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

$$\left\{\begin{matrix} \alpha_0 & \alpha_0' + \alpha_1 & \alpha_1' + \alpha_2 & \alpha_2' + \alpha_3 & \alpha_0' + \alpha_4 & \alpha_4' \\ 0 & \alpha_0 & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \beta_0 & 2\beta_0' + \beta_1 & \beta_0'' + 2\beta_1' + \beta_2 & \beta_1'' + 2\beta_2' + \beta_3 & \beta_2'' + 2\beta_3' & \beta_3'' \\ 0 & \beta_0 & \beta_0' + \beta_1 & \beta_1' + \beta_2 & \beta_2' + \beta_3 & \beta_3' \\ 0 & 0 & \beta_0 & \beta_1 & \beta_2 & \beta_3 \end{matrix}\right\},$$

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

F. N. COLE.

COLUMBIA UNIVERSITY.

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_ω composed of the

$$\omega = p^{4n}(p^{2n} - 1)(p^n - 1)$$

operators of the homogeneous quaternary abelian group in the $GF[p^n]$, $p > 2$, which multiply the variable η_1 by a constant. Those of its operators which leave ξ_1 and η_1 unaltered are given the notation

$$\begin{bmatrix} \alpha & \gamma \\ \beta & \delta \end{bmatrix}: \quad \begin{matrix} \xi_2' = \alpha\xi_2 + \gamma\eta_2, \\ \eta_2' = \beta\xi_2 + \delta\eta_2, \end{matrix} \qquad (\alpha\delta - \beta\gamma = 1).$$

Certain other operators of G_ω are given the notation

$$[k, a, c, \gamma] = \left\{\begin{matrix} 1 & k & a & c \\ 0 & 1 & 0 & 0 \\ 0 & c - \gamma a & 1 & \gamma \\ 0 & -a & 0 & 1 \end{matrix}\right\}$$

They form a group of order p^{4n}, as shown elsewhere by the writer.* The general operator of G_ω may now be exhibited as either of the products

$$T_{1,\tau}[k,\ a,\ c,\ 0]\begin{bmatrix}\alpha & \gamma\\ \beta & \delta\end{bmatrix},\quad T_{1,\tau}\begin{bmatrix}\alpha & \gamma\\ \beta & \delta\end{bmatrix}[k,\ -\beta c+\delta a,\ \alpha c-\gamma a,\ 0].$$

Now $T_{1,\tau}T_{2,\sigma}$ transforms $[k,\ a,\ c,\ \gamma]$ into $[k\tau^2,\ a\tau\sigma^{-1},\ c\tau\sigma,\ \gamma\sigma^2]$. The operators $[k,\ a,\ c,\ 0]$ are seen to form a group $G_{p^{3n}}$. The $T_{1,\tau}$ extend the latter to $G_{p^{3n}(p^n-1)}$. *Hence the groups* $G_{p^{3n}}$ *and* $G_{p^{3n}(p^n-1)}$ *are self-conjugate under* G_ω.

The quotient group $G_\omega / G_{p^{3n}(p^n-1)}$ may be taken concretely as the group $\Gamma_{p^n(p^{2n}-1)}$ of the binary substitutions $\left[\begin{smallmatrix}\alpha & \gamma\\ \beta & \delta\end{smallmatrix}\right]$. To a subgroup of order μ of the latter corresponds a subgroup of order $\mu p^{3n}(p^n-1)$ of G_ω. We obtain subgroups of order $d\mu p^{3n}$ of G_ω, where d is any divisor of p^n-1, by restricting τ in $T_{1,\tau}$ to marks which define a cyclic subgroup of order d of the cyclic group of all the p^n-1 operators $T_{1,\tau}$. If the subgroup of order μ is self-conjugate under Γ, the corresponding subgroup is self-conjugate under G_ω. This follows from the theory of isomorphism, or directly, since $[k,\ a,\ c,\ 0]$ transforms $\left[\begin{smallmatrix}\alpha & \gamma\\ \beta & \delta\end{smallmatrix}\right]$ into

$$[\gamma a^2-\beta c^2+\delta ac-\alpha ac,\ \beta c+\alpha a-a,\ \gamma a+\delta c-c,\ 0]\begin{bmatrix}\alpha & \gamma\\ \beta & \delta\end{bmatrix}.$$

2. As the first example, let $p^n=3$. Then Γ is of order 24. Now Γ_{24} contains a self-conjugate Γ_2, a self-conjugate Γ_8, one set of 3 conjugate cyclic Γ_4, one set of 4 conjugate Γ_3, one set of 4 conjugate cyclic Γ_6, but no further subgroups.† Hence G_ω contains subgroups $G_{54\mu}$, $\mu=1,\ 2,\ 3,\ 4,\ 6,\ 8$. Within G_ω, G_{54}, $G_{54\cdot2}$ and $G_{54\cdot8}$ are, therefore, self-conjugate, while $G_{54\cdot3}$ and $G_{54\cdot6}$ are self-conjugate only under $G_{54\cdot6}$, and $G_{54\cdot4}$ only under $G_{54\cdot8}$.

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

$$(1)\qquad S=\begin{bmatrix}\alpha & \gamma\\ \beta & \delta\end{bmatrix},\quad \alpha\delta-\beta\gamma\equiv 1 \pmod 5.$$

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

* *Transactions*, vol. 4 (1903), pp. 371–386.

† Dickson, *Annals of Mathematics*, vol. 5 (1903–4).

‡ Dickson, *Transactions*, vol. 2 (1901), p. 117. Instead of $S_3'=\left[\begin{smallmatrix}0 & 1\\ -1 & -1\end{smallmatrix}\right]$, we employ its transform S_3 by $\left[\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right]$. In the $GF[5^2]$, S_3 and S_6 may both be given ultimate canonical forms of the type $\left[\begin{smallmatrix}k & 0\\ 0 & k^{-1}\end{smallmatrix}\right]$, $k^6=1$.

$$(2)\qquad S_3=\begin{bmatrix}-1 & 1\\ -1 & 0\end{bmatrix},\quad S_6=\begin{bmatrix}0 & 1\\ -1 & 1\end{bmatrix}.$$

The only substitutions of Γ_{120} commutative with S_6 are its powers

$$(3)\qquad \begin{bmatrix}\alpha & \gamma\\ -\gamma & \alpha+\gamma\end{bmatrix},\qquad (\alpha^2+\alpha\gamma+\gamma^2\equiv 1).$$

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

$$(4)\qquad \begin{array}{l} I,\quad S_2=\begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix},\quad S_4=\begin{bmatrix}2 & 0\\ 0 & 3\end{bmatrix},\quad S_5=\begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix},\\ S_{10}=\begin{bmatrix}-1 & 0\\ -1 & -1\end{bmatrix},\quad S_{10}'=\begin{bmatrix}-1 & 0\\ -2 & -1\end{bmatrix},\quad S_5'=\begin{bmatrix}1 & 0\\ 2 & 1\end{bmatrix}.\end{array}$$

Indeed, S_{10} is conjugate with $\left[\begin{smallmatrix}-1 & 0\\ -t & -1\end{smallmatrix}\right]$ within Γ_{120} if and only if t is a quadratic residue of 5. Further,

$$(5)\quad S_{10}^2=S_5',\quad S_{10}^5=S_2,\quad S_{10}^6=S_5,\quad S_{10}^7=S_{10}',\quad S_{10}'^6=S_5'.$$

Now S_4 is commutative only with its powers, and

$$\begin{bmatrix}\pm 1 & 0\\ \pm t & \pm 1\end{bmatrix}\text{ only with }\begin{bmatrix}\alpha & 0\\ \beta & \alpha\end{bmatrix},\qquad (\alpha^2\equiv 1).$$

THEOREM: *The group Γ_{120} of all binary substitutions of determinant unity modulo 5 contains, in addition to the identity and the self-conjugate substitution S_2, 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 Γ_{120} which transform S_6 into its inverse are

$$(6)\qquad \begin{bmatrix}\alpha & \gamma\\ \alpha+\gamma & -\alpha\end{bmatrix},\qquad (-\alpha^2-\alpha\gamma-\gamma^2\equiv 1),$$

each of period 4. Denote by Γ_{12} the group formed by the substitutions (3) and (6). Denote by Γ_{20} the group formed by the powers of S_{10} and the 10 substitutions $\left[\begin{smallmatrix}\pm 2 & 0\\ \beta & \pm 3\end{smallmatrix}\right]$ of period 4 which transform S_{10} into its inverse. Denote by Γ_8 the group of the powers of S_4 and the substitutions $\left[\begin{smallmatrix}0 & \gamma\\ -\gamma^{-1} & 0\end{smallmatrix}\right]$ of period 4 which transform S_4 into its inverse. Since Γ_8 contains 3 groups of order 4 conjugate within Γ_{120}, it is self-conjugate under a subgroup Γ_{24}. Finally, denote by C_i the cyclic group generated by S_i.

We proceed to show that every subgroup of Γ_{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 Γ_{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 Γ_{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. There is no subgroup of order 60, since it would contain 6 cyclic G_5, 10 cyclic G_3, and 15 cyclic G_4.

THEOREM.* *The subgroups of Γ_{120}, aside from itself and identity, are conjugate with C_2, C_3, C_4, C_5, C_6, Γ_8, C_{10}, Γ_{12}, Γ_{20}, Γ_{24}. Within Γ_{120}, the largest groups in which these are self conjugate are Γ_{120}, Γ_{12}, Γ_8, Γ_{20}, Γ_{12}, Γ_{24}, Γ_{20}, Γ_{12}, Γ_{20}, Γ_{24}, respectively.*

We may derive from §1 the following subgroups of G_ω:

$$G_{500\mu} \quad (\mu = 1, 2, 3, 4, 5, 6, 8, 10, 12, 20, 24).$$

Within G_ω, G_{500} and $G_{500\cdot 2}$ are self-conjugate, while the others are self-conjugate only under the respective groups

$$G_{500\lambda} \quad (\lambda = 12, 8, 20, 12, 24, 20, 12, 20, 24).$$

4. Consider next the group H_ω of homogeneous quaternary abelian substitutions † in the $GF[p^n]$, $p > 2$, subject to the condition that two variables η_1 and η_2 are replaced by linear functions of themselves

$$(7) \qquad \begin{vmatrix} \alpha_{11} & \gamma_{11} & \alpha_{12} & \gamma_{12} \\ 0 & \delta_{11} & 0 & \delta_{12} \\ \alpha_{21} & \gamma_{21} & \alpha_{22} & \gamma_{22} \\ 0 & \delta_{21} & 0 & \delta_{22} \end{vmatrix}.$$

* By way of check, we note that the simple $G_{60} = \Gamma_{120}/C_2$ 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 $\gamma_{ij} = 0$, (7) becomes, in view of the abelian conditions,

$$(8) \qquad \left\{\begin{matrix} \delta_{22}/\Delta & 0 & -\delta_{21}/\Delta & 0 \\ 0 & \delta_{11} & 0 & \delta_{12} \\ -\delta_{12}/\Delta & 0 & \delta_{11}/\Delta & 0 \\ 0 & \delta_{21} & 0 & \delta_{22} \end{matrix}\right\}, \quad (\Delta = \delta_{11}\delta_{22} - \delta_{12}\delta_{21}).$$

The substitutions (8) form a group H_ρ 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 $\left(\begin{smallmatrix}\delta_{11} & \delta_{12} \\ \delta_{21} & \delta_{22}\end{smallmatrix}\right)$, we find that $\left(\begin{smallmatrix}\delta_{11} & \delta_{12} \\ \delta_{21} & \delta_{22}\end{smallmatrix}\right)[k, 0, c, \gamma]$ is identical with (7) if

$$\gamma_{11} = k\delta_{11} + c\delta_{21}, \qquad \gamma_{21} = c\delta_{11} + \gamma\delta_{21},$$
$$\gamma_{12} = k\delta_{12} + c\delta_{22}, \qquad \gamma_{22} = c\delta_{12} + \gamma\delta_{22}.$$

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 γ uniquely, the two values for c being equal in view of the abelian relation (C_{23} in the notation of Linear Groups, page 91)

$$\begin{vmatrix} \gamma_{11} & \gamma_{12} \\ \delta_{11} & \delta_{12} \end{vmatrix} + \begin{vmatrix} \gamma_{21} & \gamma_{22} \\ \delta_{21} & \delta_{22} \end{vmatrix} = 0.$$

By bringing the α_{ij} to the foreground in place of the δ_{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 $K_{p^{3n}}$ of the substitutions $[k, 0, c, \gamma]$ is self-conjugate under H_ω. The quotient group may be taken concretely as H_ρ. To a subgroup H_r of H_ρ corre-

* *Transactions*, vol. 4 (1903), formula (12), p. 377.

sponds a subgroup $H_{rp^{3n}}$ of H_ω. 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_ω and H_ω, we obtain $G'_{\frac{1}{2}\omega}$ and $H'_{\frac{1}{2}\omega}$, respectively. For $p^n = 3$, $G'_{\frac{1}{2}\omega}$, namely G'_{648}, has subgroups $G'_{27\mu}$, $\mu = 1, 2, 3, 4, 6, 8$ (§ 2). For $p^n = 5$, G'_{30000} has subgroups $G'_{250\mu}$, $\mu = 1, 2, 3, 4, 5, 6, 8, 10, 12, 20, 24$ (§ 3).

Let H_ρ correspond to $H'_{\frac{1}{2}\rho}$. For $p^n = 3$, H'_{24} is simply isomorphic with the group of all linear fractional substitutions $\left(\frac{\delta_{11}\delta_{12}}{\delta_{21}\delta_{22}}\right)$ 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}:

$$G_2 = \{I,\ (13)\};\quad G_3 = \{I,\ (123),\ (132)\};$$

$$G_6 = \{I,\ (123),\ (132),\ (12),\ (13),\ (23)\};$$

$$G'_2 = \{I,\ (13)(24)\};\quad G_4 = \{I,\ (13),\ (24),\ (13)(24)\};$$

$$G'_4 = \{I,\ (12)(34),\ (13)(24),\ (14)(23)\};$$

$$G''_4 = \{I,\ (1234),\ (13)(24),\ (1432)\};$$

$$G_8 = \{I,\ (1234),\ (1432),\ (13)(24),\ (12)(34),\ (14)(23),\ (13)(24);$$

every subgroup being conjugate within G_{24} with one of the foregoing. Then* G_2 is self-conjugate only under G_4, G_3 only under G_6, G_6 only under G_6, G'_2 only under G_8, G_4 only under G_8, G'_4 only under G_{24}, G''_4 only under G_8, G_8 only under G_8, 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, ∞. Then

$$(12) \sim z' = -z, \qquad (13) \sim z' = -z + 1, \qquad (34) \sim z' = 1/z,$$

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

* 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:*

$$H_2=\left\{I,\begin{pmatrix}-1&1\\0&1\end{pmatrix}\right\};\quad H_3=\left\{\begin{pmatrix}1&\delta\\0&1\end{pmatrix}\right\};\quad H_6=\left\{\begin{pmatrix}\pm1&\delta\\0&1\end{pmatrix}\right\};$$

$$H'_2=\left\{I,\begin{pmatrix}-1&1\\1&1\end{pmatrix}\right\};\quad H'_4=\left\{I,\begin{pmatrix}-1&1\\0&1\end{pmatrix},\begin{pmatrix}-1&1\\0&1\end{pmatrix},\begin{pmatrix}-1&1\\1&1\end{pmatrix}\right\};$$

$$H_4=\left\{I,\begin{pmatrix}0&-1\\1&0\end{pmatrix},\begin{pmatrix}\pm1&1\\1&\mp1\end{pmatrix}\right\};$$

$$H''_4=\left\{I,\begin{pmatrix}1&1\\1&0\end{pmatrix},\begin{pmatrix}0&1\\1&-1\end{pmatrix},\begin{pmatrix}-1&1\\1&1\end{pmatrix}\right\};$$

$$H_8=\left\{I,\begin{pmatrix}0&-1\\1&0\end{pmatrix},\begin{pmatrix}1&1\\1&0\end{pmatrix},\begin{pmatrix}-1&1\\0&1\end{pmatrix},\begin{pmatrix}-1&0\\1&1\end{pmatrix},\right.$$
$$\left.\begin{pmatrix}0&1\\1&-1\end{pmatrix},\begin{pmatrix}\pm1&1\\1&\mp1\end{pmatrix}\right\}.$$

Moreover, H_2 *is self-conjugate only under* H'_4; H_3 *only under* H_6; H'_2, H'_4 *and* H''_4 *are self-conjugate only under* H_8; H_6 *and* H_8 *only under themselves;* H_4 *and* H_{12} *only under* H_{24}.

To the preceding subgroups H_{12}, H_2, H_3, $\cdots$, H_8 of H'_{24} correspond subgroups $H_{27\cdot12}$, $H_{27\cdot2}$, $H_{27\cdot3}$, $H_{27\cdot6}$, $H'_{27\cdot2}$, $H'_{27\cdot4}$, $H_{27\cdot4}$, $H''_{27\cdot4}$, $H_{27\cdot8}$, respectively, of $H'_{\frac{1}{2}\omega}\equiv H'_{648}$. Within the latter, they are self-conjugate only under H'_{648}, $H'_{27\cdot4}$, $H_{27\cdot6}$, $H_{27\cdot6}$, $H_{27\cdot8}$, $H_{27\cdot8}$, H'_{648}, $H_{27\cdot8}$, $H_{27\cdot8}$, respectively.

THE UNIVERSITY OF CHICAGO,
July, 1903.