# THE MINIMUM DEGREE $\tau$ OF RESOLVENTS FOR THE $p$-SECTION OF THE PERIODS OF HYPERELLIPTIC FUNCTIONS OF FOUR PERIODS*

BY

LEONARD EUGENE DICKSON†

## *Introduction.*

The chief object of the investigation‡ is to prove that, if $p > 3$,

$$\tau = (p^4 - 1)/(p - 1).$$

The case $p = 3$ alone is exceptional, the problem then being equivalent to that of the 27 lines on a general cubic surface. On the final page of his *Traité*,§ JORDAN states that he had established the theorem for $p = 5$, by methods analogous to those used in his complicated discussion for $p = 3$, and says "mais ici la complication est beaucoup plus grande."

It is rather remarkable that the minimum $\tau$ should be so large as $p^3 + p^2 + p + 1$, since the fractional form of the general quaternary linear group modulo $p$ can be represented as a substitution group of this degree (and of no lower in view of the present theorem).

The paper makes considerable headway in the problem of all the subgroups of the quaternary abelian group modulo $p$, which plays the same rôle in the hyperelliptic modular theory (as yet but little developed) as the binary congruence group plays in the classic elliptic modular theory.

## *Properties of three maximal subgroups of $SA(4, p^n)$.*

1. We consider special abelian ‖ transformations of the three types

* Presented to the Society (Chicago), December 30, 1904. Received for publication November 17, 1904.

† Of the Carnegie Institution of Washington.

‡ A sequel to my series of articles in these Transactions. Occasional reference to them is made by Roman numerals as in the list in the paper, *Determination of all the subgroups of the known simple group of order* 25920, in vol. 5 (1904), p. 127.

§ Note *E*, p. 667. Also in Comptes Rendus (1870), p. 1028.

‖ The abelian conditions on $(1)_1$ and $(1)_2$ are given by (7) of $II_{374}$ and (19) of $II_{380}$, respectively. The sign $\pm$ preceding the matrices in II is now to be omitted.

$$(1)\quad \begin{Bmatrix} \alpha_{11} & \gamma_{11} & \alpha_{12} & \gamma_{12} \\ 0 & \alpha_{11}^{-1} & 0 & 0 \\ 0 & \gamma_{21} & \alpha_{22} & \gamma_{22} \\ 0 & \delta_{21} & \beta_{22} & \delta_{22} \end{Bmatrix}, \quad \begin{Bmatrix} \alpha_{11} & \gamma_{11} & \alpha_{12} & \gamma_{12} \\ 0 & \delta_{11} & 0 & \delta_{12} \\ \alpha_{21} & \gamma_{21} & \alpha_{22} & \gamma_{22} \\ 0 & \delta_{21} & 0 & \delta_{22} \end{Bmatrix}, \quad \begin{Bmatrix} \alpha_{11} & \gamma_{11} & 0 & 0 \\ \beta_{11} & \delta_{11} & 0 & 0 \\ 0 & 0 & \alpha_{22} & \gamma_{22} \\ 0 & 0 & \beta_{22} & \delta_{22} \end{Bmatrix}.$$

Those of type $(1)_1$ form a group $G_\omega$ of order $\omega = (p^{2n}-1)(p^n-1)p^{4n}$. The operators with $\alpha_{11}=1$ form a subgroup $G_{\omega'}$ of order $\omega' = (p^{2n}-1)p^{4n}$. Next, the operators of type $(1)_2$ form a group $H_\omega$; those with $\alpha_{11}\alpha_{22}-\alpha_{12}\alpha_{21}=1$ form a subgroup $H_{\omega'}$. Finally, there are $\{(p^{2n}-1)p^n\}^2$ operators $(1)_3$ with

$$(2)\qquad \alpha_{11}\delta_{11}-\beta_{11}\gamma_{11}=1, \qquad \alpha_{22}\delta_{22}-\beta_{22}\gamma_{22}=1.$$

These and their products by $P_{12}=(\xi_1\xi_2)(\eta_1\eta_2)$ form a group $K_\pi$, $\pi = 2(p^{2n}-1)^2p^{2n}$. A subgroup $K_{\pi'}$, $\pi' = (p^{2n}-1)p^{2n}$ is formed of the operators

$$(3)\quad \xi_1' = \xi_1+\gamma_{11}\eta_1, \qquad \eta_1'=\eta_1, \qquad \xi_2' = \alpha_{22}\xi_2+\gamma_{22}\eta_2, \qquad \eta_2' = \beta_{22}\xi_2+\delta_{22}\eta_2.$$

2. Theorem. *If a subgroup of $SA(4,p^n)$ contains $G_{\omega'}$, it lies in $G_\omega$. In particular, $G_\omega$ is a maximal subgroup.*

We extend $G_{\omega'}$ by a transformation $S$ of $SA(4,p^n)$, not in $G_\omega$, and prove that the group obtained is $SA(4,p^n)$. Give to $S$ the notation (1) of $\mathrm{II}_{372}$. By hypothesis, $\beta_{11}$, $\beta_{12}$, $\delta_{12}$ are not all zero. We may assume that $\beta_{11}$ and $\beta_{12}$ are not both zero, otherwise $M_2S$ has $\beta_{12}' = -\delta_{12} \neq 0$, while $M_2$ lies in $G_\omega$.

Let first $\beta_{11}=0$, $\beta_{12}\neq 0$. Employing $S^{-1}$ if necessary, we may take $\beta_{11}=0$, $\beta_{21}\neq 0$. Then $S' \equiv SN_{1,2,\rho}$, where $\alpha_{11}+\rho\beta_{21}=1$, is of the form $S$ with $\alpha_{11}=1$, $\beta_{11}=0$, $\beta_{21}\neq 0$. Now $G_{\omega'}$ contains a transformation $T$ which leaves $\eta_1$ fixed and replaces $\xi_1$ by the same function $\xi_1+\cdots$ that $S'$ does. Then $S_1 \equiv T^{-1}S'$ leaves $\xi_1$ fixed and has $\beta_{11}=0$. The abelian conditions give

$$\delta_{11}=1, \qquad \gamma_{21}=\delta_{21}=0, \qquad \alpha_{22}\delta_{22}-\beta_{22}\gamma_{22}=1.$$

The product $S_2 \equiv S_1U^{-1}$, where $U = \left(\begin{smallmatrix}\alpha_{22} & \gamma_{22}\\ \beta_{22} & \delta_{22}\end{smallmatrix}\right)$ on $\xi_2$ and $\eta_2$, is

$$\xi_1'=\xi_1, \qquad \eta_1' = \eta_1+\beta_{12}\xi_2+\delta_{12}\eta_2, \qquad \xi_2'=\xi_2+\alpha_{21}\xi_1, \qquad \eta_2'=\eta_2+\beta_{21}\xi_1.$$

By the hypothesis on $S$, $S_2$ is not in $G_\omega$, so that $\beta_{12}$ and $\delta_{12}$ are not both zero. Now $G_{\omega'}$ contains an operator $V$ which leaves $\xi_1$ and $\eta_1$ unaltered and replaces $\xi_2$ by $-\kappa^{-1}(\beta_{12}\xi_2+\delta_{12}\eta_2)$, where $\kappa$ is any mark $\neq 0$. Then $V^{-1}S_2V = R_{1,2,\kappa}$. Now $M_1^{-1}$ transforms the latter into $Q_{2,1,\kappa}$. But $G_{\omega'}$ contains $Q_{1,2,\kappa}$. Hence we reach

$$(4)\qquad P_{12} = Q_{2,1,1}^{-1}Q_{1,2,1}Q_{2,1,1}^{-1}T_{2,-1}, \qquad M_1 = P_{12}M_2P_{12},$$

and hence (*Linear Groups*, p. 92) all the generators of $SA\ (4, p^n)$.

Let next $\beta_{11} \neq 0$. Then $S' \equiv N_{1,2,-\delta_{12}\beta_{11}^{-1}} Q_{1,2,-\beta_{12}\beta_{11}^{-1}} S$ replaces $\eta_1$ by $\beta_{-1}\xi_1 + \delta\eta_1$. Then $S_1 \equiv L_{1,-\delta\beta_{11}^{-1}} S'$ replaces $\eta_1$ by $\beta_{11}\xi_1$. For $S_1$,

$$\gamma_{11} = -\beta_{11}^{-1}, \qquad \gamma_{21} = 0, \qquad \delta_{21} = 0, \qquad \alpha_{22}\delta_{22} - \beta_{22}\gamma_{22} = 1,$$

by certain abelian conditions. Then $S_2 \equiv S_1 U^{-1}$, $U$ as above, is

$$\xi_1' = \alpha_{11}\xi_1 - \beta_{11}^{-1}\eta_1 + \alpha_{12}\xi_2 + \gamma_{12}\eta_2, \qquad \eta_1' = \beta_{11}\xi_1, \qquad \xi_2' = \xi_2 + \alpha_{21}\xi_1,$$
$$\eta_2' = \eta_2 + \beta_{21}\xi_1.$$

Then $S_3 \equiv S_2 N_{1,2,-\gamma_{12}} Q_{1,2,-\alpha_{12}}$ is of the form

$$\xi_1' = \alpha\xi_1 - \beta_{11}^{-1}\eta_1, \qquad \eta_1' = \beta_{11}\xi_1, \qquad \xi_2' = \xi_2, \qquad \eta_2' = \eta_2.$$

Then $S_4 \equiv S_3 L_{1,-\alpha\beta_{11}^{-1}}$ is of the form $S_3$ with $\alpha = 0$. Now $S_4$ transforms $L_{1,\lambda}$ into $L'_{1,-\lambda\beta_{11}^2}$. Hence we reach every $L'_{1,\rho}$ and hence $M_1 = L'_{1,-1} L_{1,1} L'_{1,-1}$.

3. THEOREM. *If a subgroup of* $SA(4, p^n)$ *contains* $H_{\omega'}$, *it lies in* $H_\omega$. *In particular,* $H_\omega$ *is a maximal subgroup.*

I omit the proof, which is of the same character as that of § 2.

4. THEOREM. *If, for* $p > 2$, *a subgroup of* $SA(4, p^n)$ *contains* $K_{\pi'}$, *it lies in* $K_\pi$ *or* $G_\omega$. *In particular,* $K_\pi$ *is a maximal subgroup.**

We extend $K_{\pi'}$ by a transformation $S$ of $SA(4, p^n)$, lying in neither $K_\pi$ nor $G_\omega$, and prove that the group obtained is $SA(4, p^n)$. Giving $S$ the notation (1) of $\text{II}_{372}$, we have $\alpha_{12}, \gamma_{12}, \beta_{12}, \delta_{12}$ not all zero, since $S$ does not lie in $K_\pi$.

Applying $L_{1,\lambda}$ on the right, we may suppose that $\alpha_{12}$ and $\gamma_{12}$ are not both zero. We may take $\alpha_{12} \neq 0$, applying $M_2$ on the left if necessary. Finally, applying $T_{2,\rho} L_{2,\sigma}$ on the left, we may take $\alpha_{12} = 1$, $\gamma_{12} = 0$.

Case ($a$). Let $\delta_{12} = 0$. Then $(2)_2$ holds. Then $SU^{-1}$, where $U = \begin{pmatrix} \alpha_{22} & \gamma_{22} \\ \beta_{22} & \delta_{22} \end{pmatrix}$ on $\xi_2$ and $\eta_2$, becomes $S_1$ in view of abelian conditions $C_{14}$, $C_{24}$:

$$(5) \qquad S_1 = \begin{vmatrix} \alpha_{11} & \gamma_{11} & 1 & 0 \\ \beta_{11} & \delta_{11} & \beta_{12} & 0 \\ 0 & 0 & 1 & 0 \\ \beta_{21} & \delta_{21} & 0 & 1 \end{vmatrix}, \qquad W = \begin{vmatrix} \alpha & \gamma & 0 & 0 \\ \beta & \delta & 1 & 0 \\ 0 & 0 & 1 & 0 \\ \alpha & \gamma & 0 & 1 \end{vmatrix}$$

Since $S_1$ does not lie in $G_\omega$, $\beta_{11}$ and $\beta_{12}$ are not both zero.

Let first $\beta_{12} \neq 0$ in $S_1$. Then $T_{2,\beta_{12}}^{-1} S_1 L_{1,-\beta_{12}^{-1}} T_{2,\beta_{12}}$ is the form $W$. Then for any $\lambda \neq 0$, $W^{-1} T_{2,\lambda} W T_{2,\lambda}^{-1} = R_{1,2,1-\lambda}$. Transforming by $T_{2,\rho}$ and $M_2^{-1}$, we reach every $R_{1,2,\mu}$ and $Q_{2,1,\mu}$, if $p^n > 2$. Then† we reach $N_{1,2,\mu}$ and its

* The latter is true also for $p = 2$.

†*Linear Groups*, p. 97, formula (83) for $i = 2, j = 1$.

transform $Q_{1,2,-\mu}$ by $M_2$. Applying (4), we obtain the remaining generators of $SA(4, p^n)$.

Let next $\beta_{12} = 0$, $\beta_{11} \neq 0$, in $S_1$. Then $\beta_{21} = -\beta_{11}$, $\delta_{21} = -\delta_{11}$ by abelian conditions $C_{13}$ and $C_{23}$. Then $L_{1,-\delta_{11}\beta_{11}^{-1}} S_1 L_{1,-\alpha_{11}\beta_{11}^{-1}}$ is $Z$:

$$(6) \quad Z = \begin{bmatrix} 0 & -\beta_{11}^{-1} & 1 & 0 \\ \beta_{11} & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -\beta_{11} & 0 & 0 & 1 \end{bmatrix}, \qquad V = \begin{bmatrix} \alpha_{11} & \gamma_{11} & 1 & 0 \\ \beta_{11} & \delta_{11} & 0 & \delta_{12} \\ \alpha_{21} & \gamma_{21} & 1 & 0 \\ -\beta_{11} & -\delta_{11} & 0 & \delta_{22} \end{bmatrix}$$

$(\delta_{12} \neq 0,\ \delta_{12} + \delta_{22} = 1.)$

Then if $\gamma \neq 0$, $Z^{-1} T_{2,\lambda} Z T_{2,\lambda}^{-1} = Q_{1,2,\lambda-1}$. If $p > 2$, we reach every $Q_{1,2,\tau}$. Then

$$ZQ_{1,2,-1}:\ \xi_1' = -\beta_{11}^{-1}\eta_1,\ \eta_1' = \beta_{11}\xi_1,\ \xi_2' = \xi_2,\ \eta_2' = \eta_2$$

transforms $L_{1,\rho}$ into $L'_{1,-\rho\beta_{11}^2}$. We thus reach every transformation of determinant unity on $\xi_1$ and $\eta_1$, and then $SA(4, p^n)$.

Case ($b$). Let next $\delta_{12} \neq 0$. Applying $L'_{2,\rho}$ on the left we may make $\beta_{12} = 0$. We thus have a transformation $S'$ with $\alpha_{12} = 1$, $\gamma_{12} = 0$, $\beta_{12} = 0$, $\delta_{12} \neq 0$. Since $S'$ is not in $K_\pi$, $\alpha_{22}$, $\gamma_{22}$, $\beta_{22}$, $\delta_{22}$ are not all zero. Applying $M_2$ on the right, we may assume that $\alpha_{22}$ and $\gamma_{22}$ are not both zero in $S'$.

($b_1$). Let first $\alpha_{22} \neq 0$. We may set $\alpha_{22} = 1$ by multiplying by $T_{2,\alpha_{22}}^{-1}$ on the right. Then $V = L_{2,-\gamma_{22}} S' L_{1,\gamma_{22}\delta_{12}^{-1}} L'_{2,-\beta_{22}}$ is of the form $(6)_2$.

If $\alpha_{21} \neq 0$ in $V$, then $V_1 = L_{1,-\gamma_{21}\alpha_{21}^{-1}} V$ has $\gamma_{21} = 0$, $\gamma_{11} = 0$. Then $V_1^{-1} L'_{2,-\rho} V_1 L'_{2,\rho}$ is $Z_t$, with $t = \rho - \rho\delta_{22}^2$:

$$(7) \quad Z_t = \begin{bmatrix} 1 & 0 & 0 & 0 \\ -\rho\delta_{12}^2 & 1 & -\rho\delta_{12}\delta_{22} & 0 \\ 0 & 0 & 1 & 0 \\ -\rho\delta_{12}\delta_{22} & 0 & t & 1 \end{bmatrix}, \qquad X = \begin{bmatrix} \alpha & \gamma & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & \gamma \\ 0 & 1 & 0 & -\alpha \end{bmatrix}.$$

Then $Z_t L'_{2,-t} = Z_0$. For $\delta_{22} \neq 0$, $Z_0$ with $\rho = -\delta_{12}^{-1}\delta_{22}^{-1}$ is of the earlier type $(5)_2$. For $\delta_{22} = 0$, $Z_0 = L'_{1,-\rho}$ and $\delta_{12} = 1$, $\alpha_{11} = 0$, $\delta_{11} = -\alpha_{21}^{-1}$ in $V_1$. Then

$$V_2 \equiv L'_{1,\beta_{11}\alpha} V_1 T_{2,\alpha^{-1}}:\ \xi_1' = \xi_2,\ \eta_1' = \eta_2 - \alpha^{-1}\eta_1,\ \xi_2' = \xi_1 + \alpha^{-1}\xi_2,\ \eta_2' = \eta_1.$$

Then $(V_2^{-1} T_{2,-1} V_2 T_{2,-1})^2 = Q_{2,1,-4\alpha^{-1}}$. We thus reach $SA(4, p^n)$.

If $\alpha_{21} = 0$ in $V$, then $\alpha_{11} = 0$ by abelian condition $C_{14}$. Applying $L_{1,\rho}$ on the left, we may set $\delta_{11} = 0$. Then $L_{2,-\delta_{11}} V L_{1,\delta_{22}\delta_{21}^{-1}} L_{2,1}$ is of the form $(6)_2$ with $\alpha'_{21} = -\beta_{11} \neq 0$.

($b_2$). Let finally $\alpha_{22} = 0$, $\gamma_{22} \neq 0$ in $S'$. We may set $\beta_{22} = 0$, since otherwise $S' L_{2,1}$ is of the form $S'$ with $\alpha_{22} \neq 0$. Applying on the right the inverse of $\left(\begin{smallmatrix}\alpha_{21} & \gamma_{21}\\ \beta_{21} & \delta_{21}\end{smallmatrix}\right)$ on $\xi_2$ and $\eta_2$, we reach $(7)_2$, in view of the abelian conditions. If $\alpha=\gamma=0$, $X=P_{12}$ would belong to $K_\pi$. If $\alpha\neq 0$, $X^{-1}$ is of the form $S'$ with $\alpha_{22}\neq 0$. Hence we may set $\alpha=0$, $\gamma\neq 0$. Then $X^2=N_{1,2,2\gamma}$. If $p>2$, we reach every $N_{1,2,\rho}$. Now $XN_{1,2,-\gamma}=P_{12}$. Hence we reach the generators of $SA(4,p^n)$.

*The subgroups of order a power of p.*

5. Consider the subgroup $G_{p^{4n}}$ of the operators $S=[k,a,c,d]$ defined by (3) of $\text{II}_{372}$. Let $\Sigma=[\kappa,\alpha,\gamma,\delta]$. Then the commutator $S^{-1}\Sigma^{-1}S\Sigma$ is

$$(8)\qquad [k',0,c',0]\quad (k'=2\alpha c-2\gamma a+\alpha^2 d-a^2\delta,\ c'=\alpha d-a\delta).$$

If $p>2$, we may make $k'$ and $c'$ assume arbitrary values in the field by taking $a=-1$, $\alpha=0$, $\delta=c'$, $2\gamma=k'+c'$. If $p=2$, we may make $k'$ and $c'$ assume arbitrary values each $\neq 0$ by taking $\delta=0$, $\alpha=k'/c'$, $d=c'^2/k'$; also we may make $k'=c'=0$. The number of operators thus reached is $(2^n-1)^2+1$, which exceeds $\frac{1}{2}2^{2n}$ if $n>1$, so that they generate $K_{2^{2n}}$ below. If $p=2$, $n=1$, then $k'=c'=\alpha d-a\delta$.

THEOREM. *For $p^n>2$, the commutator subgroup of $G_{p^{4n}}$ is*

$$(9)\qquad K_{p^{2n}}=\{[k,0,c,0],\ k,c\ \textit{arbitrary}\};$$

*for $p^n=2$ it is the group of the two operators $[k,0,k,0]$, $k=0,1$.*

6. It is easily shown that if the $p$th power of every operator of a group $G_{p^a}$ belongs to its commutator subgroup $G_{p^b}$, there are exactly $(p^{a-b}-1)/(p-1)$ subgroups of order $p^{a-1}$ in $G_{p^a}$.

For $G_{p^{4n}}$ the condition is satisfied. Hence the number of its subgroups of order $p^{4n-1}$ is $(p^{2n}-1)/(p-1)$ if $p^n>2$, and 7 if $p^n=2$.

When a subgroup $G_{p^{4n}}$ can be defined by certain independent relations $f_1=0,\cdots,f_r=0$ between the coefficients $k,a,c,d$ of $S$, we denote it $\{f_1=0,\cdots,f_r=0\}$. Thus (9) is denoted $\{a=0,d=0\}$.

*For $p>2$, $n=1$, the $p+1$ subgroups of order $p^3$ of $G_{p^4}$ are*

$$(10)\qquad \{d=0\},\qquad \{a=td\}\qquad (t=0,1,\cdots,p-1).$$

7. The group $\{a=0\}$ is commutative of type $(1,1,1)$ and hence has $p^2+p+1$ subgroups of order $p^2$. As in §5, it follows that, for $p>2$, the commutator group of either $\{d=0\}$ or $\{a=td\}$, $t\neq 0$, is formed of the operators $[k,0,0,0]$, and contains the $p$th power of every $S$. Hence either group has exactly $p+1$ subgroups of order $p^2$. They are seen to be the ones given in the following table:

| Order $p^3$. | Subgroups of order $p^2$. |
|---|---|
| $\{d=0\}$ | $\{d=0,\ a=0\}$, $\{d=0,\ c=sa\}$, |
| $\{a=td\}$, $t \neq 0$ | $\{a=0,\ d=0\}$, $\{a=td,\ c=sd+\frac{1}{2}td^2\}$, |
| $\{a=0\}$ | $\{a=0,\ d=0\}$, $\{a=0,\ c=sd\}$, $\{a=0,\ k=rc+sd\}$ |

where $r$ and $s$ take independently the values $0, 1, \cdots, p-1$.

Now $T_{1,t^{-1}}$ transforms $\{a=td\}$, $t \neq 0$, into $\{a=d\}$. The $2p^2+p+1$ distinct subgroups of order $p^2$ of $G_{p^4}$ are found to be conjugate within $SA(4,p)$ with the four types* in the 5th–8th rows of the table of § 8.

8. In the following table is given in the first column a representative of each set of subgroups of $G_{p^4}$ conjugate within $SA(4,p)$, $p>2$; in the second column the largest subgroup of $SA(4,p)$ transforming into itself the representative.

| | |
|---|---|
| $G_{p^4}$ | $G_{p^4}$, $T_{1,\alpha_{11}}T_{,\alpha_{22}}$ |
| $\{a=0\}$ | $H_\omega$ of operators $(1)_2$ |
| $\{d=0\}$ | $G_\omega$ of operators $(1)_1$ |
| $\{a=d\}$ | $G_{p^4}$, $T_{1,\alpha^3}T_{2,\alpha}$ |
| $\{a=d=0\}$ | $G_{p^4}$, $T_{1,\alpha_{11}}T_{2,\alpha_{22}}$ |
| $\{a=c=0\}$ | $\{a=0\}$, $T_{1,\alpha_{11}}T_{2,\alpha_{22}}$, $P_{12}$ |
| $\{a=0,\ k=\nu d\}$ | $2p^3(p^2-1)$ operators $(11)_1$ |
| $\{a=d,\ c=\frac{1}{2}d^2\}$ | $\{a=d\}$, $T_{1,\alpha^3}T_{2,\alpha}$ |
| $(L_{11})$ | $G_\omega$ of operators $(1)_1$ |
| $(L_{1\mu}L_{21})$ | $(p\mp\epsilon)(p-1)p^3$ operators $(11)_2$ |
| $(B)$ if $p>3$ | $\left[\gamma,\ \alpha,\ \frac{\alpha+\alpha^2}{2},\ \alpha\right]$, $T_{1,s^3}T_{2,s}\left[0,\ 0,\ \frac{s^4-1}{12},\ \frac{s^2-1}{2}\right]$ |

where $\nu$ is a particular not-square, $\mu=1$ or $\nu$, $B=[0,-1,0,-1]$, and $\epsilon=\pm 1$ according as $p=4l\pm 1$, and where

$$(11)\quad \begin{pmatrix} \pm\alpha_{22} & \gamma_{11} & \pm\nu\alpha_{21} & \gamma_{12} \\ 0 & \alpha_{22}/\Delta & 0 & -\alpha_{21}/\Delta \\ \alpha_{21} & \gamma_{21} & \alpha_{22} & \gamma_{22} \\ 0 & \mp\nu\alpha_{21}/\Delta & 0 & \pm\alpha_{22}/\Delta \end{pmatrix},\quad \begin{pmatrix} \alpha_{11} & \gamma_{11} & \alpha_{12} & \gamma_{12} \\ 0 & t^{-1}\alpha_{11} & 0 & t^{-1}\mu^{-1}\alpha_{12} \\ \mp\mu^{-1}\alpha_{12} & \gamma_{21} & \pm\alpha_{11} & \gamma_{22} \\ 0 & \mp t^{-1}\alpha_{12} & 0 & \pm t^{-1}\alpha_{11} \end{pmatrix}$$

$$\Delta=\pm(\alpha_{22}^2-\nu\alpha_{21}^2)\neq 0,\quad t=\alpha_{11}^2+\mu^{-1}\alpha_{12}^2\neq 0.$$

* These correspond to $K_{p^2}$, $K_{p^2}^{*}$, $K_{p^2}^{**}$, and (16′), respectively of II. The types of period $p$ are taken from I; the transform of $A_1$ of $I_{112}$ by $M_1M_2T_{1,-1}$ gives $B$.

*General plan of the subsequent investigation.*

9. Let $H$ be a subgroup of order $p^i N$ of $SA(4, p)$, $i > 0$, $N$ prime to $p$, $p > 2$. Applying a suitable transformation within $SA(4, p)$, we may assume that $H$ contains a subgroup $G_{p^i}$ lying in the $G_{p^4}$ of §§ 5–7. If $H$ contains $G_{p^i}$ self-conjugately, $H$ lies in one of the groups in the second column of the table in § 8, and hence lies in $G_\omega$, $H_\omega$, or $(G_{p^4}, T_{1,\alpha_{11}} T_{2,\alpha_{22}})$. In this case the determination of $H$ depends upon the determination* of all subgroups of the binary linear-homogeneous group of determinant unity. Suppose next that $G_{p^i}$ is not self-conjugate in $H$. Let $p^m$ be the maximal order of a subgroup common to $G_{p^i}$ and any of its conjugates under $H$; let $G_{p^m}$ be such a subgroup. By a theorem † discovered independently by BURNSIDE and FROBENIUS, $H$ must contain an operator $S$, of period prime to $p$, commutative with $G_{p^m}$ but not with $G_{p^i}$.

Now, if $p > 2$, $(p^4 - 1)(p^2 - 1)$ has no factor of the form $1 + p^3 x$, $x > 0$. For if so, call the quotient $q$. Then $0 < q < p^3$, $-p^2 + 1 \equiv q \pmod{p^3}$. Hence $q = p^3 - p^2 + 1$. But the latter is relatively prime to $(p^2 - 1)^2$, and exceeds $p^2 + 1$ if $p > 2$. Hence the number of conjugates to $G_{p^i}$ in $H$ is not $\equiv 1 \pmod{p^3}$, so that ‡ $m \geqq i - 2$. *We may set $m = i - 1$ or $i - 2$.*

10. LEMMA. *Any binary transformation $B = \left(\begin{smallmatrix} \alpha & \gamma \\ \beta & \delta \end{smallmatrix}\right)$, $\beta \neq 0$, together with all the $S_\lambda = \left(\begin{smallmatrix} 1 & \lambda \\ 0 & 1 \end{smallmatrix}\right)$ generate every binary transformation of determinant unity.*

Indeed, $S_{-\delta\beta^{-1}} B S_{-\alpha\beta^{-1}} = \left(\begin{smallmatrix} 0 & \tau \\ \beta & 0 \end{smallmatrix}\right)$, where $\tau = -\beta^{-1}(\alpha\delta - \beta\gamma) \neq 0$. The latter operator transforms $S_\lambda$ into $\left(\begin{smallmatrix} 1 & 0 \\ \sigma & 1 \end{smallmatrix}\right)$, where $\sigma = \lambda\beta\tau^{-1}$ may be made arbitrary.

*The subgroups $H$ of order $p^4 N$, $p > 2$.*

11. Now $i = 4$, $m = 3$ or $2$ in § 9. For $m = 3$, we may take $G_{p^m}$ to be $\{a = 0\}$ or $\{d = 0\}$, since every operator commutative with $\{a = d\}$ lies in $(G_{p^4}, T_{1\alpha^3} T_{2,\alpha})$ and hence is commutative with $G_{p^4}$ (§ 8).

For $\{d = 0\}$, $S$ is of the form $(1)_1$. Then $\beta_{22} \neq 0$ since $S$ is not commutative with $G_{p^4}$. The quotient-group § $G_\omega / \{d = 0\}$ may be taken concretely as the group of the products $T_{1,\alpha_{11}} U$, $U$ a binary transformation of determinant unity on $\xi_2$ and $\eta_2$. Also, $G_{p^4}/\{d = 0\}$ is $(L_{2,\gamma})$. Then, by § 10, we reach every $U$. These, with $G_{p^4}$, generate $G_{\omega'}$. Hence, by § 2, $H$ is a subgroup of $G_\omega$.

For $\{a = 0\}$, $S$ is of the form $(1)_2$, with $\alpha_{21} \neq 0$. The quotient-groups

* This has been done by the writer for any Galois field.

† References in BURNSIDE's *Theory of Groups*, p. 97.

‡ Compare, for example, BURNSIDE's *Theory of Groups*, p. 94, Cor. II.

§ Bulletin of the American Mathematical Society, vol. 10 (1904), pp. 178–184.

$$\frac{H_\omega}{\{a=0\}} = \begin{bmatrix} \alpha_{11} & 0 & \alpha_{12} & 0 \\ 0 & \alpha_{22}/\Delta & 0 & -\alpha_{21}/\Delta \\ \alpha_{21} & 0 & \alpha_{22} & 0 \\ 0 & -\alpha_{12}/\Delta & 0 & \alpha_{11}/\Delta \end{bmatrix}, \qquad \frac{G_{p^4}}{\{a=0\}} = \begin{bmatrix} 1 & 0 & a & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -a & 0 & 1 \end{bmatrix},$$

where $\Delta = \alpha_{11}\alpha_{22} - \alpha_{12}\alpha_{21}$, are simply isomorphic with the binary groups

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix}, \qquad \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}.$$

Hence, in view of § 10 and § 3, $H$ is a subgroup of $H_\omega$.

12. Let next $i = 4$, $m = 2$. Then, by § 8, $G_{p^2}$ is neither $\{a = d = 0\}$ nor $\{a = d,\ c = \frac{1}{2}d^2\}$. If $G_{p^2}$ is $\{a = c = 0\}$, $S = S_1 P_{12}$, where $S_1$ lies in $\{a = 0\}$ extended by $T_{1,\alpha_1}$, $T_{2,\alpha_2}$, so that $S_1$ transforms $G_{p^4}$ into itself. But $G_{p^4}$ and its transform by $P_{12}$ have $\{a = 0\}$ in common, in contradiction with $m = 2$. Finally, let $G_{p^2}$ be $\{a = 0,\ k = \nu d\}$, so that $S$ is of the form $(11)_1$. Now the general quaternary abelian operator with every $\beta_{ij} = 0$ transforms $[k, a, c, d]$ into an operator of the form $(1)_2$, written in capital letters, with

$$A_{ij} = \tau_{ij} + a\alpha_{i1}\delta_{j2}, \qquad D_{ij} = \tau_{ij} - a\delta_{i2}\alpha_{j1},$$

$$C_{ij} = k\alpha_{i1}\alpha_{j1} + c\alpha_{i1}\alpha_{j2} + (c - ad)\alpha_{i2}\alpha_{j1} + d\alpha_{i2}\alpha_{j2} - a\alpha_{i1}\gamma_{j2} - a\gamma_{i2}\alpha_{j1},$$

where $\tau_{ij} = 1\ (i = j)$, $\tau_{ij} = 0\ (i \neq j)$. Hence $G_{p^4}$ and its transform by $S$ would have $\{a = 0\}$ in common, in contradiction with $m = 2$.

*The subgroups $H$ of order $p^3 N$, $p > 2$.*

13. Let first $i = 3$, $m = 2$ in § 9. In view of § 8 the only case not immediately excluded is $G_{p^2} = \{a = d = 0\}$, $G_{p^3} = \{a = d\}$. Then $S$ lies in $(G_{p^4}, T_{1,\alpha_{11}} T_{2,\alpha_{22}})$ and hence transforms $\{a = d\}$ into $\{a = \alpha_{11}\alpha_{22}^{-3} d\}$; the latter two generate $G_{p^4}$ in contradiction with $i = 3$.

14. Let $i = 3$, $m = 1$. If $G_p = (L_{1,\mu} L_{2,1})$, then $G_{p^3} = \{a = 0\}$. Since $(11)_2$ is of the form $(1)_2$, this case is excluded by § 8. If $G_p = (B)$, $p$ being $> 3$, then $G_{p^3} = \{a = d\}$; so that (§ 8) any operator commutative with $G$ is commutative with $G_{p^3}$. Let finally $G_p = (L_{1,1})$. Let first $G_{p^3}$ be $\{a = 0\}$, so that $S$ is of the form $(1)_1$ with $\beta_{22} \neq 0$. Then $S$ transforms $[0, 0, 1, 0]$ into $[2\alpha_{11}\alpha_{12}, -\alpha_{11}\beta_{22}, \alpha_{11}\alpha_{22}, 0]$, which extends $G_{p^3}$ to $G_{p^4}$, in contradiction with $i = 3$. The same argument excludes $G_{p^3} = \{a = d\}$. Finally, $G_{p^3} = \{d = 0\}$ is excluded by § 8.

Theorem. *Every subgroup of order $p^3N$ has a self-conjugate $G_{p^3}$ and hence lies in either $G_\omega$ or $H_\omega$.*

*The subgroups $H$ of order $p^2N$, $p > 2$.*

15. Let $i = 2$, $m = 1$. Let first $G_p = (L_{1,1})$, whence $S = (1)_1$. Then $G_{p^2}$ is

$$\{ a = d = 0 \}, \qquad \{ a = c = 0 \}, \qquad \text{or} \qquad \{ a = d,\ c = sd + \tfrac{1}{2}d^2 \}.$$

We may set $s = 0$ by transforming by $[0, 0, -s, 0]$, which is commutative with $(L_{1,1})$. The argument at the end of § 14 excludes $\{ a = d = 0 \}$.

Let $G_{p^2} = \{ a = c = 0 \}$. Now $S$ transforms $[k, 0, 0, \gamma]$ into $\Sigma$, given by the second matrix of $\mathrm{II}_{374}$ when $a = c = 0$. The supposition $\beta_{22} = 0$ contradicts $i = 2$. If $\alpha_{22} \neq 0$, we employ $\Sigma$ for $\gamma = \alpha_{22}^{-1}\beta_{22}^{-1}$. Hence we may set $\beta_{22} \neq 0$, $\alpha_{22} = 0$ in $S$. Then, for $\gamma = -\beta_{22}^{-2}$, $\Sigma L_{1,-k'}$ has the form $L'_{2,1} Q_{1,2,\delta}$. This is transformed into $L'_{2,1} L_{1,\delta^2}$ by $N_{1,2,-\delta}$, which is commutative with $\{ a = c = 0 \}$. Hence $H$ contains $L'_{2,1}$ and $\{ a = c = 0 \}$, which generate $K_{\pi'}$ of § 1. By § 4, $H$ lies in $K_\pi$ or $G_\omega$.

For $G_{p^2} = \{ a = d,\ c = \frac{1}{2}d^2 \}$, a similar argument shows $H$ contains an operator $U_{r,s}$, with $s \neq 0$:

$$U_{r,s} = \begin{pmatrix} 1 & 0 & r & s \\ 0 & 1 & 0 & 0 \\ 0 & s & 1 & 0 \\ 0 & s-r & 1 & 1 \end{pmatrix}, \qquad X = \begin{pmatrix} 1 & 0 & \frac{1}{2} & \frac{1}{2} \\ 0 & 1 & 0 & 0 \\ 0 & -\frac{1}{2} & 0 & 1 \\ 0 & -\frac{3}{2} & -1 & 2 \end{pmatrix}.$$

Now $N_{1,2,-r}$, which is commutative with $G_{p^2}$, transforms $U_{r,s}$ into $L_{1,r^2-rs} U_{0,s}$. Hence, $H$ contains $G_{p^2}$ and $U_{0,s}$. Set $E_d = [0, d, d^2/2, d]$. Then $H$ contains $X \equiv L_{1,2s} U_{0,s}^{-1} E_1 U_{0,s}$ and $Y$, the transform of $E_{-1}$ by $[2, 2, 2, 2]X$. Now $N_{1,2,2}$ transforms $G_{p^2}$ into itself, and $Y$ into $L_{1,27/4} U_{0,1}$. We may thus assume that $H$ contains $G_{p^2}$ and $U_{0,1}$. Then $H$ contains

$$X^{-1} L_{1,\frac{9}{4}} E_{-1} U_{0,1}^{-1} E_1 = [-1, -2, 0, 0],$$

which belongs to $G_{p^4}$, but not to $G_{p^2}$, contrary to $i = 2$.

16. Let next $G_p = (L_{1,\mu} L_{2,1})$. Then $S$ is of the form $(11)_2$, a special case of $(1)_2$. Hence $S$ transforms $\{ a = 0 \}$ into itself. But the only $G_{p^2}$ containing $G_p$ are $\{ a = c = 0 \}$ and $\{ a = 0,\ k = rc + \mu d \}$. Hence $S$ transforms either of these into a subgroup of $G_{p^4}$, in contradiction with $i = 2$.

17. Let finally $G_p = (B)$, $p$ being $> 3$. Then $G_{p^2}$ must be either

$$\{ a = d = 0 \}, \qquad \text{or} \qquad \{ a = d,\ c = \sigma d + \tfrac{1}{2}d^2 \}.$$

The first is excluded by § 8. The second is transformed into itself by any operator of $\{a = d\}$, and into $\{a = d,\ c = s^2\sigma d + \frac{1}{2}d^2\}$ by $T_{1,s^3}T_{2,s}$. Transforming the result by $[0, 0, (s^4 - 1)/12, (s^2 - 1)/2]$, we obtain

$$\{a = d,\ c = [s^2\sigma - \tfrac{1}{2}(s^2 - 1)]d + \tfrac{1}{2}d^2\}.$$

This lies in $G_{p^4}$, in contradiction with $i = 2$.

18. It remains to consider the $H_{p^2N}$ no two of whose subgroups $G_{p^2}$ have in common an operator $\neq I$. Hence the number of conjugate $G_{p^2}$ is $M$, where $M \equiv 1 \pmod{p^2}$. It is readily shown that the only factors of the form $1 + p^2x$ of $\omega = (p^4 - 1)(p^2 - 1)$ are $1$, $p^2 + 1$, $(p^2 - 1)^2$ and $\omega$. Hence if $H$ is of index $< \tau$, where $\tau = (p^4 - 1)/(p - 1)$, we may set $M = p^2 + 1$ or $(p^2 - 1)^2$. The latter case is immediately excluded in view of the orders of the largest subgroups containing a $G_{p^2}$ self-conjugately (§ 8). For $M = p^2 + 1$, $G_{p^2}$ is self-conjugate in a $G_{p^2t}$ within $H$, where $t$ divides $(p^2 - 1)^2$. In fact, $t \leqq 2(p^2 - 1)$ by § 8. Hence, for $p > 3$, $H$ is of index $> \tau$.

19. If a subgroup $H$ of order $pN$ is of index $< \tau$, then $N = \omega$. The details of the exclusion (for $p > 3$) of this isolated case will be omitted, in view of an anticipated treatment of all orders $pN$. In this direction I have shown that any $H_{pN}$ with more than one $C_p$ conjugate with $(L_{1,1})$ may be transformed into the group $\Gamma$ of the binary transformations of determinant unity on $\xi_1$ and $\eta_1$, or else into a direct product of $\Gamma$ and a binary group on $\xi_2$ and $\eta_2$ with no operator of period $p$ (and hence of order $2$, $4d$, $24$, $48$ or $120$).

THE UNIVERSITY OF CHICAGO,
*October* 1, 1904.