient to make the letters 1, 2, 3, 4 correspond to the respective marks 1, $-1$, 0, $\infty$. Then

$(12) \sim z' = -z$, $(13) \sim z' = -z + 1$, $(34) \sim z' = 1/z$,
$(23) \sim z' = -z - 1$, $(24) \sim z' = -z/(z + 1)$, $(14) \sim z/(z - 1)$.

* That the chosen groups, and not some of their conjugates, appear as the largest groups in which the types are self-conjugate is a result of the notation used.
THEOREM. Every subgroup of \( H'_{24} \) is conjugate with \( H'_{24}, H_{12} \) (group of all of determinant + 1), identity, or one of the following:

\[
\begin{align*}
H_2 &= \left\{ I, \left( \begin{array}{cc} -11 \\ 01 \end{array} \right) \right\}; \\
H_3 &= \left\{ I, \left( \begin{array}{cc} 18 \\ 01 \end{array} \right) \right\}; \\
H_4 &= \left\{ I, \left( \begin{array}{cc} -11 \\ 10 \end{array} \right) \right\}; \\
H_5 &= \left\{ I, \left( \begin{array}{cc} +16 \\ 01 \end{array} \right) \right\}; \\
H_6 &= \left\{ I, \left( \begin{array}{cc} 11 \\ 10 \end{array} \right) \right\}; \\
H_7 &= \left\{ I, \left( \begin{array}{cc} 0-1 \\ 10 \end{array} \right), \left( \frac{1}{1-1} \right) \right\}; \\
H_8 &= \left\{ I, \left( \begin{array}{cc} -11 \\ 01 \end{array} \right), \left( \frac{1}{1-1} \right) \right\}; \\
H_9 &= \left\{ I, \left( \begin{array}{cc} 0-1 \\ 10 \end{array} \right), \left( \frac{1}{1-1} \right) \right\}; \\
H_10 &= \left\{ I, \left( \begin{array}{cc} -11 \\ 01 \end{array} \right), \left( \frac{1}{1-1} \right) \right\}.
\end{align*}
\]

Moreover, \( H_2 \) is self-conjugate only under \( H'_{12}; \) \( H_8 \) only under \( H'_4, H'_5, H'_6, \) and \( H''_4 \) are self-conjugate only under \( H'_8; \) \( H_6 \) and \( H_8 \) only under themselves; \( H'_4 \) and \( H''_6 \) only under \( H'_{24}. \)

To the preceding subgroups \( H_{12}, H_3, H_5, \ldots, H_9 \) of \( H'_{24} \) correspond subgroups \( H_{27,12}, H_{27,13}, H_{27,21} \), \( H_{27,23}, H_{27,53}, H_{27,61}, H_{27,63}, H_{27,41}, H_{27,43}, H_{27,47}, \) \( H_{27,49}, H_{27,51} \) respectively, of \( H'_{24} \). Within the latter, they are self-conjugate only under \( H_{6483}, H_{27,41}, H_{27,43}, H_{27,61}, H_{27,63} \), \( H_{27,53}, H_{27,63}, H_{27,83} \) respectively.

THE UNIVERSITY OF CHICAGO,
July, 1903.