ON THE SUBGROUPS OF ORDER A POWER OF p IN THE QUATERNARY ABELIAN GROUP IN THE GALOIS FIELD OF ORDER p^n*

BY

LEONARD EUGENE DICKSON

1. The problem of the p-section of the periods of hyperelliptic functions of four periods leads to the quaternary abelian group modulo p, where p is supposed to be an odd prime number. The equation for this p-section has two essentially distinct resolvents of degree $(p^4-1)/(p-1)$, as shown by JORDAN† and as follows incidentally in the present paper, §§ 2, 4 (Corollary), 16.

For the case $p=3$, the group arises in the problem of the 27 lines on a general cubic surface, as well as in the reduction of a binary sextic to CAYLEY's canonican form T^2-U^3.

The question of the existence of resolvents of degree lower than that mentioned above and the related, but more general, problem of the determination of all the subgroups of the abelian group form the subject of investigations now in progress by the writer. On account of the great complexity‡ of these problems only small values of p are being considered. The discussions for the various values of p have at least one question in common, that of the subgroups of order a power of p. To avoid duplication, this question is here treated for general p, together with a number of related questions.

2. The group of quaternary special abelian substitutions in the $GF[p^n]$ has a self-conjugate subgroup composed of the identity and the substitution which merely changes the sign of each variable. The quotient group G is simple except in the case $p=2$, $n=1$, when it is holoedrically isomorphic with the symmetric group on 6 letters.§ The order of G is

$$\tfrac{1}{2}p^{4n}(p^{4n}-1)(p^{2n}-1) \quad \text{if } p>2; \qquad p^{4n}(p^{4n}-1)(p^{2n}-1) \quad \text{if } p=2.$$

* Presented to the Society at the Boston meeting, August 31–September 1, 1903. Received for publication June 23, 1903.

† *Traité des Substitutions*, Note E, p. 666; Comptes Rendus (1870), pp. 326–328, 1028.

‡ Compare JORDAN, Note E, *loc. cit.*

§ *Linear Groups*, pp. 94–100.

The operators of G are conveniently designated as follows:

$$(1) \qquad \pm \begin{bmatrix} \alpha_{11} & \gamma_{11} & \alpha_{12} & \gamma_{12} \\ \beta_{11} & \delta_{11} & \beta_{12} & \delta_{12} \\ \alpha_{21} & \gamma_{21} & \alpha_{22} & \gamma_{22} \\ \beta_{21} & \delta_{21} & \beta_{22} & \delta_{22} \end{bmatrix}.$$

When needed, the variables are designated $\xi_1, \eta_1, \xi_2, \eta_2$ in order.

An abelian substitution permutes the $p^{4n}-1$ letters $L_{\xi_1, \eta_1, \xi_2, \eta_2}$ in which $\xi_1, \eta_1, \xi_2, \eta_2$ are not simultaneously zero. Combining them into systems

$$\{L_{\mu\xi_1, \mu\eta_1, \mu\xi_2, \mu\eta_2}, \quad \text{where } \mu \text{ ranges over the marks } \neq 0 \text{ of the } GF[p^n]\},$$

we obtain $(p^{4n}-1)/(p^n-1)$ systems which are permuted amongst themselves by the *homogeneous* abelian substitutions. *Hence the group G may be represented as a (transitive †) substitution group on $(p^{4n}-1)/(p^n-1)$ letters.*

3. An operator of G is commutative with $L_{1,1}$ if and only if it be of the form

$$(2) \qquad \pm \begin{bmatrix} 1 & k & a & c \\ 0 & 1 & 0 & 0 \\ 0 & \alpha c - \gamma a & \alpha & \gamma \\ 0 & \beta c - \delta a & \beta & \delta \end{bmatrix} \qquad (\alpha\delta - \beta\gamma = 1).$$

The number of these operators is $p^{3n}\cdot(p^{2n}-1)p^n$. They form a subgroup $G_{p^{4n}(p^{2n}-1)}$. In view of their importance and frequent occurrence a notation for certain of these operators is introduced:

$$(3) \qquad [k, a, c, \gamma] = \pm \begin{bmatrix} 1 & k & a & c \\ 0 & 1 & 0 & 0 \\ 0 & c - \gamma a & 1 & \gamma \\ 0 & -a & 0 & 1 \end{bmatrix}.$$

They form a group $G_{p^{4n}}$ in view of the formula of composition

$$(4) \qquad [K, A, C, \Gamma][k, a, c, \gamma] = [K + k + aC - cA - aA\Gamma, A + a, C + c + a\Gamma, \Gamma + \gamma].$$

It follows that the second, third, fourth and fifth powers of (3) are respectively

$$[2k - a^2\gamma, 2a, 2c + a\gamma, 2\gamma], \quad [3k - 4a^2\gamma, 3a, 3c + 3a\gamma, 3\gamma],$$

† American Journal of Mathematics, vol. 23 (1901), p. 367.

$$[4k - 10a^2\gamma,\ 4a,\ 4c + 6a\gamma,\ 4\gamma], \qquad [5k - 20a^2\gamma,\ 5a,\ 5c + 10a\gamma,\ 5\gamma].$$

By one-step induction, we readily find that

$$(5)\quad [k, a, c, \gamma]^r = [rk - \tfrac{1}{6}r(r^2-1)a^2\gamma,\ ra,\ rc + \tfrac{1}{2}r(r-1)a\gamma,\ r\gamma].$$

It follows that, if $p>3$, the pth power of $[k, a, c, \gamma]$ is $[0, 0, 0, 0]$, namely, identity; for $p = 2$ or 3, the power p^2 is the identity, while the pth power is the identity if and only if $a\gamma = 0$.

THEOREM. *For $p > 3$ the group $G_{p^{4n}}$ contains, in addition to the identity, only operators of period p. For $p = 2$ or 3, it contains only operators of periods $1, p, p^2$.*

Since p^{4n} is the highest power of p which divides the order of G, there is a single set of conjugate subgroups of order p^{4n}.

COROLLARY.* *For $p > 3$, the group G contains no operator of period p^a, $a > 1$. For $p = 2$ or 3, G contains no operator of period p^a, $a > 2$.*

4. THEOREM. *Within G, the group $G_{p^{4n}}$ is self-conjugate only under the group*

$$(6)\quad G_{\frac{1}{2}p^{4n}(p^n-1)^2} = (G_{p^{4n}},\ T_{1,a_1}T_{2,a_2}) : \pm \begin{Vmatrix} \alpha_{11} & \gamma_{11} & \alpha_{12} & \gamma_{12} \\ 0 & \alpha_{11}^{-1} & 0 & 0 \\ 0 & \alpha_{11}^{-1}(\alpha_{22}\gamma_{12} - \alpha_{12}\gamma_{22}) & \alpha_{22} & \gamma_{22} \\ 0 & -\alpha_{11}^{-1}\alpha_{22}^{-1}\alpha_{12} & 0 & \alpha_{22}^{-1} \end{Vmatrix}.$$

The operator (1) transforms $[k, a, c, \gamma]$ into an operator T replacing η_1 by

$$A_2\xi_1 + B_2\eta_1 + C_2\xi_2 + D_2\eta_2,$$

where, after reductions by means of the abelian conditions on (1),

$$A_2 = -k\beta_{11}^2 - \gamma\beta_{12}^2 + 2a\beta_{11}\delta_{12} - 2c\beta_{11}\beta_{12} + a\gamma\beta_{11}\beta_{12},$$

$$B_2 = 1 + k\alpha_{11}\beta_{11} + \gamma\alpha_{12}\beta_{12} - a\beta_{11}\gamma_{12} - a\alpha_{11}\delta_{12} + c\alpha_{11}\beta_{12} + c\beta_{11}\alpha_{12} - a\gamma\alpha_{11}\beta_{12},$$

$$C_2 = -k\beta_{11}\beta_{21} - \gamma\beta_{12}\beta_{22} + a\beta_{11}\delta_{22} + a\delta_{12}\beta_{21} - c\beta_{11}\beta_{22} - c\beta_{12}\beta_{21} + a\gamma\beta_{12}\beta_{21},$$

$$D_2 = k\beta_{11}\alpha_{21} + \gamma\beta_{12}\alpha_{22} - a\beta_{11}\gamma_{22} - a\delta_{12}\alpha_{21} + c\beta_{11}\alpha_{22} + c\alpha_{21}\beta_{12} - a\gamma\alpha_{21}\beta_{12}.$$

Since T shall belong to $G_{p^{4n}(p^{2n}-1)}$, we must have

$$A_2 = 0, \quad B_2 = 1, \quad C_2 = 0, \quad D_2 = 0,$$

for every set of marks k, a, c, γ of the $GF[p^n]$. But a linear homogeneous function of $k, a, c, \gamma, a\gamma$ with coefficients in a field F of order > 1 equals zero for

*Compare Transactions, vol. 2 (1901), p. 113. The signs of Z and W in the footnote should be changed.

every mark k, a, c, γ of F if and only if each of its coefficients is zero. Hence $A_2 = 0$ requires that $\beta_{11} = \beta_{12} = 0$; then $B_2 = 1$ requires that $\alpha_{11}\delta_{12} = 0$; $C_2 = 0$ requires that $\delta_{12}\beta_{21} = 0$; $D_2 = 0$ requires that $\delta_{12}\alpha_{21} = 0$. If $\delta_{12} \neq 0$, then all the coefficients in the first column of (1) are zero. Hence $\delta_{12} = 0$.

Applying the abelian conditions, we find that (1) becomes

$$(7) \qquad \pm \begin{bmatrix} \alpha_{11} & \gamma_{11} & \alpha_{12} & \gamma_{12} \\ 0 & \alpha_{11}^{-1} & 0 & 0 \\ 0 & \gamma_{21} & \alpha_{22} & \gamma_{22} \\ 0 & \delta_{21} & \beta_{22} & \delta_{22} \end{bmatrix}, \quad \begin{pmatrix} \gamma_{21} = \alpha_{11}^{-1}(\alpha_{22}\gamma_{12} - \alpha_{12}\gamma_{22}) \\ \delta_{21} = \alpha_{11}^{-1}(\beta_{22}\gamma_{12} - \alpha_{12}\delta_{22}) \\ \alpha_{22}\delta_{22} - \beta_{22}\gamma_{22} = 1 \end{pmatrix}$$

The latter is seen to transform $[k, a, c, \gamma]$ into

$$\pm \begin{bmatrix} 1 & k' & a\alpha_{11}\delta_{22} - c\alpha_{11}\beta_{22} - \gamma\alpha_{12}\beta_{22} & c' \\ 0 & 1 & 0 & 0 \\ 0 & c\alpha_{11}\alpha_{22} - a\alpha_{11}\gamma_{22} - a\gamma\alpha_{11}\alpha_{22} + \gamma\alpha_{12}\alpha_{22} & 1 - \gamma\alpha_{22}\beta_{22} & \gamma\alpha_{22}^2 \\ 0 & c\alpha_{11}\beta_{22} - a\alpha_{11}\delta_{22} - a\gamma\alpha_{11}\beta_{22} + \gamma\alpha_{12}\beta_{22} & -\gamma\beta_{22}^2 & 1 + \gamma\alpha_{22}\beta_{22} \end{bmatrix},$$

where

$$k' = k\alpha_{11}^2 - 2a\alpha_{11}\gamma_{12} + 2c\alpha_{11}\alpha_{12} - a\gamma\alpha_{11}\alpha_{12} + \gamma\alpha_{12}^2, \quad c' = c\alpha_{11}\alpha_{22} - a\alpha_{11}\gamma_{22} + \gamma\alpha_{12}\alpha_{22}.$$

For $\gamma \neq 0$, this operator is of the form (2) with $\beta = 0$ only when $\beta_{22} = 0$. Inversely, if $\beta_{22} = 0$, it has the form $[k', a\alpha_{11}\delta_{22}, c', \gamma\alpha_{22}^2]$.

Since (7) is the product of an operator (2) by $T_{1, a_{11}}$ and since the latter transforms every operator (2) into an operator (2), we derive

COROLLARY I. *Within G, the group $G_{p^{4n}(p^{2n}-1)}$ is self-conjugate only under the group $G_{\frac{1}{2}p^{4n}(p^{2n}-1)(p^n-1)} = (G_{p^{4n}(p^{2n}-1)}, T_{1,a})$ of the operators (7). The latter is therefore one of $(p^{4n}-1)/(p^n-1)$ conjugate subgroups of G.*

COROLLARY II. *Within G, the group $G_{\frac{1}{2}p^{4n}(p^n-1)^2}$ is self-conjugate only under itself and hence is one of $(p^{2n}+1)(p^n+1)^2$ conjugate subgroups.*

Distribution of the operators of $G_{p^{4n}}$ into sets of conjugates.

5. Upon specialization of (7) by setting $\alpha_{11} = 1$, $\alpha_{22} = \delta_{22} = 1$, $\beta_{22} = 0$, it follows from the preceding section that $[p, q, r, s]$ transforms $[k, a, c, \gamma]$ into

$$[k + 2qc - 2ra - qa\gamma + q^2\gamma, a, c + q\gamma - sa, \gamma].$$

In order that the latter shall be identical with $[k, a, c, \gamma]$ for every p, q, r, s, it is necessary and sufficient that $a = \gamma = c = 0$ if $p > 2$, and that $a = \gamma = 0$

if $p = 2$. *Hence the only self-conjugate operators in* $G_{p^{4n}}$ *are* $[k, 0, 0, 0]$ *if* $p > 2$, *but are* $[k, 0, c, 0]$ *if* $p = 2$.

Henceforth let $p > 2$. Let a and γ have fixed values each $\neq 0$. Then $[k, a, c, \gamma]$ is conjugate with $[k', a, c', \gamma]$ if and only if

$$k' = k + 2qc - 2ra - qa\gamma + q^2\gamma, \qquad c' = c + q\gamma - sa$$

have solutions p, q, r, s in the field. The second equation can be satisfied by a suitable choice of q or s, and the first by a subsequent choice of r. *Hence the operators* $[k, a, c, \gamma]$, $a \neq 0, \gamma \neq 0$, *fall into* $(p^n - 1)^2$ *sets* $S_{a,\gamma}$ *each of* p^{2n} *conjugate operators within* $G_{p^{4n}}$.

An operator $[k, a, c, 0]$, $a \neq 0$, is conjugate with $[k', a, c', 0]$ if and only if there exist solutions q, r, s of

$$k' = k + 2qc - 2ra, \qquad c' = c - sa.$$

We may take $q = 0$ and determine r and s by the first and second equations, respectively. *Hence the operators* $[k, a, c, 0]$, $a \neq 0$, *fall into* $p^n - 1$ *sets* S_a *each of* p^{2n} *conjugate operators.*

Similarly, *the operators* $[k, 0, c, 0]$, $c \neq 0$, *fall into* $p^n - 1$ *sets* S'_c *each of* p^n *conjugate operators.*

There remain the operators $[k, 0, c, \gamma]$, $\gamma \neq 0$. The latter is conjugate only with $[k', 0, c', \gamma]$, where $k' = k + 2qc + q^2\gamma$, $c' = c + q\gamma$. Hence

$$q = \frac{1}{\gamma}(c' - c), \qquad k' = k + \frac{1}{\gamma}(c'^2 - c^2).$$

Hence if k, c, c', γ are any given marks such that $\gamma \neq 0$, there exists an unique mark k' for which $[k, 0, c, \gamma]$ and $[k', 0, c', \gamma]$ are conjugate. *Hence the operators* $[k, 0, c, \gamma]$, $\gamma \neq 0$, *fall into* $p^n(p^n - 1)$ *sets* $\Sigma_{k,\gamma}$ *each of* p^n *conjugate operators.*

For a set $S_{a,\gamma}$, S_a or S'_c, the subscripts are defining invariants. But for $\Sigma_{k,\gamma}$, the subscript γ alone is an invariant.

THEOREM. *The operators of* $G_{p^{4n}}$ *fall into* $2p^{2n} - 1$ *distinct sets of conjugate operators;* p^n *sets contain each a single operator,* $p^{2n} - p^n$ *sets contain each* p^{2n} *operators,* $p^{2n} - 1$ *sets contain each* p^n *operators.*

6. In illustration of the results of § 5, consider the important case $p^n = 3$. Then, by § 3, $[k, a, c, \gamma]^3 = [0, 0, 0, 0] =$ identity if and only if $a\gamma = 0$. Hence the 44 operators of period 3 in G_{81} are $[k, a, c, 0]$ and $[k, 0, c, \gamma]$, excluding $[0, 0, 0, 0]$. The remaining 36 operators $[k, a, c, \gamma]$, $a\gamma \neq 0$, are of period 9. The 81 operators fall into the following 17 sets of conjugates: *

* The last six sets may be given compactly as follows

$$\{[k, 0, 1, \gamma], [k, 0, -1, \gamma], [k-\gamma, 0, 0, \gamma]\} \quad (k=0,1,-1;\ \gamma=1,-1).$$

$$[0,0,0,0];\quad [1,0,0,0];\quad [-1,0,0,0];$$

$$[k,1,c,1];\quad [k,1,c,-1];\quad [k,-1,c,1];\quad [k,-1,c,-1];$$

$$[k,1,c,0];\quad [k,-1,c,0];\quad [k,0,1,0];\quad [k,0,-1,0];$$

$$\{[0,0,1,\pm 1],[0,0,-1,\pm 1],[\mp 1,0,0,\pm 1]\};$$

$$\{[0,0,0,\pm 1],[\pm 1,0,1,\pm 1],[\pm 1,0,-1,\pm 1]\};$$

$$\{[\pm 1,0,0,\pm 1],[\mp 1,0,1,\pm 1],[\mp 1,0,-1,\pm 1]\},$$

where the upper (or lower) signs belong together, while the operators given by $k, c = 0, 1, -1$ belong to the same set.

Determination of the self-conjugate subgroups of $G_{p^{4n}}$.

7. If a self-conjugate subgroup H contains one operator of a set $S_{a,\gamma}$, $a \neq 0$, $\gamma \neq 0$, it contains every $[k, a, c, \gamma]$, k and c being arbitrary. By (5), H contains one, and hence every, operator $[k, ra, c, r\gamma]$, for each integer $r = 1, 2, \cdots, p-1$. But, by (4),

$$[K, Ra, C, R\gamma][k, ra, c, r\gamma]$$

$$= [K + k + raC - Rac - R^2ra^2\gamma, (R+r)a, C + c + Rra\gamma, (R+r)\gamma].$$

It follows first that H contains also every $[k, 0, c, 0]$ and second that H contains the *group*

$$(8)\quad H^{a,\gamma}_{p^{2n+1}} = \{[k, ra, c, r\gamma], (r = 0, 1, 2, \cdots, p-1;\ k \text{ and } c \text{ arbitrary})\}.$$

Note that (a, γ) and (a', γ') define the same group if $a'/a = \gamma'/\gamma =$ an integer prime to p, so that there are $p^{n-1}(p^n - 1)$ distinct groups (8).

If H contains one operator of a set S_a, $a \neq 0$, it contains $[k, a, c, 0]$ for k and c arbitrary. Then, by (5), H contains every $[k, ra, c, 0]$, $r = 1, \cdots, p-1$. By (4),

$$[K, Ra, C, 0][k, ra, c, 0] = [K + k + raC - Rac, (R+r)a, C + c, 0].$$

Hence H contains also every $[k, 0, c, 0]$, and contains the *group*

$$(9)\quad G^{a}_{p^{2n+1}} = \{[k, ra, c, 0], (r = 0, 1, \cdots, p-1;\ k \text{ and } c \text{ arbitrary})\}.$$

If H contains one operator of a set S'_c, $c \neq 0$, it contains $[k, 0, c, 0]$ for k arbitrary. The rth power of the latter is $[rk, 0, rc, 0]$. Also

$$[K, 0, Rc, 0][k, 0, rc, 0] = [K + k, 0, Rc + rc, 0].$$

Hence H contains the *commutative group*

$$(10) \qquad K^{c}_{p^{n+1}} = \{[k, 0, rc, 0], (r = 0, 1, \cdots, p-1;\ k \text{ arbitrary})\}.$$

If H contains $[k, 0, 0, 0]$, it contains the cyclic group

$$(11) \qquad C^{k}_{p} = \{[rk, 0, 0, 0], (r = 0, 1, \cdots, p-1)\}.$$

Finally, let H contain one $[k, 0, c, \gamma]$, $\gamma \neq 0$. By (4),

$$(12) \qquad [K, 0, C, \Gamma][k, 0, c, \gamma] = [K + k, 0, C + c, \Gamma + \gamma].$$

Now $[k, 0, c, \gamma]$ is conjugate with $[k + (c'^2 - c^2)/\gamma, 0, c', \gamma]$, c' being arbitrary. Multiplying the latter by the inverse of the former and setting $c' - c = \lambda$, we get $A = [(\lambda^2 + 2\lambda c)/\gamma, 0, \lambda, 0]$, which therefore occurs in H for λ arbitrary. Replacing λ by $-\lambda$, and taking the product of the resulting operator by A, we get $[2\lambda^2/\gamma, 0, 0, 0]$. Hence, if $p > 2$, H contains every $[k, 0, 0, 0]$, since $\lambda_1^2 - \lambda_2^2$ can be made to take any desired value, so that H contains every $[k, 0, c, 0]$. The same result follows for any p by § 5, since A is conjugate with every $[k, 0, \lambda, 0]$. By (5),

$$[k, 0, c, \gamma]^r = [rk, 0, rc, r\gamma].$$

Hence H contains the *commutative group*

$$(13) \qquad K^{\gamma}_{p^{2n+1}} = \{[k, 0, c, r\gamma], (r = 0, 1, \cdots, p-1;\ k \text{ and } c \text{ arbitrary})\}.$$

THEOREM. *The* $p^{n-1}(p^n - 1)$ *groups* (8), *the* p^{n-1} *groups* (9), *the* p^{n-1} *groups* (10), *the* p^{n-1} *groups* (11) *in addition to the identity, and the* p^{n-1} *groups* (13), *together with all groups resulting from their combination, give all the self-conjugate subgroups of* $G_{p^{4n}}$.

8. For $n = 1$, the complete list of self-conjugate subgroups follows without further computation. We may now drop one of the superscripts in the notation for each group, giving the following groups:*

$$(8') \qquad H^{t}_{p^3} = \{[k, ta, c, a], (k, a, c = 0, 1, \cdots, p-1)\} \quad (t = 1, 2, \cdots, p-1),$$

$$(9') \qquad G_{p^3} = \{[k, a, c, 0], (k, a, c = 0, 1, \cdots, p-1)\},$$

$$(10') \qquad K_{p^2} = \{[k, 0, c, 0], (k, c = 0, 1, \cdots, p-1)\},$$

$$(11') \qquad C_{p} = \{[k, 0, 0, 0], (k = 0, 1, \cdots, p-1)\},$$

$$(13') \qquad K_{p^3} = \{[k, 0, c, \gamma], (k, c, \gamma = 0, 1, \cdots, p-1)\}.$$

* In (8), only the ratio a/γ is now invariant. It is set equal to t.

Evidently C_p lies in all these groups, while K_{p^2} lies in all of order p^3. Hence a combination of two or more of these groups leads to no new group other than G_{p^4}. We may therefore state the

THEOREM. *The group G_{p^4} contains only the self-conjugate subgroups* (8′)–(13′) *in addition to itself and the identity.*

Since a subgroup $G_{p^{m-1}}$ of G_{p^m} is necessarily self-conjugate, we have the

COROLLARY. *The $p+1$ groups* (8′), (9′), (13′) *give all the subgroups of order p^3 of G_{p^4}.*

9. THEOREM. *Within G for $n=1$, every subgroup of order p^3 is conjugate with* * *H_{p^3}, G_{p^3} or K_{p^3}, while no two of the latter are conjugate.*

Within G, every subgroup of order p^3 is contained† in one or more subgroups of order p^4, the latter being conjugate with G_{p^4} by SYLOW's theorem. We may therefore confine our attention to the groups (8′), (9′) and (13′). But $T_{1,t-1}$ transforms $[k, ta, c, a]$ into $[kt^{-2}, a, t^{-1}c, a]$ and hence transforms $H_{p^3}^t$ into $H_{p^3}^1 \equiv H_{p^3}$. In view of the formulæ

$$[K, A, C, A][k, a, c, a] = [K+k+aC-cA-aA^2, A+a, C+c+aA, A+a], \tag{14}$$

$$[K, A, C, 0][k, a, c, 0] = [K+k+aC-cA, A+a, C+c, 0], \tag{15}$$

the only self-conjugate operators in either H_{p^3} or G_{p^3} are $[k, 0, 0, 0]$. Hence neither is conjugate with the commutative group K_{p^3}. The first two are not conjugate by §§ 14–15. For $p=3$, this also follows from the fact that H_{27} contains operators of period 9, while G_{27} and K_{27} contain only operators of periods 1 and 3.

Conjugacy of the operators of H_{p^3}; its self-conjugate subgroups.

10. By § 5, $[p, q, r, q]$ transforms $[k, a, c, a]$ into $[k', a, c, a]$, where

$$k' = k + 2qc - 2ra - qa^2 + q^2a.$$

Let k, a, c be given. If $a \neq 0$, we may take $q=0$ and choose r to make k' take any assigned value. If $a=0$, $c \neq 0$, we can choose q to make k' arbitrary. *Hence the operators of H_{p^3} fall into exactly p^2+p-1 sets of conjugates:*

$\{[k, a, c, a], k=0, 1, \cdots, p-1\}$ (*a, c fixed integers not both $\equiv 0$*),

$\{[k, 0, 0, 0]\}$ (*k a fixed integer*).

* For $t=1$, (8′) is designated also H_{p^3}.

† BURNSIDE, *The Theory of Groups*, p. 94, Corollary III

11. If a self-conjugate subgroup J contains the operator $[k', a, c, a]$, where a and c are not both $\equiv 0$, it contains every $[k, a, c, a]$, $k = 0, 1, \cdots, p-1$. By (14), the inverse of the latter is $[-k, -a, -c+a^2, -a]$. The product of the latter by $[K, a, c, a]$ is $[K-k, 0, 0, 0]$. Hence J contains the commutative group generated by $[1, 0, 0, 0]$ and $[0, a, c, a]$:

$$(16)\quad H_{p^3}^{a,c} = \{[k, ra, rc + \tfrac{1}{2}r(r-1)a^2, ra], (k, r = 0, 1, \cdots, p-1)\}.$$

For $a = 0$, the group is (10′). For $p = 3$, $a \neq 0$, the group is a cyclic group of order 9 since $[0, a, c, a]^3 = [-a^3, 0, 0, 0]$.

THEOREM. *For $p > 2$ the group H_{p^3} has only the following self-conjugate subgroups in addition to itself, the identity and C_p:*

if $p > 3$, K_{p^2} and p further non-cyclic groups (16) *with $a \neq 0$;*

if $p = 3$, K_9 and 3 cyclic groups of order 9 generated by respectively $[0,1,1,1]$, $[1,-1,1,-1]$ *and* $[1,1,-1,1]$.

COROLLARY. *For $p > 2$, H_{p^3} has exactly $p+1$ subgroups of order p^2.*

Conjugacy of the operators of G_{p^3}; its self-conjugate subgroups.

12. By § 5, $[p, q, r, 0]$ transforms $[k, a, c, 0]$ into $[k', a, c, 0]$, where $k' = k + 2qc - 2ra$. If a and c are fixed marks on the $GF[p]$, $p > 2$, not both zero, we can choose q and r to make k' take any assigned value. But if $a = c = 0$, then $[k, 0, 0, 0]$ is self-conjugate.

Hence the operators of G_{p^3} fall into exactly $p^2 + p - 1$ sets of conjugates:

$$\{[k, a, c, 0], k = 0, 1, \cdots, p-1\} \quad (a, c, \textit{fixed integers not both} \equiv 0),$$

$$\{[k, 0, 0, 0]\} \quad (k \textit{ a fixed integer}).$$

13. If a self-conjugate subgroup J of G_{p^3} contains one operator $[k, a, c, 0]$, where a and c are fixed integers not both zero, it contains them all. Also J contains the inverse $[-k, -a, -c, 0]$ [see formula (14)]. The product of the latter by $[K, a, c, 0]$ is $[K-k, 0, 0, 0]$. Hence J contains the commutative group generated by $[1, 0, 0, 0]$ and $[0, a, c, 0]$:

$$(17)\qquad K_{p^2}^{a,c} = \{[k, ra, rc, 0], (k, r = 0, 1, \cdots, p-1)\}.$$

For $a = 0$, the group is (10′). Whether $p = 3$ or $p > 3$, the groups are non-cyclic.

THEOREM. *For $p \neq 2$, the group G_{p^3} has as its self-conjugate subgroups, besides itself and the identity, the group C_p and $p+1$ non-cyclic commutative groups* (17). *It thus has exactly $p+1$ subgroups of order p^2.*

Largest subgroups in which G_{p^3}, H_{p^3}, K_{p^3} are self-conjugate.

14. THEOREM. *Within $G_{n=1}$, the group G_{p^3} is self-conjugate only under the group $G_{\frac{1}{2}p^4(p^2-1)(p-1)}$ of the operators* (7) *with coefficients modulo p.*

Proceeding as in § 4 with $\gamma = 0$, we must have $A_2 = 0$, $B_2 = 1$, $C_2 = 0$, $D_2 = 0$ for every set of integers k, a, c. Hence

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

If $\beta_{12} \neq 0$, then $\alpha_{11} = \beta_{21} = \alpha_{21} = 0$, so that all the coefficients in the first column of (1) are zero; hence must $\beta_{12} = 0$. Similarly, $\delta_{12} = 0$. Hence (1) reduces to (7). The latter transforms $[k, a, c, 0]$ into $[k', a', c', 0]$, where, by § 4,

$$k' = k\alpha_{11}^2 - 2a\alpha_{11}\gamma_{12} + 2c\alpha_{11}\alpha_{12},\quad a' = a\alpha_{11}\delta_{22} - c\alpha_{11}\beta_{22},\quad c' = c\alpha_{11}\alpha_{22} - a\alpha_{11}\gamma_{22}.$$

For general n, the conditions that k', a', c' shall be integers modulo p, $p > 2$, for every set of integers k, a, c, are that α_{11}^2, $\alpha_{11}\gamma_{12}$, $\alpha_{11}\alpha_{12}$, $\alpha_{11}\delta_{22}$, $\alpha_{11}\beta_{22}$, $\alpha_{11}\alpha_{22}$ and $\alpha_{11}\gamma_{22}$ shall be integral marks. The same is then true for $\alpha_{11}\gamma_{21}$ and $\alpha_{11}\delta_{21}$. Hence the ratios of the various coefficients of (7) to α_{11} must belong to the $GF[p]$. Hence (7) is the product of an operator with integral coefficients by $T_{1,\alpha_{11}}T_{2,\alpha_{11}}$, where α_{11}^2 is integral. We may restrict α_{11} to the roots of $x^2 = \nu$, where ν is a particular non-residue of p. We have therefore the

COROLLARY. *For $p > 2$ and n even, the group G_{p^3} is self-conjugate within G only under the group $G_{p^4(p^2-1)(p-1)}$ of operators (7) whose coefficients are all integers or all integral multiples of a square root of a non-residue of p. For n odd, the group is that in the theorem.*

15. THEOREM. *Within $G_{n=1}$, the group H_{p^3} is self-conjugate only under*

$$G_{\frac{1}{2}p^4(p-1)} = (G_{p^4},\ T_{1,a^3}T_{2,a}). \tag{18}$$

Proceeding as in § 4 with $\gamma = a$, we must have $A_2 = 0$, $B_2 = 1$, $C_2 = 0$, $D_2 = 0$ for every set of integers k, c, a. If a linear homogeneous function of k, c, a, a^2 is zero for every k, c, a, then its coefficients are all zero. The conditions are therefore $\beta_{11} = \beta_{12} = 0$, $\alpha_{11}\delta_{12} = 0$, $\beta_{21}\delta_{12} = 0$, $\alpha_{21}\delta_{12} = 0$, respectively. Hence $\delta_{12} = 0$, so that the transformer must be of the form (7). Then, as in § 4, $\beta_{22} = 0$, and $[k, a, c, a]$ is transformed into $[k', a\alpha_{11}\delta_{22}, c', a\alpha_{22}^2]$. Hence must $\alpha_{11}\delta_{22} = \alpha_{22}^2$. But $\alpha_{22}\delta_{22} = 1$. Hence $\alpha_{11} = \alpha_{22}^3$.

16. THEOREM. *Within $G_{n=1}$, the group K_{p^3} is self-conjugate only under the group $H_{\frac{1}{2}p^4(p^2-1)(p-1)}$ of the operators*

$$\pm \begin{bmatrix} \alpha_{11} & \gamma_{11} & \alpha_{12} & \gamma_{12} \\ 0 & \delta_{11} & 0 & \delta_{12} \\ \alpha_{21} & \gamma_{21} & \alpha_{22} & \gamma_{22} \\ 0 & \delta_{21} & 0 & \delta_{22} \end{bmatrix}, \quad \begin{pmatrix} \alpha_{11}\delta_{11} + \alpha_{12}\delta_{12} = 1,\ \alpha_{11}\delta_{21} + \alpha_{12}\delta_{22} = 0 \\ \alpha_{22}\delta_{22} + \alpha_{21}\delta_{21} = 1,\ \alpha_{22}\delta_{12} + \alpha_{21}\delta_{11} = 0 \\ \alpha_{11}\gamma_{21} + \alpha_{12}\gamma_{22} - \alpha_{21}\gamma_{11} - \alpha_{22}\gamma_{12} = 0 \end{pmatrix}, \tag{19}$$

and hence is one of $(p^4 - 1)/(p - 1)$ conjugate subgroups.

Proceeding as in § 4 with $a = 0$, we find that $A_2 = 0$ for every k, c, γ requires that $\beta_{11} = \beta_{12} = 0$. In view of these values, we have $B_2 = 1, C_2 = 0, D_2 = 0$, identically. By computation, the operator (1) with $\beta_{11} = \beta_{12} = 0$ is seen to transform $[k, 0, c, \gamma]$ into

$$(20) \qquad \pm \begin{Vmatrix} 1 & K & A & C \\ 0 & 1 & 0 & 0 \\ 0 & C & 1-E & \Gamma \\ 0 & -A & B & 1+E \end{Vmatrix},$$

$$(21) \quad \begin{cases} K = k\alpha_{11}^2 + \gamma\alpha_{12}^2 + 2c\alpha_{11}\alpha_{12}, & A = -k\alpha_{11}\beta_{21} - c\alpha_{11}\beta_{22} - c\alpha_{12}\beta_{21} - \gamma\alpha_{12}\beta_{22}, \\ \Gamma = k\alpha_{21}^2 + \gamma\alpha_{22}^2 + 2c\alpha_{21}\alpha_{22}, & C = k\alpha_{11}\alpha_{21} + c\alpha_{11}\alpha_{22} + c\alpha_{12}\alpha_{21} + \gamma\alpha_{12}\alpha_{22}, \\ B = -k\beta_{21}^2 - \gamma\beta_{22}^2 - 2c\beta_{21}\beta_{22}, & E = k\alpha_{21}\beta_{21} + c\alpha_{22}\beta_{21} + c\alpha_{21}\beta_{22} + \gamma\alpha_{22}\beta_{22}. \end{cases}$$

In order that (20) shall reduce to $[K, 0, C, \Gamma]$, it is necessary that $\beta_{21} = \beta_{22} = 0$ (from $B = 0$) and sufficient (since then $A = 0, E = 0$). Then the transformer becomes (19) on applying the abelian conditions. The first four of the resulting conditions (19) may be solved and given the equivalent form

$$(22) \quad \alpha_{11} = \delta_{22}/\Delta, \quad \alpha_{12} = -\delta_{21}/\Delta, \quad \alpha_{21} = -\delta_{12}/\Delta, \quad \alpha_{22} = \delta_{11}/\Delta, \quad \Delta \equiv \delta_{11}\delta_{22} - \delta_{12}\delta_{21}.$$

Evidently Δ is $\not\equiv 0$ since it is a factor of the determinant of (19). The number of sets of integers δ_{ij} modulo p for which $\Delta \not\equiv$ is $(p^2-1)(p^2-p)$. The fifth condition (19) involves the γ_{ij} linearly with coefficients not all zero, so that three of the γ_{ij} are arbitrary. The number of homogeneous substitutions (19) is therefore $p^3(p^2-1)(p^2-p)$.

Subgroups of order p^2 of the commutative group K_{p^3}.

17. Such a subgroup contains, in addition to the identity, only operators of period p. Hence it is generated by two commutative operators A and B of period p. The quotient of $(p^3-1)(p^3-p)$, the number of ways A and B may be selected, by $(p^2-1)(p^2-p)$, the number of ways a given group (A, B) can be generated, gives *the number p^2+p+1 of distinct subgroups of order p^2.*

Now $[p, q, r, s]$ transforms the general operator $[k, 0, c, \gamma]$ of K_{p^3} into $[k', 0, c', \gamma]$, where

$$k' = k + 2qc + q^2\gamma, \qquad c' = c + q\gamma.$$

If $\gamma \not\equiv 0$, we can choose q to make $c' = 0$. By (5), the rth power of $[k', 0, 0, \gamma]$ is $[rk', 0, 0, r\gamma]$. Hence we can choose $[k, 0, 0, 1]$ as the first generator. If $\gamma = 0$, $c \not\equiv 0$, and if $p > 2$, we can choose q to make

$k' = 0$. A suitable power of $[0, 0, c, 0]$ gives $[0, 0, 1, 0]$. Finally, if $\gamma = c = 0$, we are led to $[1, 0, 0, 0]$.* With $A = [k, 0, 0, 1]$, the group contains a second generator $[k', 0, c, 0]$. We may therefore suppose that the first generator is $[1, 0, 0, 0]$ or $[0, 0, 1, 0]$.

For $A = [1, 0, 0, 0]$, we may take $[0, 0, c, \gamma]$ as the second generator. If $\gamma = 0$, a suitable power gives $B = [0, 0, 1, 0]$. If $\gamma \neq 0$, a suitable power gives $[0, 0, c, 1]$. But $[p, q, r, s]$ transforms A into itself and $[0, 0, c, 1]$ into $[2qc + q^2, 0, c + q, 1]$. Taking $q = -c$, we are led to $B = [0, 0, 0, 1]$. The resulting groups are

$$(23) \qquad K_{p^2} = \{[k, 0, c, 0]\}, \qquad K^*_{p^2} = \{[k, 0, 0, \gamma]\}.$$

For $A = [0, 0, 1, 0]$, we may take $[k, 0, 0, \gamma]$ as the second generator. The case $\gamma = 0$ leads to K_{p^2}. For $\gamma \neq 0$, a suitable power gives $[\sigma, 0, 0, 1]$. If $\sigma = 0$, the resulting group $\{[0, 0, c, \gamma]\}$ is transformed by P_{12} into $\{[\gamma, 0, c, 0]\} = K_{p^2}$. The case $\sigma \neq 0$ requires detailed study.

We proceed to determine whether or not a group $\{[\sigma\gamma, 0, c, \gamma]\}$ is conjugate within $G_{n=1}$ with another such group or with one of the groups (23). If (1) transforms $[\sigma\gamma, 0, c, \gamma]$ into an operator T leaving η_1 fixed, then (as in § 4 with $k = \sigma\gamma$, $a = 0$)

$$A_2 \equiv -\sigma\gamma\beta_{11}^2 - \gamma\beta_{12}^2 - 2c\beta_{11}\beta_{12} = 0$$

for every c and γ. Hence $\beta_{11}\beta_{12} = 0$, $\sigma\beta_{11}^2 + \beta_{12}^2 = 0$, so that $\beta_{11} = \beta_{12} = 0$. We may therefore proceed as in § 16, with $k = \sigma\gamma$, and impose the conditions $A = B = E$ that T shall reduce to the form $[K, 0, C, \Gamma]$. Now

$$B \equiv -\sigma\gamma\beta_{21}^2 - \gamma\beta_{22}^2 - 2c\beta_{21}\beta_{22} = 0$$

for every c and γ requires that $\beta_{21} = \beta_{22} = 0$. Hence (1) must become (19).

The condition $\Gamma = 0$ for every c and γ requires $\alpha_{21} = \alpha_{22} = 0$, which is impossible. *Hence a group* $\{[\sigma\gamma, 0, c, \gamma]\}$ *is not conjugate with* K_{p^2}.

---

* For the problem of the conjugacy of the cyclic subgroups of order p of K_{p^3}, we note that we may restrict the generators to $[1, 0, 0, 0]$, $[0, 0, 1, 0]$, $[\tau, 0, 0, 1]$, where $-\tau$ is a particular quadratic non-residue of p. Indeed, (19) transforms $[k, 0, 0, 1]$ into $K, 0, C, \Gamma]$, where

$$K = ka_{11}^2 + a_{12}^2, \qquad C = ka_{11}a_{21} + a_{12}a_{22}, \qquad \Gamma = ka_{21}^2 + a_{22}^2.$$

But for any set of integers a_{ij} such that $\Delta_1 \equiv a_{11}a_{22} - a_{12}a_{21}$ is $\neq 0$, there exists a substitution (19). If $-k$ is a quadratic residue or 0, the conditions $K = \tau\Gamma$, $C = 0$, $\Delta_1 \neq 0$ become

$$kx^2 + z^2 - \tau ky^2 - \tau = 0, \qquad kxy + z = 0, \qquad x - yz \neq 0,$$

upon setting $a_{11} = xa_{22}$, $a_{21} = ya_{22}$, $a_{12} = za_{22}$, and noting that $a_{22} \neq 0$. Eliminating z, we get

$$(kx^2 - \tau)(ky^2 + 1) = 0, \qquad x(1 + ky^2) \neq 0.$$

Hence the conditions can be satisfied if and only if τ/k is a residue, i. e., if $-\tau$ is a non-residue. A suitable power of $[\tau\Gamma, 0, 0, \Gamma]$ gives $[\tau, 0, 0, 1]$.

The condition $C = 0$ for every c and γ requires

$$\sigma\alpha_{11}\alpha_{21} + \alpha_{12}\alpha_{22} = 0, \qquad \alpha_{11}\alpha_{22} + \alpha_{12}\alpha_{21} = 0. \tag{24}$$

Taking α_{11} and α_{12} as the unknowns, not both of which are zero by (19), we see that the determinant $\sigma\alpha_{21}^2 - \alpha_{22}^2$ is zero. Taking α_{21} and α_{22} as the unknowns, the determinant $\sigma\alpha_{11}^2 - \alpha_{12}^2 = 0$. *Hence σ must be a square.* With this condition satisfied, we have $\alpha_{22} = s\alpha_{21}$, $\alpha_{12} = -s\alpha_{11}$, the sign following from either condition (24). The abelian conditions (19) then give

$$\delta_{21} = s\delta_{22}, \qquad \delta_{11} = -s\delta_{12}, \qquad -2s\alpha_{11}\delta_{12} = 1, \qquad 2s\alpha_{21}\delta_{22} = 1,$$

with a linear relation on the γ_{ij}. *The resulting $p^3(p-1)^2$ operators of $G_{n=1}$ transform $\{[s^2\gamma, 0, c, \gamma]\}$ into $K_{p^2}^*$.*

In order that (19) shall transform

$$\{[\sigma\gamma, 0, c, \gamma]\} \text{ into } \{[\sigma_1\gamma_1, 0, c_1, \gamma_1]\}$$

where σ and σ_1 are not-squares, it is necessary and sufficient that $K = \sigma_1\Gamma$, viz.,

$$\sigma\gamma\alpha_{11}^2 + \gamma\alpha_{12}^2 + 2c\alpha_{11}\alpha_{12} = \sigma_1(\sigma\gamma\alpha_{21}^2 + \gamma\alpha_{22}^2 + 2c\alpha_{21}\alpha_{22}),$$

for every c and γ. The conditions are

$$\alpha_{11}\alpha_{12} = \sigma_1\alpha_{21}\alpha_{22}, \qquad \sigma\alpha_{11}^2 + \alpha_{12}^2 = \sigma_1\sigma\alpha_{21}^2 + \sigma_1\alpha_{22}^2.$$

Squaring each, we find that

$$\sigma\alpha_{11}^2 - \alpha_{12}^2 = \pm\sigma_1(\sigma\alpha_{21}^2 - \alpha_{22}^2).$$

Hence $2\sigma\alpha_{11}^2$ equals either $2\sigma_1\sigma\alpha_{21}^2$ or else $2\sigma_1\alpha_{22}^2$. The first case is excluded since σ_1 is a not-square and α_{11} and α_{21} are not both zero in view of the abelian conditions. Hence $\alpha_{22} = s\alpha_{11}$, where $s^2 = \sigma/\sigma_1$. Whether α_{11} is zero or not, we have $\alpha_{12} = s\sigma_1\alpha_{21}$. Since

$$\Delta_1 = \alpha_{11}\alpha_{22} - \alpha_{21}\alpha_{12} = s\alpha_{11}^2 - s\sigma_1\alpha_{21}^2 \neq 0,$$

the δ_{ij} are uniquely determined in terms of the α_{ji} by the conditions (19):

$$\delta_{22} = \alpha_{11}/\Delta_1, \quad \delta_{21} = -s\sigma_1\alpha_{21}/\Delta_1, \quad \delta_{12} = -\alpha_{21}/\Delta_1, \quad \delta_{11} = s\alpha_{11}/\Delta_1.$$

There remains a linear relation on the γ_{ij}. Since $\Delta_1 \neq 0$ requires merely that α_{11} and α_{21} shall not both vanish, *the number of operators transforming the group given by σ into that given by σ_1 is $p^3(p^2-1)$.*

COROLLARY. *The group $K_{p^2}^{**} = \{[\sigma\gamma, 0, c, \gamma]\}$, where σ is a particular not-square, is self-conjugate only under a group of order $p^3(p^2-1)$.*

18. THEOREM. *Within $G_{n=1}$, the group K_{p^2} is self-conjugate only under $G_{\frac{1}{2}p^4(p-1)^2}$. Within G for n odd, it is self-conjugate only under the group of*

operators (6) *with* α_{11} *and* α_{12} *integers. Within* G *for* n *even, it is self-conjugate only under the group of operators* (6) *with* α_{11}^2 *and* $\alpha_{11}\alpha_{12}$ *integers.*

We proceed as in § 4 with $a = \gamma = 0$. Then

$$A_2 = -k\beta_{11}^2 - 2c\beta_{11}\beta_{12}, \qquad B_2 = 1 + k\alpha_{11}\beta_{11} + c\alpha_{11}\beta_{12} + c\beta_{11}\alpha_{12},$$

$$C_2 = -k\beta_{11}\beta_{21} - c\beta_{11}\beta_{22} - c\beta_{12}\beta_{21}, \quad D_2 = k\beta_{11}\alpha_{21} + c\beta_{11}\alpha_{22} + c\alpha_{21}\beta_{12}.$$

The condition $A_2 = 0$ for every k and c requires that $\beta_{11} = 0$. Then $B_2 = 1$ gives $\alpha_{11}\beta_{12} = 0$, $C_2 = 0$ gives $\beta_{12}\beta_{21} = 0$, $D_2 = 0$ gives $\alpha_{21}\beta_{12} = 0$. Hence $\beta_{12} = 0$. Proceeding as in § 16, we must have A, B, Γ, E all zero for every k and c. Now

$$B = -k\beta_{21}^2 - 2c\beta_{21}\beta_{22}, \ \Gamma = k\alpha_{21}^2 + 2c\alpha_{21}\alpha_{22}, \ A = -k\alpha_{11}\beta_{21} - c\alpha_{11}\beta_{22} - c\alpha_{12}\beta_{21}.$$

Hence $\beta_{21} = 0$, $\alpha_{21} = 0$, $\alpha_{11}\beta_{22} = 0$. If $\alpha_{11} = 0$, all the coefficients in the first column of (1) would vanish; hence $\beta_{22} = 0$. The abelian conditions now give

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

Hence $\delta_{12} = 0$, so that the transformer reduces to (6). Further,

$$E = 0, \qquad K = k\alpha_{11}^2 + 2c\alpha_{11}\alpha_{12}, \qquad C = c\alpha_{11}\alpha_{22}.$$

Hence K and C are integers for every k and c if and only if α_{11}^2 and $\alpha_{11}\alpha_{12}$ are integers. If n be odd, α_{11} must be an integer.

19. THEOREM. *Within* $G_{n=1}$ *the group* $K_{p^2}{}^*$ *is self-conjugate only under the group* $H_{p^{3(p-1)^2}}$ *of the operators*

$$(25)\quad U = \pm\begin{bmatrix} \alpha_{11} & \gamma_{11} & 0 & \gamma_{12} \\ 0 & \alpha_{11}^{-1} & 0 & 0 \\ 0 & \alpha_{11}^{-1}\alpha_{22}\gamma_{12} & \alpha_{22} & \gamma_{22} \\ 0 & 0 & 0 & \alpha_{22}^{-1} \end{bmatrix}, \quad V = \pm\begin{bmatrix} 0 & \alpha_{21}^{-1}\alpha_{12}\gamma_{22} & \alpha_{12} & \gamma_{12} \\ 0 & 0 & 0 & \alpha_{12}^{-1} \\ \alpha_{21} & \gamma_{21} & 0 & \gamma_{22} \\ 0 & \alpha_{21}^{-1} & 0 & 0 \end{bmatrix}.$$

Proceeding as in § 4 with $a = c = 0$, we find that $A_2 = -k\beta_{11}^2 - \gamma\beta_{12}^2 = 0$ for every k and γ requires that $\beta_{11} = \beta_{12} = 0$. Then $B_2 = 1$, $C_2 = 0$, $D_2 = 0$, identically. Proceeding as in § 16, with also $c = 0$, we have

$$B = -k\beta_{21}^2 - \gamma\beta_{22}^2, \qquad C = k\alpha_{11}\alpha_{21} + \gamma\alpha_{12}\alpha_{22}.$$

Then $B = 0$, $C = 0$, for every k and γ, give $\beta_{21} = \beta_{22} = 0$, $\alpha_{11}\alpha_{21} = \alpha_{12}\alpha_{22} = 0$. Then $A = 0$, $E = 0$, identically. The transformer is thus of the form (19).

If $\alpha_{11} \neq 0$, then

$$\alpha_{21} = 0, \ \alpha_{22} \neq 0, \ \alpha_{12} = 0, \ \delta_{21} = 0, \ \delta_{12} = 0, \ \alpha_{11}\delta_{11} = \alpha_{22}\delta_{22} = 1.$$

If $\alpha_{11} = 0$, then

$$\alpha_{21} \neq 0, \ \alpha_{12} \neq 0, \ \alpha_{22} = 0, \ \delta_{11} = 0, \ \delta_{22} = 0, \ \alpha_{12}\delta_{12} = \alpha_{21}\delta_{21} = 1.$$

The operators U form the group $(K_{p^3}, T_{1,\alpha_{11}} T_{2,\alpha_{22}})$. The operators V are given uniquely by the products UP_{12} [or also by $P_{12}U$].

The types of non-conjugate subgroups of order p^2 in $G_{n=1}$.

20. By § 9, we may confine the discussion to the subgroups of H_{p^3}, G_{p^3} and K_{p^3}. Each of these three groups has the self-conjugate subgroup K_{p^2}. By § 11 the only additional subgroups of order p^2 in H_{p^3} are, for $p > 3$, the p non-cyclic groups $H_{p^2}^{a_j c}$, with $a \neq 0$, and, for $p = 3$, 3 cyclic groups of order 9. The latter are all conjugate within G_{25920}, each being self-conjugate only in a group of order 27.* *Hence these cyclic groups are all conjugate and each is self-conjugate only under the group H_{27}.*

Now $[p, q, r, s]$ transforms $[k, \rho a, \delta, \rho a]$ into $[k', \rho a, c', \rho a]$, where $c' = \delta + \rho q a - \rho s a$. For the groups† (16), $a \neq 0$, $\delta = \rho c + \frac{1}{2}\rho(\rho - 1)a^2$. Taking $s = 0$, $q = -c/a$, we have $c' = \frac{1}{2}\rho(\rho - 1)a^2$. *Hence the groups $H_{p^2}^{a_j c}$, $a \neq 0$ are all conjugate with*

$$(16') \quad H_{p^2}^{a_j 0} = \{[k, \rho a, \tfrac{1}{2}\rho(\rho - 1)a^2, \rho a], (k, \rho = 0, 1, \cdots, p - 1)\}.$$

To find the group transforming (16′) into itself, we proceed as in § 4 and find that the transformer must be of the form (7) with $\beta_{22} = 0$. The latter transforms the general operator of (16′) into $[k', \rho a \alpha_{11}\delta_{22}, c', \rho a \alpha_{22}^2]$, where

$$c' = \tfrac{1}{2}\rho(\rho - 1)a^2\alpha_{11}\alpha_{22} - \rho a \alpha_{11}\gamma_{22} + \rho a \alpha_{12}\alpha_{22}.$$

Hence must $\alpha_{11}\delta_{22} = \alpha_{22}^2$, $c' = \frac{1}{2}\rho\alpha_{22}^2(\rho\alpha_{22}^2 - 1)a^2$. Since $\alpha_{22}\delta_{22} = 1$, we get

$$\alpha_{11} = \alpha_{22}^3, \quad -\tfrac{1}{2}a\alpha_{22}^2 = -\alpha_{11}\gamma_{22} + \alpha_{12}\alpha_{22} - \tfrac{1}{2}a\alpha_{11}\alpha_{22}.$$

Hence (16′) *is self-conjugate only under a subgroup of order $\frac{1}{2}p^3(p - 1)$ of $G_{n=1}$.*

The group G_{p^3} contains in addition to K_{p^2} only the p groups (17) with $a \neq 0$. Transforming $[k, ra, rc, 0]$ by the general operator (7) of the largest subgroup in which G_{p^3} is self-conjugate, we obtain $[k', ra', rc', 0]$, where

$$a' = a\alpha_{11}\delta_{22} - c\alpha_{11}\beta_{22}, \qquad c' = c\alpha_{11}\alpha_{22} - a\alpha_{11}\gamma_{22}, \qquad \alpha_{22}\delta_{22} - \beta_{22}\gamma_{22} = 1.$$

Since $a \neq 0$, we can determine α_{22}, β_{22}, γ_{22}, δ_{22} so that these three conditions are satisfied, whatever be the values, not both zero, of a' and c'. Thus

$$\delta_{22} = (a' + c\alpha_{11}\beta_{22})/a\alpha_{11}. \qquad \gamma_{22} = (c\alpha_{11}\alpha_{22} - c')/a\alpha_{11}$$

*Transactions, vol. 2 (1901), p. 138. This also follows from the discussion of (16′).

† We now write ρ instead of r, to avoid confusion with the new r.

from the first two, so that the third reduces to $a'\alpha_{22} + c'\beta_{22} = a\alpha_{11}$. Each of the groups is therefore conjugate with $\{[k', 0, rc', 0], (k', r = 0, 1, \cdots, p-1)\}$. *Hence the* $p+1$ *subgroups of order* p^2 *of* G_{p^3} *are conjugate within* $G_{n=1}$.

Finally, the p^2+p+1 subgroups of order p^2 of K_{p^3} are conjugate with K_{p^2}, $K_{p^2}^{*}$ or $K_{p^2}^{**} = \{[\sigma\gamma, 0, c, \gamma]\}$, the latter being conjugate with neither of the first two (§ 17). Since these groups are self-conjugate only under subgroups of orders $\frac{1}{2}p^4(p-1)^2$, $p^3(p-1)^2$, $p^3(p^2-1)$, respectively (§§ 17–19), while for (16′) the order is $\frac{1}{2}p^3(p-1)$, no two of these four groups are conjugate.

THEOREM. *For* $p \geqq 3$, *there are exactly four types of non-conjugate subgroups of order* p^2 *of the group* $G_{n=1}$.

THE UNIVERSITY OF CHICAGO, *June* 22, 1903.