Paul Fong
Nagoya Math. J.
Vol. 39 (1970), 39–79

A CHARACTERIZATION OF THE FINITE SIMPLE GROUPS PSp(4,q), G_2(q), D_4^2(q), II

PAUL FONG[1]

Our object in this paper is to prove the following result.

THEOREM. *Let G be a finite group satisfying the following conditions:*

(*) *G has subgroups L_1, L_2 such that $L_1 \simeq SL(2,q_1)$, $L_2 \simeq SL(2,q_2)$, $[L_1, L_2]=1$, $L_1 \cap L_2 = \langle j \rangle$, where j is an involution, and $|C(j) : L_1L_2| = 2$.*

(**) *$C(j) = L_1L_2\langle n \rangle$, where $n^2 = 1$, $L_1^n = L_1$, $L_2^n = L_2$.*

Then $G = C(j)O(G)$, or G is isomorphic to one of the simple groups $G_2(q)$ or $D_4^2(q)$, where $q = min\{q_1, q_2\}$.

The groups $G_2(q)$ are the simple groups of order $q^6(q^6-1)(q^2-1)$ discovered by Dickson [3], [4] in the 1900's. The groups $D_4^2(q)$ are the simple groups of order $q^{12}(q^6-1)(q^2-1)(q^8+q^4+1)$ discovered by Steinberg and Tits [8], [13] in the 1950's. These groups, for q odd, thus take their place among those finite simple groups which can be characterized by the structure of the centralizer of an involution.

Some remarks on the theorem and its proof may be appropriate at this point. Condition (**) can be dropped if G is assumed to be not isomorphic with $PSp(4,q)$, where $q = \min\{q_1, q_2\}$. This is a consequence of [5] (2*A*) and [15]. Moreover, [5] (7*I*) implies that either q_1 and q_2 are equal, or one is the cube of the other, these being in fact the values of the parameters q_1, q_2 in case G is $G_2(q)$ or $D_4^2(q)$. If $(q_1q_2)^3$ is assumed to divide $|G|$, then it is fairly straightforward to construct a subgroup $\tilde{G}$ of G which is isomorphic to $G_2(q)$ or $D_4^2(q)$. This is accomplished by presenting $\tilde{G}$ as a group with a (B,N)-pair in the sense of Tits [12] and imposing a unique multiplication table on B and on N, and hence on $\tilde{G}$. $\tilde{G}$ can then be

Received January 16, 1969.

[1] This research was partially supported by the National Science Foundation grant *GP*-6539.

shown to be equal to G. That $(q_1q_2)^3$ does in fact divide $|G|$ follows from [5], §§5-7 except possibly in the cases $q_1 = q_2 \leqslant 11$. These cases are in fact non-exceptional, so that the theorem does hold without any conditions on q_1 and q_2 other than those imposed by $(*)$.

The group $G_2(3)$ has been characterized by Janko [7] in terms of the centralizer of an involution. $G_2(3)$ has also been characterized in quite different terms by Thompson [11], and a characterization of the groups $G_2(3^n)$ by Gorenstein is along lines of this latter characterization. Also, the groups $G_2(2^n)$ have recently been characterized by Thomas [10] in terms of the centralizer of an involution.

The author wishes to thank the National Science Foundation and the British Research Council for their support of this research, a part of which was done at the University of Warwick Symposium on Group Theory, 1966-1967.

1. We begin with some remarks on representations of $L = SL(2, q)$, where q is a power of an odd prime p.

(I) Let Γ be the natural representation of L as 2×2 matrices over F_q, $\mathscr{V}$ the underlying space of Γ, and $\mathscr{B} = \{v_1, v_2\}$ an ordered basis for $\mathscr{V}$ such that an element in L is represented by itself with respect to $\mathscr{B}$. Thus if $a = (\alpha_{ij}) \in L$, then

$$a : v_i \longrightarrow \alpha_{i1}v_1 + \alpha_{i2}v_2, \quad i = 1, 2.$$

Let $\mathscr{L}_1$, $\mathscr{L}_2$ be the subspaces of $\mathscr{V}$ generated by v_1, v_2 respectively. Clearly $\mathscr{L}_1$ and $\mathscr{L}_2$ admit the subgroup

$$H = \left\{ h(\alpha) = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}, \ \alpha \neq 0 \ \text{ in } \ F_q \right\}.$$

If $q > 3$, then any 1-dimensional subspace $\mathscr{L}$ of $\mathscr{V}$ admitting H must be $\mathscr{L}_1$ or $\mathscr{L}_2$, and these two lines can be distinguished by the relations (in the semidirect product $\mathscr{V}L$)

$$[\mathscr{L}_1, X] = \mathscr{L}_2, \ [\mathscr{L}_2, X] = 1,$$

where X is the subgroup

$$X = \left\{ x(\alpha) = \begin{pmatrix} 1 & \alpha \\ & 1 \end{pmatrix}, \ \alpha \ \text{ in } \ F_q \right\}.$$

If $q = 3$, then every 1-dimensional subspace $\mathscr{L}$ of $\mathscr{V}$ admits H. Of the 4 lines in $\mathscr{V}$, only $\mathscr{L}_2$ admits X. Since $\mathscr{L}_1 = \mathscr{L}_2^{\omega}$, where $\omega = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $\mathscr{L}_1$ and $\mathscr{L}_2$ are distinguished again by the action of L on $\mathscr{V}$.

(II) Γ induces a representation on the space $\mathscr{V}^{(3)}$ of cubic homogeneous forms. If $\mathscr{B}^{(3)}$ is the ordered basis $\{v_1^3, v_1^2v_2, v_1v_2^2, v_2^3\}$ for $\mathscr{V}^{(3)}$, then the elements $h(\alpha)$, $x(\alpha)$, ω in L are represented with respect to $\mathscr{B}^{(3)}$ respectively by the matrices

$$(1.\ 1) \qquad \begin{pmatrix} \alpha^3 & & & \\ & \alpha & & \\ & & \alpha^{-1} & \\ & & & \alpha^{-3} \end{pmatrix}, \quad \begin{pmatrix} 1 & 3\alpha & 3\alpha^2 & \alpha^3 \\ & 1 & 2\alpha & \alpha^2 \\ & & 1 & \alpha \\ & & & 1 \end{pmatrix}, \quad \begin{pmatrix} & & & 1 \\ & & -1 & \\ & 1 & & \\ -1 & & & \end{pmatrix}.$$

We shall denote this matrix form of the representation by $\Gamma^{(3)}$. Let $\mathscr{L}_1$, $\mathscr{L}_2$, $\mathscr{L}_3$, $\mathscr{L}_4$, be the 1-dimensional subspaces of $\mathscr{V}^{(3)}$ generated by the vectors in $\mathscr{B}^{(3)}$ respectively. By (1. 1) the four lines in the set $\{\mathscr{L}_1, \mathscr{L}_2, \mathscr{L}_3, \mathscr{L}_4\}$ are ordered by the action of X and ω on $\mathscr{V}^{(3)}$. Suppose $\mathscr{L}$ is a 1-dimensional subspace of $\mathscr{V}^{(3)}$ admitting H, and u is a non-zero vector in $\mathscr{L}$. If $(\mu_1, \mu_2, \mu_3, \mu_4)$ are the coordinates of u with respect to $\mathscr{B}^{(3)}$, then for any $\alpha \neq 0$ in F_q, there exists $\lambda_\alpha \neq 0$ in F_q such that

$$(\alpha^3\mu_1, \alpha\mu_2, \alpha^{-1}\mu_3, \alpha^{-3}\mu_4) = \lambda_\alpha(\mu_1, \mu_2, \mu_3, \mu_4).$$

From this it readily follows that one of the following cases occurs:

(i) $\mathscr{L} = \mathscr{L}_1, \mathscr{L}_2, \mathscr{L}_3, \mathscr{L}_4$

(ii) $q = 3$ or 7, and $\mathscr{L} \subseteq \langle \mathscr{L}_1, \mathscr{L}_4 \rangle$

(iii) $q = 3$ or 5, and $\mathscr{L} \subseteq \langle \mathscr{L}_1, \mathscr{L}_3 \rangle$ or $\langle \mathscr{L}_2, \mathscr{L}_4 \rangle$

(iv) $q = 3$, and $\mathscr{L} \subseteq \langle \mathscr{L}_1, \mathscr{L}_2 \rangle$, $\langle \mathscr{L}_2, \mathscr{L}_3 \rangle$, or $\langle \mathscr{L}_3, \mathscr{L}_4 \rangle$.

Since $\Gamma^{(3)}$ is reducible if the characteristic of F_q is 3 and we will be concerned with $\Gamma^{(3)}$ only if it is irreducible, we restrict our remarks to the case $q \neq 3$. In (ii) among the 8 lines in $\langle \mathscr{L}_1, \mathscr{L}_4 \rangle$, only $\mathscr{L}_4$ centralizes X, and then $\mathscr{L}_1 = \mathscr{L}_4^{\omega}$. In (iii) we have by (1. 1) that among the 12 lines in $\langle \mathscr{L}_1, \mathscr{L}_3 \rangle$ and $\langle \mathscr{L}_2, \mathscr{L}_4 \rangle$, only $\mathscr{L}_4$ centralizes X, and only $\mathscr{L}_3$ and $\mathscr{L}_4$ centralizes X modulo $\mathscr{L}_4$. Then $\mathscr{L}_2 = \mathscr{L}_3^{\omega}$, $\mathscr{L}_1 = \mathscr{L}_4^{\omega}$. Thus in cases (i), (ii), (iii) for $q \neq 3$, the lines $\mathscr{L}_1, \mathscr{L}_2, \mathscr{L}_3, \mathscr{L}_4$ are distinguished by the action of L on $\mathscr{V}^{(3)}$.

(III) Suppose Δ is the direct sum of Γ and $\Gamma' = \Gamma^{\rho}$, where ρ is the representation of L obtained by applying the field automorphism ρ of F_q to the matrix coefficients of Γ. If $\mathscr{V}'$ and $\mathscr{B}'$ have the same meaning for

Γ' that $\mathscr{V}$ and $\mathscr{B}$ have for Γ, then we make take $\mathscr{V}'\oplus\mathscr{V}$ as the underlying space for Δ, and $\mathscr{B}'\cup\mathscr{B}$ as an ordered basis for this space. Let $\mathscr{L}_1$, $\mathscr{L}_2$ $\mathscr{L}_3$, $\mathscr{L}_4$ be the 1-dimensional subspaces spanned by the vectors in $\mathscr{B}'\cup\mathscr{B}$ respectively. Of the four lines in $\{\mathscr{L}_1, \mathscr{L}_2, \mathscr{L}_3, \mathscr{L}_4\}$, only $\mathscr{L}_2$ and $\mathscr{L}_4$ centralize X, and indeed, the set of vectors fixed under X is $\langle\mathscr{L}_2, \mathscr{L}_4\rangle$. Then $\mathscr{L}_1=\mathscr{L}_2^{\omega}$, $\mathscr{L}_3=\mathscr{L}_4^{\omega}$. Suppose $\mathscr{L}$ is a 1-dimensional subspace of $\mathscr{V}'\oplus\mathscr{V}$ admitting H. As in (II) we readily see that one of the following cases occurs:

(i) $\mathscr{L}=\mathscr{L}_1, \mathscr{L}_2, \mathscr{L}_3, \mathscr{L}_4$

(ii) ρ is the identity automorphism, and $\mathscr{L}\subseteq\langle\mathscr{L}_1, \mathscr{L}_3\rangle$ or $\langle\mathscr{L}_2, \mathscr{L}_4\rangle$

(iii) $q=3$, and $\mathscr{L}$ is arbitrary.

In (ii) $\mathscr{L}\subseteq\langle\mathscr{L}_2, \mathscr{L}_4\rangle$ if and only if $[\mathscr{L}, X]=1$. Let u be a non-zero vector in $\mathscr{L}$, and set $u_1=u$, $u_2=u^{\omega}$ if $\mathscr{L}\subseteq\langle\mathscr{L}_1, \mathscr{L}_3\rangle$, and $u_1=-u^{\omega}$, $u_2=u$ if $\mathscr{L}\subseteq\langle\mathscr{L}_2, \mathscr{L}_4\rangle$. Then u_1, u_2 span a subspace $\mathscr{U}$ admitting L, and with respect to this basis, L is represented on $\mathscr{U}$ by Γ. Since one of the sums $\mathscr{V}'+\mathscr{U}$, $\mathscr{V}+\mathscr{U}$ is direct, we may assume after a change of notation that (i) in fact holds. We note that in (iii) the same assumption can be made if we know that $\mathscr{L}\subseteq\langle\mathscr{L}_1, \mathscr{L}_3\rangle$ or $\langle\mathscr{L}_2, \mathscr{L}_4\rangle$, and this is the case if and only if $[\mathscr{L}, X^{\omega}]=1$ or $[\mathscr{L}, X]=1$.

(IV) Suppose E is an indecomposable representation of L such that

$$E(g)=\begin{pmatrix}\Gamma'(g) & * \\ 0 & \Gamma(g)\end{pmatrix} \tag{1. 2}$$

where Γ and Γ' are as in (III). Since p does not divide the order of $\langle H, \omega\rangle$, we may assume $*$ in (1. 2) vanishes for g in $\langle H, \omega\rangle$. Let $\mathscr{B}'$, $\mathscr{B}$ be the ordered bases for Γ', Γ; we may assume with abuse of notation that $\mathscr{B}'\cup\mathscr{B}$ is a basis for the underlying space of E giving the matrix form (1. 2). Let $\mathscr{L}_1$, $\mathscr{L}_2$, $\mathscr{L}_3$, $\mathscr{L}_4$ be the 1-dimensional subspaces spanned respectively by the vectors in $\mathscr{B}'\cup\mathscr{B}$. Since E is indecomposable, it has a unique proper subrepresentation. In particular, the subset $\{\mathscr{L}_3, \mathscr{L}_4\}$ is distinguished among all 2-element subsets of $\{\mathscr{L}_1, \mathscr{L}_2, \mathscr{L}_3, \mathscr{L}_4\}$ in that $\langle\mathscr{L}_3, \mathscr{L}_4\rangle$ admits L. We can then conclude as in (I) that the lines $\mathscr{L}_1$, $\mathscr{L}_2$, $\mathscr{L}_3$, $\mathscr{L}_4$ in $\{\mathscr{L}_1, \mathscr{L}_2, \mathscr{L}_3, \mathscr{L}_4\}$ are distinguished by the action of L. Suppose $\mathscr{L}$ is a 1-dimensional subspace admitting H. One of the cases (i), (ii),

(iii) of (III) must then hold. In (ii) and (iii) we note that if $[\mathscr{L}, X]=1$, then $\mathscr{L}\subseteq\langle\mathscr{L}_2, \mathscr{L}_4\rangle$. Moreover, if $[\mathscr{L}, X]=1$ and $\langle\mathscr{L}^{\omega}, \mathscr{L}\rangle$ admits L, then $\langle\mathscr{L}^{\omega}, \mathscr{L}\rangle=\langle\mathscr{L}_3, \mathscr{L}_4\rangle$, and we may then conclude that $\mathscr{L}=\mathscr{L}_4$, $\mathscr{L}^{\omega}=\mathscr{L}_3$. Similarly, if $[\mathscr{L}, X]\equiv 1 \pmod{\langle\mathscr{L}_3, \mathscr{L}_4\rangle}$ and $\mathscr{L}\not\subseteq\langle\mathscr{L}_3, \mathscr{L}_4\rangle$, then $\mathscr{L}=\mathscr{L}_2$, $\mathscr{L}^{\omega}=\mathscr{L}_1$.

(V) If $q=q_0{}^3$, let $\bar{\alpha}=\alpha^{q_0}$ for α in F_q, so that $\alpha\longrightarrow\bar{\alpha}$ is an automorphism of order 3 of F_q with fixed field F_{q_0}. Let $\bar{\mathscr{V}}$, $\bar{\bar{\mathscr{V}}}$ and $\bar{\mathscr{B}}$, $\bar{\bar{\mathscr{B}}}$ have the meaning for $\bar{\Gamma}$, $\bar{\bar{\Gamma}}$ that $\mathscr{V}$ and $\mathscr{B}$ have for Γ, and let $\Gamma\times\bar{\Gamma}\times\bar{\bar{\Gamma}}$ be the representation of L induced on $V\times\bar{V}\times\bar{\bar{V}}$. The set $B^{[3]}$ of vectors

$$\begin{aligned}
w_1 &= v_1\times\bar{v}_1\times\bar{\bar{v}}_1 & \qquad w_5 &= v_1\times\bar{v}_2\times\bar{\bar{v}}_2\\
w_2 &= v_2\times\bar{v}_1\times\bar{\bar{v}}_1 & w_6 &= v_2\times\bar{v}_1\times\bar{\bar{v}}_2\\
w_3 &= v_1\times\bar{v}_2\times\bar{\bar{v}}_1 & w_7 &= v_2\times\bar{v}_2\times\bar{\bar{v}}_1\\
w_4 &= v_1\times\bar{v}_1\times\bar{\bar{v}}_2 & w_8 &= v_2\times\bar{v}_2\times\bar{\bar{v}}_2
\end{aligned}$$

is then a basis for the underlying space $V^{[3]}=V\times\bar{V}\times\bar{\bar{V}}$. It is easily checked that with respect to this basis, $h(\alpha)$ is represented by

$$\begin{pmatrix}
\alpha\overline{\alpha\overline{\alpha}} &&&&&&& \\
& \bar{\alpha}\bar{\bar{\alpha}}/\alpha &&&&&& \\
&& \bar{\bar{\alpha}}\alpha/\bar{\alpha} &&&&& \\
&&& \alpha\bar{\alpha}/\bar{\bar{\alpha}} &&&& \\
&&&& \alpha/\bar{\alpha}\bar{\bar{\alpha}} &&& \\
&&&&& \bar{\alpha}/\bar{\bar{\alpha}}\alpha && \\
&&&&&& \bar{\bar{\alpha}}/\alpha\bar{\alpha} & \\
&&&&&&& 1/\alpha\bar{\alpha}\bar{\bar{\alpha}}
\end{pmatrix} \tag{1. 3}$$

$x(\alpha)$ is represented by

$$\begin{pmatrix}
1 & \alpha & \bar{\alpha} & \bar{\bar{\alpha}} & \bar{\alpha}\bar{\bar{\alpha}} & \bar{\bar{\alpha}}\alpha & \alpha\bar{\alpha} & \alpha\bar{\alpha}\bar{\bar{\alpha}}\\
 & 1 & 0 & 0 & 0 & \bar{\bar{\alpha}} & \bar{\alpha} & \bar{\bar{\alpha}}\bar{\alpha}\\
 & & 1 & 0 & \bar{\bar{\alpha}} & 0 & \alpha & \alpha\bar{\bar{\alpha}}\\
 & & & 1 & \bar{\alpha} & \alpha & 0 & \bar{\alpha}\alpha\\
 & & & & 1 & 0 & 0 & \alpha\\
 & & & & & 1 & 0 & \bar{\alpha}\\
 & & & & & & 1 & \bar{\bar{\alpha}}\\
 & & & & & & & 1
\end{pmatrix} \tag{1. 4}$$

and ω by

$$(1.\ 5)\qquad \begin{pmatrix} & & & & & & & 1 \\ & & & & -1 & & & \\ & & & & & -1 & & \\ & & & & & & -1 & \\ & 1 & & & & & & \\ & & 1 & & & & & \\ & & & 1 & & & & \\ -1 & & & & & & & \end{pmatrix}$$

Let θ be an element of order $q-1$ in F_q. The vectors

$$(1.\ 6)\qquad \begin{aligned} u_1 &= w_1 & u_5 &= w_5 + w_6 + w_7 \\ u_2 &= w_2 + w_3 + w_4 & u_6 &= \theta w_5 + \bar{\theta} w_6 + \bar{\bar{\theta}} w_7 \\ u_3 &= \theta w_2 + \bar{\theta} w_3 + \bar{\bar{\theta}} w_4 & u_7 &= \theta^2 w_5 + \bar{\theta}^2 w_6 + \bar{\bar{\theta}}^2 w_7 \\ u_4 &= \theta^2 w_2 + \bar{\theta}^2 w_3 + \bar{\bar{\theta}}^2 w_4 & u_8 &= w_8 \end{aligned}$$

also form a basis $\mathscr{B}_0$ of $\mathscr{V}^{[3]}$. Let $\mathscr{V}_0$ be the vector space spanned by $\mathscr{B}_0$ over F_{p_0}; $\mathscr{V}_0$ is contained in $\mathscr{V}^{[3]}$, but not as a subspace. Using (1. 4), (1. 5) it is not difficult to see that $\mathscr{V}_0$ admits L. The representation Γ_0 of L afforded by the basis $\mathscr{B}_0$ in $\mathscr{V}_0$ is then equivalent to $\Gamma \times \bar{\Gamma} \times \bar{\bar{\Gamma}}$. Let $\mathscr{L}_1$, $\mathscr{L}_2$, $\mathscr{L}_3$, $\mathscr{L}_4$ be the subspaces of $\mathscr{V}_0$ spanned over F_{q_0} by u_1; u_2, u_3, u_4; u_5, u_6, u_7; u_8 respectively. These subspaces admit H by (1. 3), (1. 6). Since $\mathscr{L}_1$, $\mathscr{L}_4$ are 1-dimensional, they are irreducible under H. $\mathscr{L}_2$ and $\mathscr{L}_3$, which are 3-dimensional, are also irreducible under H, as a consideration of the characteristic values of $h(\theta)$ on these subspaces shows. $\mathscr{L}_1$, $\mathscr{L}_4$ are non-equivalent H-modules for $q_0 > 3$, since the characteristic values $(\theta\bar{\theta}\bar{\bar{\theta}})$ and $(\theta\bar{\theta}\bar{\bar{\theta}})^{-1}$ of $h(\theta)$ on $\mathscr{L}_1$ and $\mathscr{L}_4$ are then distinct. $\mathscr{L}_2$ and $\mathscr{L}_3$ are non-equivalent without this condition on q_0. Otherwise by (1. 3), (1. 6), $\bar{\theta}\bar{\bar{\theta}}/\theta$ must be equal to $\theta/\bar{\theta}\bar{\bar{\theta}}$, $\bar{\theta}/\bar{\bar{\theta}}\theta$, or $\bar{\bar{\theta}}/\theta\bar{\theta}$. If $\bar{\theta}\bar{\bar{\theta}}/\theta$ is $\bar{\theta}/\bar{\bar{\theta}}\theta$ or $\bar{\bar{\theta}}/\theta\bar{\theta}$, then $\theta^2 = 1$, which is impossible. If $\bar{\theta}\bar{\bar{\theta}}/\theta$ is $\theta/\bar{\theta}\bar{\bar{\theta}}$, then $\theta^{2(q_0^2+q_0-1)} = 1$, which is also impossible since $0 < 2(q_0^2 + q_0 - 1) < (q_0 - 1)(q_0^2 + q_0 + 1) = q - 1$.

Suppose $\mathscr{L}$ is a subspace of $\mathscr{V}_0$ admitting H. If either $q_0 > 3$ and $\mathscr{L}$ is 1-dimensional, or $\mathscr{L}$ is 3-dimensional, then $\mathscr{L}$ must be $\mathscr{L}_1$, $\mathscr{L}_2$, $\mathscr{L}_3$, or $\mathscr{L}_4$ by the Frobenius-Schur Theorem. Moreover, $\mathscr{L}_4$ and $\mathscr{L}_3$ are distinguished by the relations $[\mathscr{L}_4, X] = 1$, $[\mathscr{L}_3, X] \leqslant \mathscr{L}_4$ by (1. 4), (1. 6), and then $\mathscr{L}_1 = \mathscr{L}_4^{\omega}$, $\mathscr{L}_2 = \mathscr{L}_3^{\omega}$. If $q_0 = 3$ and $\mathscr{L}$ is 1-dimensional, then the

Frobenius-Schur Theorem gives $\mathscr{L} \subseteq \langle \mathscr{L}_1, \mathscr{L}_4 \rangle$. But only $\mathscr{L}_4$ among the four lines in $\langle \mathscr{L}_1, \mathscr{L}_4 \rangle$ centralizes X, and then $\mathscr{L}_1 = \mathscr{L}_4^{\omega}$. Thus in all cases, the subspaces $\mathscr{L}_1$, $\mathscr{L}_2$, $\mathscr{L}_3$, $\mathscr{L}_4$ are distinguished by the action of L on $\mathscr{V}_0$.

Let $\mathfrak{R}$ be the regular representation of F_q considered as an algebra over F_p. If $\mathfrak{B}$ is any one of the representations Γ, $\Gamma^{(3)}$, Δ, E, or Γ_0, then the representations $\mathfrak{R} \circ \mathfrak{B}$ constitute up to equivalence, all representations over F_p of L of degree not greater than $4n$, where $q = p^n$, in which j is represented by $-I$. This is essentially [5] (1E).

2. Throughout the remainder of this paper, G will be a finite group satisfying

(*) G has subgroups L_1, L_2 such that $L_1 \simeq SL(2, q_1)$, $L_2 \simeq SL(2, q_2)$, $[L_1, L_2] = 1$, $L_1 \cap L_2 = \langle j \rangle$, where j is an involution, and $|C(j) : L_1 L_2| = 2$.

Such groups have been studied in [5], and as the present paper is a continuation of [5], we shall continue with the notation of [5]. Suppose $G \neq C(j)O(G)$, so that by [5], (2A) $C(j) = L_1 L_2 \langle n \rangle$, where $n^2 = 1$. If $L_1^n = L_2$, then $G \simeq PSp(4, q)$ with $q = q_1 = q_2$ by [15]. This case may then be excluded as done, and so by [5], (2A) and (7I), G satisfies the condition

(**) $C(j) = L_1 L_2 \langle n \rangle$, where $n^2 = 1$, $L_1^n = L_1$, $L_2^n = L_2$. q_1 and q_2 are equal, or one is the cube of the other.

§§5–7 of [5] show that $|G|$ is divisible by $(q_1 q_2)^3$ if it is not the case that $q_1 = q_2 \leqslant 11$. We consider in addition, then, the condition

(***) $|G|$ is divisible by $(q_1 q_2)^3$.

The exceptional cases $q_1 = q_2 \leqslant 11$ will be discussed at the end in **§6.**

Set $q_1 \geqslant q_2 = q = p^n$. By (**) $q_1 = q_2 = q$, or $q_1 = q^3$, $q_2 = q$. In the latter case, we shall set $\bar{\alpha} = \alpha^q$, $\bar{\bar{\alpha}} = \alpha^{q^2}$. Recalling the notation and results of [5], we have the following. The images of $\begin{pmatrix} 1 & \alpha \\ & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & \\ \alpha & 1 \end{pmatrix}$, $\begin{pmatrix} \alpha & \\ & \alpha^{-1} \end{pmatrix}$, $\begin{pmatrix} & 1 \\ -1 & \end{pmatrix}$ under the isomorphism ϕ_i of $SL(2, q_i)$ onto L_i are $x_i(\alpha)$, $x_{-i}(\alpha)$, $h_i(\alpha)$, ω_i respectively, $i = 1, 2$. X_i, X_{-i}, H_i are the subgroups of L_i generated by elements of the form $x_i(\alpha)$, $x_{-i}(\alpha)$, $h_i(\alpha)$ respectively. δ is a non-square of order a power of 2 in F_q, and $C(j) = \langle L_1 L_2, h_0 \rangle$, where h_0 acts on L_i as conjugation by the matrix $\begin{pmatrix} 1 & \\ & \delta \end{pmatrix}$, and $h_0^2 = h_1(\delta^{-1}) h_2(\delta^{-1})$. In particular,

$h_0{}^{-1}\omega_i h_0 = \omega_i h_i(\delta^{-1})$, and so $\omega_i^{-1}h_0\omega_i = h_0 h_i(\delta)$. The subgroup $H = \langle H_1H_2, h_0\rangle$ is abelian of order $(q_1-1)(q_2-1)$. If D is the 4-subgroup of H, then

$$N(D) = N(H) = \langle H, \omega_1, \omega_2, \eta\rangle,$$

where η is an element of order a power of 3 permuting the involutions $j = j_0, j_1, j_2$ of D cyclically.

Let $K = O(C(X_2))$; we have then $L_1 \cap K = 1$, $C(X_2) = L_1K$, and $N(X_2) = HL_1K$. The element j inverts K/X_2. If M is the S_p-subgroup of K, then M can be factored as

$$M = X_2(X_{-1}X_{-2})^{\eta}(X_1X_{-2})^{\eta^2}.$$

$P = X_1M$ is then a p-subgroup of order $(q_1q_2)^3$. If $B = HP$, then $\tilde{G} = BN(H)B$ is a subgroup of G with a Bruhat decomposition. The order of $\tilde{G}$ is

$$(q_1q_2)^3\,(q_1^2-1)\,(q_2^2-1)\,(q_1^2q_2^2+q_1q_2+1)$$

Let $\hat{P} = X_2X_{-2}^{\eta}X_{-2}^{\eta^2}$, $\hat{B} = H\hat{P}$, and $\hat{N} = \langle H, \omega_2, \eta\rangle$. Then $\hat{G} = \hat{B}\hat{N}\hat{B}$ is also a subgroup of G with a Bruhat decomposition. The order of $\hat{G}$ is

$$q_2^3(q_2^3-1)\,(q_2+1)\,(q_1-1),$$

and $\hat{G}/K_0$ is isomorphic to $PGL(3,q)$, $SL(3,q)$, or $PSL(3,q)\times Z_3$, where $K_0 = H^{q-1} \leqslant Z(\hat{G})$.

(2*A*) *The representation* $\mathfrak{V}$ *of* L_1 *induced on the elementary abelian p-group* $\mathscr{V} = M/X_2$ *is indecomposable.*

Proof. Suppose not. Then $\mathscr{V} = \mathscr{V}' \oplus \mathscr{V}''$, where $\mathscr{V}'$ and $\mathscr{V}''$ are subspaces admitting L_1. Now j inverts $\mathscr{V}$, and thus j inverts $\mathscr{V}'$ and $\mathscr{V}''$ as well. Since $|\mathscr{V}| = q^4$ if $q_1 = q_2 = q$ and $|\mathscr{V}| = q^8$ if $q_1 = q^3$, $q_2 = q$, it follows that we must have $|\mathscr{V}| = q^4$ and $q_1 = q_2 = q$. Moreover, if $\mathfrak{V}'$, $\mathfrak{V}''$ are the representations of L_1 induced on $\mathscr{V}'$, $\mathscr{V}''$ respectively, then bases can be chosen in $\mathscr{V}'$, $\mathscr{V}''$ so that $\mathfrak{V}' = \mathfrak{R}\circ\Gamma$, $\mathfrak{V}'' = \mathfrak{R}\circ\Gamma$, where $\mathfrak{R}$ is the regular representation of F_q considered as an algebra over F_p. Now $\mathscr{L} = X_{-2}^{\eta^2}X_2/X_2$ admits H_1, and by [5], (7*C*), $[\mathscr{L}, X_1] = 1$. As in §1 (III), we find that $[\mathscr{L}^{\omega_1}, X_1] \leqslant \mathscr{L}$, and so

$$[X_{-2}^{\eta}, X_1] \leqslant X_{-2}^{\eta^2}X_2 \tag{2. 1}$$

By [5], (6. 3) $U = X_1X_1^{\eta^2}X_{-1}^{\eta}X_{-2}^{\eta^2}X_2$ is a subgroup. Since $[M, M] \leqslant X_2$, it now follows by (2. 1) that X_{-2}^{η} normalizes U. ω_2^{η} normalizes U as well, since

$\omega^{\eta}_{2} \equiv \omega_2 \eta^2 \pmod{H}$. Thus L^{η}_{2} normalizes U. On the other hand, the subgroup $U_0 = X^{\eta}_{-1} X^{\eta^2}_{-2} X_2$ admits L^{η}_{2} as well, since X^{η}_{-2} and ω^{η}_{2} clearly normalize U_0. Thus the elementary p-group $\mathscr{U} = U/U_0$ of order q^2 admits L^{η}_{2}; let $\mathfrak{U}$ be the representation of L^{η}_{2} on $\mathscr{U}$. With obvious identifications we can choose as before a basis in $\mathscr{U}$ so that $\mathfrak{U} = \mathfrak{R} \circ \Gamma$. Since $X^{\eta^2}_{1} U_0/U_0$ and $X_1 U_0/U_0$ admit H^{η}_{2}, $[X^{\eta^2}_{1}, X^{\eta}_{-2}] \leqslant X_2$, and ω^{η}_{2} interchanges $X^{\eta^2}_{1} U_0/U_0$ and $X_1 U_0/U_0$, it follows by the remarks of **§1** (I) that $[X_1, X^{\eta}_{-2}] \equiv X^{\eta^2}_{1} \pmod{U_0}$, which contradicts (2. 1). This completes the proof.

By (2*A*) the commuting algebra $\mathfrak{C}$ of $\mathfrak{V}$ is completely primary. Now $[L_1, H_2] = 1$ and H_2 normalizes $\mathscr{V}$. If h is an element in H_2 centralizing $\mathscr{V}$, then h centralizes X^{η}_{-2} and $X^{\eta^2}_{-2}$ modulo X_2. Since h normalizes X^{η}_{-2} and $X^{\eta^2}_{-2}$, it follows that h centralizes X^{η}_{-2}, $X^{\eta^2}_{-2}$, and so h centralizes $[X^{\eta}_{-2}, X^{\eta^2}_{-2}] = X_2$ as well. Thus $h \in \langle j \rangle$. Since j inverts $\mathscr{V}$, we have that $h = 1$, and H_2 is then embedded in $\mathfrak{C}$. In particular, H_2 is isomorphic to a cyclic subgroup of order $q-1$ in a finite field, say of p^m elements. If $q = p^n$, then $p^n - 1$ divides $p^m - 1$, and necessarily n divides m. Thus H_2 acts on $\mathscr{V}$ as scalar multiplication by elements of F_q, and $\mathscr{V}$ can then be considered as a vector space over F_q admitting L_1 as an indecomposable group of linear transformations. We shall henceforth assume this interpretation of $\mathscr{V}$. With a suitable choice of basis in $\mathscr{V}$, we have the following three cases:

(A) $q_1 = q_2 = q$, $\mathfrak{V}$ is irreducible, $\mathfrak{V} = \Gamma^{(3)\sigma}$, where $\Gamma^{(3)}$ is the representation of **§1** (II), and σ is a field automorphism. The characteristic of F_q is not 3.

(B) $q_1 = q_2 = q$, $\mathfrak{V}$ is reducible, $\mathfrak{V} = E^{\sigma}$, where E is the representation of **§1** (IV), and σ is a field automorphism.

(C) $q_1 = q^3$, $q_2 = q$, $\mathfrak{V}$ is irreducible, and $\mathfrak{V} = \Gamma_0^{\sigma}$, where Γ_0 is the representation of **§1** (V) (with q, q_0 replaced by q^3, q), and σ is a field automorphism.

In each of the above cases, let $\mathscr{L}_1$, $\mathscr{L}_2$, $\mathscr{L}_3$, $\mathscr{L}_4$ have the meaning assigned to these symbols in the corresponding cases of **§1**. $\mathscr{L}_1$, $\mathscr{L}_2$, $\mathscr{L}_3$, $\mathscr{L}_4$ are subspaces of $\mathscr{V}$ by definition. Since X^{η}_{-1}, $X^{\eta^2}_{1}$, X^{η}_{-2}, $X^{\eta^2}_{-2}$ admit H_2, their images in $\mathscr{V}$ are also subspaces of $\mathscr{V}$. We have

(2*B*) *The subspaces determined by* X^{η}_{-2}, $X^{\eta^2}_{1}$, X^{η}_{-1}, $X^{\eta^2}_{-2}$ *modulo* X_2 *are respectively* $\mathscr{L}_1$, $\mathscr{L}_2$, $\mathscr{L}_3$, $\mathscr{L}_4$ *in cases* (*A*) *and* (*C*). *In case* (*B*) *the subspace* $\mathscr{L}$ *determined* *by $X_{-2}^{\eta_2^2}$ modulo X_2 is contained in $\langle \mathscr{L}_2, \mathscr{L}_4 \rangle$, but $\mathscr{L} \neq \mathscr{L}_4$. If the field automorphism ρ appearing in E is non-trivial, then $\mathscr{L} = \mathscr{L}_2$.*

Proof. ω_1 interchanges $X_{-1}^{\eta}, X_1^{\eta^2}$ as well as $X_{-2}^{\eta}, X_{-2}^{\eta_2^2}$. Since these subgroups all admit H_1, the results claimed in cases (A) and (C) follow from [5], (7C) and the remarks of **§1.** Similarly, we can show that the subspace $\mathscr{L}$ determined by $X_{-2}^{\eta_2^2}$ modulo X_2 in case (B) is contained in $\langle \mathscr{L}_2, \mathscr{L}_4 \rangle$. If $\mathscr{L} = \mathscr{L}_4$, then (2. 1) would hold, and as in the proof of (2A), this gives a contradiction. If ρ is non-trivial, then (i) in **§1** (III) holds. Since $[\mathscr{L}, X_1] = 1$ by [5], (7C), $\mathscr{L}$ is either $\mathscr{L}_2$ or $\mathscr{L}_4$, and thus $\mathscr{L} = \mathscr{L}_2$. Thus completes the proof.

(2C) *In cases (A) and (B), $\hat{G}$ is isomorphic to $SL(3, q)$, and in case (C), $\hat{G}/K_0$ is isomorphic to $PGL(3, q)$.*

Proof. We first note that K_0 is trivial in cases (A) and (B), and that $K_0 = H_1^{q-1}$ is cyclic of order $q^2 + q + 1$ in case (C). Thus $|\hat{G}/K_0| = q^3(q^3 - 1)(q^2 - 1)$. If $q \not\equiv 1 \pmod 3$, then $PGL(3, q)$, $SL(3, q)$, and $PSL(3, q)$ are all isomorphic groups of order $q^3(q^3 - 1)(q^2 - 1)$. Since $\hat{G}/K_0$ is isomorphic to $PGL(3, q)$, $SL(3, q)$, or $PSL(3, q) \times Z_3$, the result follows in this case. Thus we may assume $q \equiv 1 \pmod 3$, so that the S_3-subgroup T of H is non-trivial with two generators.

Suppose case (A) or (B) holds. η normalizes T, and so centralizes some element t in T of order 3. Since $|H : H_1 H_2| = 2$ so that $T \leqslant H_1 H_2$, we may express

$$t = h_1(\tau_1) h_2(\tau_2), \tag{2. 2}$$

where τ_1, τ_2 are elements in F_q such that $\tau_1^3 = \tau_2^3 = 1$. If $\tau_1 = 1$, then $t \in H_2$, and so t acts on $\mathscr{V}$ as scalar multiplication by some element in F_q. But since t centralizes L_1 and η, it follows that t centralizes $X_{-1}^{\eta}, X_1^{\eta^2}$ and so t centralizes $\mathscr{V}$, which is impossible. Thus $C(\eta) \cap T$ is cyclic. Since $C(\eta) \cap T$ admits ω_1 and ω_2, it follows that t^{ω_1} and t^{ω_2} are in $\langle t \rangle$. By (2. 2) and the preceding discussion, we have that $\tau_2 = 1$. Thus $t \in H_1$, and since $\hat{G} = \hat{B}\hat{N}\hat{B}$, it readily follows that $t \in Z(\hat{G})$, so that $\hat{G}$ is isomorphic to $SL(3, q)$ or $PSL(3, q) \times Z_3$. Suppose $\hat{G} \simeq PSL(3, q) \times Z_3$. If $q \equiv 1 \pmod 9$, then the S_3-subgroup T of H cannot be generated by 2 elements; if $q \not\equiv 1 \pmod 9$, then $C(\eta) \cap T$ is non-cyclic. In either case we have a contradiction, so that $\hat{G} \simeq SL(3, q)$ as claimed.

Suppose case (C) holds. If $\hat{G}/K_0$ is isomorphic to $SL(3,q)$ or $PSL(3,q)\times Z_3$, then there exists an element t of order a power of 3 in H but not in K_0 such that $\langle t, K_0\rangle/K_0$ is the center of $\hat{G}/K_0$. Again, we may express

$$t = h_1(\tau_1)h_2(\tau_2)$$

where τ_1, τ_2 are elements in F_{q^3}, F_q of order a power of 3. But ω_2 and t commute modulo K_0, and so $\tau_2 = 1$. Thus $t = h_1(\tau_1)$ is in H_1. Moreover, t and η commute modulo K_0, and since $K_0 \leqslant H_1$, it follows that t^η, t^{η^2} belong to H_1. In particular, t centralizes X^{η}_{-2} and $X^{\eta^2}_{-2}$. By (1. 3) and (2B) it follows that $\tau_1{}^{q^2+q+1} = 1$. Since $q^2+q+1 \not\equiv 0 \pmod 9$, t is an element of order 3 in H_1. On the other hand, $q^2+q+1 \equiv 0 \pmod 3$ implies that $t \in K_0$, which is a contradiction. This completes the proof.

Let λ be a non-zero element in F_q or F_{q^3}, and μ a non-zero element in F_q. Then in the corresponding cases (A), (B), (C), $h_0h_1(\lambda)h_2(\mu)$ acts on L_1 as conjugation by $\begin{pmatrix}1 & \\ & \lambda-2\delta\end{pmatrix}$ and on L_2 as conjugation by $\begin{pmatrix}1 & \\ & \mu-2\delta\end{pmatrix}$. Moreover,

$$(h_0h_1(\lambda)h_2(\mu))^2 = h_1(\lambda^2\delta^{-1})h_2(\mu^2\delta^{-1}).$$

Since δ is a non-square in both F_q and F_{q^3}, it follows that for any non-zero elements α in F_q or F_{q^3}, β in F_q, there exists an element $h(\alpha,\beta)$ in H such that $h(\alpha,\beta)$ acts on L_1 as conjugation by $\begin{pmatrix}1 & \\ & \alpha\end{pmatrix}$ and on L_2 as conjugation by $\begin{pmatrix}1 & \\ & \beta\end{pmatrix}$, and such that

$$h(\alpha,\beta)^2 = h_1(\alpha^{-1})h_2(\beta^{-1}).$$

The element $h(\alpha,\beta)$ is not uniquely determined by these conditions, but only up to a factor of j. Let ξ be a fixed primitive element of order $q-1$ in F_q. In particular, we set $h_0(\xi) = h(\xi,\xi^{-1})$, and for any $\alpha \neq 0$ in F_q, we define

$$h_0(\alpha) = h_0(\xi)^i, \tag{2. 3}$$

where $\alpha = \xi^i$. This definition depends on making one of two possible choices for $h_0(\xi)$. If H_0 is the set of all elements of the form $h_0(\alpha)$, then H_0 is cyclic of order $q-1$ and $H = H_1 \times H_0$. We note that $h_0(\xi)^{-1}\omega_1h_0(\xi) = \omega_1h_1(\xi^{-1})$, $h_0(\xi)^{-1}\omega_2h_0(\xi) = \omega_2h_2(\xi)$, so that

$$\begin{aligned}\omega_1^{-1}h_0(\xi)\omega_1 &= h_0(\xi)h_1(\xi)\\ \omega_2^{-1}h_0(\xi)\omega_2 &= h_0(\xi)h_2(\xi^{-1}).\end{aligned}\tag{2. 4}$$

(2*D*) *Suppose case* (*A*) *or* (*B*) *holds. Define the following elements and subgroups in* $SL(3,q)$.

$$a=\begin{pmatrix}\xi & & \\ & \xi^{-1} & \\ & & 1\end{pmatrix},\quad b=\begin{pmatrix}1 & & \\ & \xi & \\ & & \xi^{-1}\end{pmatrix},\quad \tilde{\eta}=\begin{pmatrix}0 & 0 & 1\\ -1 & 0 & 0\\ 0 & -1 & 0\end{pmatrix},$$

$$\tilde{\omega}=\begin{pmatrix}0 & 0 & 1\\ 0 & 1 & 0\\ -1 & 0 & 0\end{pmatrix},\quad \tilde{P}=\left\{\begin{pmatrix}1 & * & *\\ & 1 & *\\ & & 1\end{pmatrix}\right\},\quad \tilde{H}=\left\{\begin{pmatrix}* & & \\ & * & \\ & & *\end{pmatrix}\right\}.$$

With a suitable choice of η *and* $h_0(\xi)$ *there exists an isomorphism* f *of* $\hat{G}$ *onto* $SL(3,q)$ *such that*

$$f(\hat{P})=\tilde{P},\quad f(H)=\tilde{H},\quad f(\eta)=\tilde{\eta},$$
$$f(\omega_2)=\tilde{\omega},\quad f(h_1(\xi))=(ab^{-1})^t,$$
$$f(h_2(\xi))=ab,\quad f(h_0(\xi))=a^{(1-t)/2}b^{(1+t)/2}.$$

t *is an integer such that* $1\leqslant t\leqslant q-1$ *and* $(t,q-1)=1$.

Proof. Since $\tilde{P}$ is an S_p-subgroup of $SL(3,q)$, it follows by (2C) that there exists an isomorphism f of $\hat{G}$ onto $SL(3,q)$ such that $f(\hat{P})=\tilde{P}$, $f(X_2)=Z(\tilde{P})$. In particular, $f: N(\hat{P})\cap\hat{G}\longrightarrow N(\tilde{P})$. But $N(\hat{P})\cap\hat{G}=\hat{P}H$ and $N(\tilde{P})=\tilde{P}\tilde{H}$. Thus $f(H)$ is a complement of $\tilde{P}$ in $N(\tilde{P})$, and so $f(H)$ and $\tilde{H}$ are conjugate by some element c in $\tilde{P}$. Replacing f by the composition of f with the inner automorphism of $SL(3,q)$ induced by c, we may assume $f(H)=\tilde{H}$ and so $f: N(H)\cap\hat{G}\longrightarrow N(\tilde{H})$. But $N(H)\cap\hat{G}=\langle H,\eta,\omega_2\rangle$ and $N(\tilde{H})=\langle\tilde{H},\tilde{\eta},\tilde{\omega}\rangle$. In particular, $f^{-1}(\tilde{\eta})=h\eta^i$ for some h in H and $i=1$ or 2. We may assume $i=1$ by replacing f by the composition of f with the automorphism of $SL(3,q)$ defined by conjugating a matrix by $\begin{pmatrix} & & 1\\ & 1 & \\ 1 & & \end{pmatrix}$, and then passing onto the contragredient of the resulting matrix. The preceding properties of f are not affected by this replacement.

a and b generate $\tilde{H}$. Since H_1 centralizes X_2, it follows that $f(H_1)=\langle ab^{-1}\rangle$. Since $\hat{P}^{\omega_2}\cap\hat{P}=1$ and $\tilde{P}^{\tilde{\omega}}\cap\tilde{P}=1$, we have that $f(\omega_2)=\tilde{h}\tilde{\omega}$ for some $\tilde{h}$ in $\tilde{H}$. Let

$$\tilde{h}=\begin{pmatrix}\alpha & & \\ & \beta & \\ & & \alpha^{-1}\beta^{-1}\end{pmatrix};$$

we have then

$$(\tilde{h}\tilde{\omega})^2 = \begin{pmatrix} -\beta^{-1} & & \\ & \beta^2 & \\ & & -\beta^{-1} \end{pmatrix}.$$

Since $f(\omega_2)$ has order 4, we must have $\beta = 1$, so that

$$f(\omega_2) = \begin{pmatrix} & & \alpha \\ & 1 & \\ -\alpha^{-1} & & \end{pmatrix}.$$

Now

$$\begin{pmatrix} 1 & & \\ & \alpha^{-1} & \\ & & \alpha \end{pmatrix}\begin{pmatrix} & & \alpha \\ & 1 & \\ -\alpha^{-1} & & \end{pmatrix}\begin{pmatrix} 1 & & \\ & \alpha & \\ & & \alpha^{-1} \end{pmatrix} = \begin{pmatrix} & & 1 \\ & 1 & \\ -1 & & \end{pmatrix}$$

Replacing f by the composition of f with the inner automorphism of $SL(3,q)$ induced by $\begin{pmatrix} 1 & & \\ & \alpha & \\ & & \alpha^{-1} \end{pmatrix}$, we may assume $f(\omega_2) = \tilde{\omega}$. The preceding properties of f are not affected by this change. With f so fixed, we choose η so that $f(\eta) = \tilde{\eta}$.

Suppose

$$f(x_2(1)) = \begin{pmatrix} 1 & 0 & \alpha \\ & 1 & 0 \\ & & 1 \end{pmatrix}, \quad f(x_{-2}(1)) = \begin{pmatrix} 1 & & \\ 0 & 1 & \\ \beta & 0 & 1 \end{pmatrix},$$

where $\alpha, \beta \in F_q$. Since $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, we have $\omega_2 = x_2(1)x_{-2}(-1)x_2(1)$, and hence

$$\tilde{\omega} = f(\omega_2) = \begin{pmatrix} 1 & 0 & \alpha \\ & 1 & 0 \\ & & 1 \end{pmatrix}\begin{pmatrix} 1 & & \\ 0 & 1 & \\ -\beta & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & \alpha \\ & 1 & 0 \\ & & 1 \end{pmatrix} = \begin{pmatrix} 1-\alpha\beta & 0 & 2\alpha-\alpha^2\beta \\ 0 & 1 & 0 \\ -\beta & 0 & 1-\alpha\beta \end{pmatrix}.$$

Thus $\alpha = \beta = 1$. Since

$$\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \alpha^{-1}-1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ \alpha-1 & 1 \end{pmatrix}\begin{pmatrix} 1 & -\alpha^{-1} \\ 0 & 1 \end{pmatrix}$$

we also have

$$f(h_2(\alpha)) = \begin{pmatrix} \alpha & & \\ & 1 & \\ & & \alpha^{-1} \end{pmatrix} \text{ for } \alpha \in F_p.$$

Identifying $\langle Z(\tilde{P}), \tilde{\omega} \rangle$ with $SL(2,q)$ in the obvious way, we see that f restricted to L_2 induces an automorphism of $SL(2,q)$ which fixes the elements of the subgroup $SL(2, p)$. Such an automorphism is necessarily one defined by applying a field automorphism τ of F_q to $SL(2, q)$. Replacing f by the composition of f with the automorphism of $SL(3, q)$ obtained by applying τ^{-1} to the matrix coefficients, we may assume

$$f(x_2(\alpha)) = \begin{pmatrix} 1 & 0 & \alpha \\ & 1 & 0 \\ & & 1 \end{pmatrix}, \quad f(x_{-2}(\alpha)) = \begin{pmatrix} 1 & & \\ 0 & 1 & \\ \alpha & 0 & 1 \end{pmatrix}$$

for $\alpha \neq 0$ in F_q, so in particular, $f(h_2(\xi)) = ab$. The earlier properties of f are unaffected by this change. We now define the integer t by the condition

$$f(h_1(\xi)) = (ab^{-1})^t,$$

where $1 \leqslant t \leqslant q-1$ and $(t,\ q-1) = 1$. Since $h_0(\xi)^2 = h_1(\xi^{-1})h_2(\xi)$, we have that

$$f(h_0(\xi))^2 = (ab^{-1})^{-t}(ab) = a^{1-t}b^{1+t}.$$

The integers $1-t$, $1+t$ are even since $(t,\ q-1) = 1$ and q is odd. Now $f(j) = (ab)^{(q-1)/2}$, so replacing $h_0(\xi)$ by $h_0(\xi)j$ if necessary, we may assume that

$$f(h_0(\xi)) = a^{(1-t)/2}b^{(1+t)/2}c,$$

where $c = \begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix}$ or $\begin{pmatrix} 1 & & \\ & -1 & \\ & & -1 \end{pmatrix}$. But $h_0(\xi)$ transforms $x_2(\alpha)$ onto $x_2(\alpha\xi^{-1})$. This implies that $c = 1$, which completes the proof.

A similar result holds in case (C). We fix a primitive element θ of order $q^3 - 1$ in F_{q^3} such that $\xi = \theta^{q^2+q+1}$, and represent elements of $\hat{G}/K_0$ and $pGL(3, q)$ by elements in the corresponding cosets in $\hat{G}$ and $GL(3, q)$.

(2*E*) *Suppose case* (*C*) *holds. Define the following elements and subgroups in* $PGL(3, q)$.

$$a = \begin{pmatrix} \xi & & \\ & 1 & \\ & & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & & \\ & \xi & \\ & & 1 \end{pmatrix}, \quad \tilde{\eta} = \begin{pmatrix} 0 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}$$

$$\tilde{\omega} = \begin{pmatrix} & & 1 \\ & 1 & \\ -1 & & \end{pmatrix}, \quad \tilde{P} = \left\{\begin{pmatrix} 1 & * & * \\ & 1 & * \\ & & 1 \end{pmatrix}\right\}, \quad \tilde{H} = \left\{\begin{pmatrix} * & & \\ & * & \\ & & * \end{pmatrix}\right\}.$$

With a suitable choice of η and $h_0(\xi)$, there exists an isomorphism f of $\hat{G}/K_0$ onto $PGL(3, q)$ such that

$$f(\hat{P}) = \tilde{P}, \quad f(H) = \tilde{H}, \quad f(\eta) = \tilde{\eta}$$
$$f(\omega_2) = \tilde{\omega}, \quad f(h_1(\theta)) = b^t, \quad f(h^2(\xi)) = a^2b$$
$$f(h_0(\xi)) = ab^{(1-t(q^2+q+1))/2}.$$

t is an integer such that $1 \leqslant t \leqslant q-1$ and $(t, q-1) = 1$.

Proof. As in the proof of (2D) we can find an isomorphism f of $\hat{G}/K_0$ onto $PGL(3, q)$ such that $f(\hat{P}) = \tilde{P}$, $f(H) = \tilde{H}$, and $f(H\eta) = \tilde{H}\tilde{\eta}$. Now $\tilde{H} = \langle a, b\rangle$, and since H_1 centralizes X_2, it follows that $f(H_1) = \langle b\rangle$. Since $\hat{P}^{\omega_2} \cap \hat{P} = 1$ and $\tilde{P}^{\tilde{\omega}} \cap \tilde{P} = 1$, we have $f(\omega_2) = \tilde{h}\tilde{\omega}$ for some $\tilde{h}$ in $\tilde{H}$. Let $\tilde{h} = \begin{pmatrix} \alpha & & \\ & \beta & \\ & & 1 \end{pmatrix}$; then

$$(\tilde{h}\tilde{\omega})^2 = \begin{pmatrix} -\alpha & & \\ & \beta^2 & \\ & & -\alpha \end{pmatrix},$$

and since $f(\omega_2)$ has order 4, we must have $\beta^2 = \alpha$. Thus

$$f(\omega_2) = \begin{pmatrix} & & \beta^2 \\ & \beta & \\ -1 & & \end{pmatrix}.$$

Now

$$\begin{pmatrix} 1 & & \\ & 1 & \\ & & \beta \end{pmatrix} \begin{pmatrix} & & \beta^2 \\ & \beta & \\ -1 & & \end{pmatrix} \begin{pmatrix} 1 & & \\ & 1 & \\ & & \beta^{-1} \end{pmatrix} = \begin{pmatrix} & & \beta \\ & \beta & \\ -\beta & & \end{pmatrix},$$

and as in the proof of (2D), we may assume that $f(\omega_2) = \tilde{\omega}$. With f so fixed, we choose an element η of order a power of 3 so that $f(\eta) = \tilde{\eta}$. Moreover, we can assume

$$f(x_2(\alpha)) = \begin{pmatrix} 1 & 0 & \alpha \\ & 1 & 0 \\ & & 1 \end{pmatrix}, \quad f(x_{-2}(\alpha)) = \begin{pmatrix} 1 & & \\ 0 & 1 & \\ \alpha & 0 & 1 \end{pmatrix},$$

so in particular, $f(h_2(\xi)) = a^2b$. We define the integer t by the condition

$$f(h_1(\theta)) = b^t,$$

where $1 \leqslant t \leqslant q-1$ and $(t, q-1) = 1$. It follows that $f(h_1(\xi)) = b^{t(q^2+q+1)}$. Since $h_0(\xi)^2 = h_1(\xi^{-1})h_2(\xi)$, we have that

$$f(h_0(\xi))^2 = b^{-t(q^2+q+1)}(a^2b) = a^2b^{1-t(q^2+q+1)}.$$

Replacing $h_0(\xi)$ by $h_0(\xi)j$ if necessary, we may assume that

$$f(h_0(\xi)) = ab^{(1-t(q^2+q+1))/2}c,$$

where $c = \begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix}$ or $\begin{pmatrix} -1 & & \\ & 1 & \\ & & 1 \end{pmatrix}$. Since $h_0(\xi)$ transforms $x_2(\alpha)$ onto $x_2(\xi^{-1}\alpha)$, it follows that $c = 1$. This completes the proof.

The results obtained so far are unchanged if the isomorphism ϕ_1 of $SL(2, q)$ onto L_1 is replaced by the composition of ϕ_1 with the automorphism of L_1 induced by conjugation by an element h of H. Indeed, the subgroups X_1, X_{-1} are not changed, though their elements are relabeled; the elements of H_1 remain unchanged since H is abelian. So certainly (2A) and (2B) remain valid. (2C), (2D), and (2E) concern the subgroup $\hat{G} = \langle X_2, H, \eta, \omega_2\rangle$; the same isomorphism f, as well as the same choice of elements η and $h_0(\xi)$, work for the new ϕ_1. We shall refer to this change as a relabeling of L_1 by $L_1{}^h$.

3. In this section we show that the subgroup $N(H)$ has a unique multiplication table. We fix a choice of the elements η and $h_0(\xi)$ so that (2D) and (2E) hold.

Suppose first that case (A) or (B) holds. Since $H = H_1 \times H_0$, there are uniquely determined integers r, s, u, v modulo $q-1$ such that

$$\begin{aligned} h_1(\xi)^\eta &= h_1(\xi^r)h_0(\xi^s) \\ h_0(\xi)^\eta &= h_1(\xi^u)h_0(\xi^v) \end{aligned} \tag{3. 1}$$

We have the following result.

(3*A*) *In cases* (*A*) *and* (*B*) *the integer* t *of* (2*D*) *is* 1. *Moreover*, $r \equiv -2$, $s \equiv -3$, $u \equiv v \equiv 1$ (*mod* $q-1$).

Proof. By (2D) there exists an isomorphism f of $\hat{G}$ onto $SL(3, q)$ such that $f(h_1(\xi)) = (ab^{-1})^t$, $f(h_0(\xi)) = a^{(1-t)/2}b^{(1+t)/2}$, and $f(\eta) = \tilde{\eta}$, where a, b, $\tilde{\eta}$ have the meaning given in (2D). Since $\tilde{\eta} : a \longrightarrow (ab)^{-1}$ and $\tilde{\eta} : b \longrightarrow a$, it follows that

$$f(h_1(\xi^r)h_0(\xi^s)) = \tilde{\eta}^{-1}f(h_1(\xi))\tilde{\eta} = a^{-2t}b^{-t},$$

and so

$$(3.\ 2)\qquad \begin{aligned} tr + \frac{1}{2}(1-t)s &\equiv -2t \\ -tr + \frac{1}{2}(1+t)s &\equiv -t \end{aligned} \qquad (\mathrm{mod}\ q-1).$$

The sum of these two congruences is

$$(3.\ 3)\qquad s \equiv -3t \ (\mathrm{mod}\ q-1).$$

If this is substituted back into the first congruence of (3. 2) and the common factor t, which is relatively prime to $q-1$, is cancelled, we find that

$$(3.\ 4)\qquad r \equiv -2 + \frac{3}{2}(1-t) \ (\mathrm{mod}\ q-1)$$

Suppose case (A) holds. By (2B) the subspaces of $\mathscr{V}$ determined by $X_{-2}^{\eta_2^2}$ and $X_1^{\eta^2}$ modulo X_2 are the lines $\mathscr{L}_4$ and $\mathscr{L}_2$. Moreover, $h_1(\xi)$ acts as scalar multiplication on each of these two lines, and (1. 1) shows that the scalar multiple on $\mathscr{L}_4$ is the inverse cube of that on $\mathscr{L}_2$. On the other hand, using (2. 4) and (3. 1), we see that

$$\begin{aligned} h_1(\xi) &: x_2(\alpha)^{\omega_2\eta^2} \longrightarrow x_2(\alpha\xi^s)^{\omega_2\eta^2} \\ h_1(\xi) &: x_1(\alpha)^{\eta^2} \longrightarrow x_1(a\xi^{-2r+s})^{\eta^2} \end{aligned}$$

Thus $3(-2r+s) \equiv -s$ (mod $q-1$) and so

$$(3.\ 5)\qquad 6r \equiv 4s \ (\mathrm{mod}\ q-1).$$

Substituting (3. 3) and (3. 4) into (3. 5) then gives $-12 + 9(1-t) \equiv -12t$ (mod $q-1$), and thus $3t \equiv 3$ (mod $q-1$). Now t is an integer such that $1 \leqslant t \leqslant q-1$ and $(t, q-1) = 1$. If $t = 1$, then $r \equiv -2$, $s \equiv -3$ (mod q—1) by (3. 4) and (3. 5). Moreover, $f(h_0(\xi)) = b$, $f(h_1(\xi)) = ab^{-1}$, so that $f(h_0(\xi))^{\tilde{\eta}} = \tilde{\eta}^{-1}b\tilde{\eta} = a$, and $u \equiv v \equiv 1$ (mod $q-1$).

We may then assume $q \equiv 1$ (mod 3), and $t = 1 + \frac{1}{3}(q-1)$ or $t = 1 + \frac{2}{3}(q-1)$. Let

$$U = X_1 X_1^{\eta^2} X_{-1}^{\eta} X_{-2}^{\eta_2^2} X_2, \quad U_0 = X_{-1}^{\eta} X_{-2}^{\eta_2^2} X_2.$$

X_{-2}^{η} normalizes U_0 and $X_1^{\eta^2} X_{-1}^{\eta} X_{-2}^{\eta_2^2} X_2$ since the subgroup M/X_2 is abelian. By (2B) the subspaces of $\mathscr{V}$ determined by X_{-2}^{η}, $X_1^{\eta^2}$, X_{-1}^{η}, $X_{-2}^{\eta_2^2}$ modulo X_2 are the lines $\mathscr{L}_1$, $\mathscr{L}_2$, $\mathscr{L}_3$, $\mathscr{L}_4$. Thus by (1. 1) X_{-2}^{η} normalizes U as well. Since U and U_0 admit ω_2^{η}, it follows that L_2^{η} has a representation $\mathfrak{U}$ on the factor group $\mathscr{U} = U/U_0$. Since $|\mathscr{U}| = q^2$ and j inverts $\mathscr{U}$, this representation is irreducible over F_p. But $[L_2^\eta, H_1^\eta] = 1$ and H_1^η normalizes $\mathscr{U}$. As in an earlier argument, we see that H_1^η acts on $\mathscr{U}$ as scalar multiplication by elements of F_q. Thus $\mathscr{U}$ can be considered as a vector space over F_q which admits L_2^η as an irreducible group of linear transformations. It now follows that with respect to a suitable basis, $\mathfrak{U}$ has the form Γ^τ, where τ is a field automorphism of F_q. An element a^η of L_2^η is thus represented by the matrix a^τ. Since $X_1^{\eta 2}U_0/U_0$ and X_1U_0/U_0 admit H_2^η, $[X_1^{\eta 2}, X_{-2}^\eta] \leqslant X_2$, and ω_2^η interchanges $X_1^{\eta 2}U_0/U_0$ and X_1U_0/U_0, it follows by the remarks of **§1**, (I) that the subspace X_1U_0/U_0 is the line $\mathscr{L}_2$ of **§1**, (I). In particular, $h_2(\xi)^\eta$ acts on X_1U_0/U_0 as multiplication by the scalar $\xi^{-\tau}$.

Suppose $t = 1 + \frac{1}{3}(q-1)$. By (2D) we have

$$f(h_1(\xi)) = a^{1+(q-1)/3}b^{-1-(q-1)/3} \tag{3. 6}$$
$$f(h_0(\xi)) = a^{-(q-1)/6}b^{1+(q-1)/6}.$$

Since t is relatively prime to $q-1$, we may choose an integer w such that $w\left(1 + \frac{1}{3}(q-1)\right) \equiv 1 \pmod{q-1}$. Now from (3. 6) we find that

$$b^{1+(q-1)/3} = f(h_1(\xi)^{(q-1)/6}h_0(\xi)^{1+(q-1)/3})$$

and so

$$b = f(h_1(\xi)^{w(q-1)/6}h_0(\xi)). \tag{3. 7}$$

Since $f(h_2(\xi)^\eta) = (ab)^{\tilde{\eta}} = b^{-1}$, it follows by (3. 7) that

$$h_2(\xi)^\eta = h_1(\xi)^{-w(q-1)/6}h_0(\xi)^{-1},$$

and so in particular,

$$h_2(\xi)^\eta : x_1(a) \longrightarrow x_1(\alpha\xi^{-1+w(q-1)/3}).$$

Thus $\xi^\tau = \xi^{1-w(q-1)/3}$ and τ fixes the $1 + \frac{1}{3}(q-1)$ elements of $(F_q)^3$. Now any proper subfield of F_q has at most $\sqrt{q}$ elements. If τ is non-trivial, then $1 + \frac{1}{3}(q-1) \leqslant \sqrt{q}$, which is a contradiction since $q \geqslant 5$ in case (A). On the other hand, if τ is trivial, then $\xi^{-w(q-1)/3} = 1$, which is also impossible. The case $t = 1 + \frac{2}{3}(q-1)$ can be excluded in a similar fashion.

Suppose case (B) holds. Let $\mathscr{L}$ be the subspace of $\mathscr{V}$ determined by $X_{-2}^{\eta 2}$ modulo X_2. (2. 4) and (3. 1) show that $h_1(\xi)$ acts on $\mathscr{L}$ as multiplication by the scalar ξ^s. By (2B) $\mathscr{L}$ is a line in $\langle\mathscr{L}_2, \mathscr{L}_4\rangle$ different from $\mathscr{L}_4$, and $\mathscr{L} = \mathscr{L}_2$ if the automorphism ρ appearing in E is non-trivial. Whichever is the case, we have that the mapping $\alpha \longrightarrow \alpha^{-s}$ is a field automorphism of F_q. It then follows by (3. 3) that

$$3t \equiv p^i \pmod{q-1}, \tag{3. 8}$$

where i is an integer such that $0 < i \leqslant n$. In particular, (3. 8) shows that $q \not\equiv 1 \pmod 3$.

Using (2. 4) and (3. 1) we have as well that

$$\begin{aligned} h_1(\xi) &: x_1(\alpha)^{\eta^2} \longrightarrow x_1(\alpha\xi^{-2r+s})^{\eta^2} \\ h_1(\xi) &: x_1(\alpha)^{\omega_1\eta} \longrightarrow x_1(\alpha\xi^{2r^2+2su-rs-sv})^{\omega_1\eta} \\ h_1(\xi) &: x_2(\alpha)^{\omega_2\eta} \longrightarrow x_2(\alpha\xi^{rs+sv})^{\omega_2\eta}. \end{aligned}$$

The subspaces of $\mathscr{V}$ determined by $X_1^{\eta^2}$, X_{-1}^{η}, X_{-2}^{η} modulo X_2 are thus also lines of $\mathscr{V}$ invariant under the action of $h_1(\xi)$. Since ω_1 inverts $h_1(\xi)$ and interchanges X_{-2}^{η}, $X_{-2}^{\eta^2}$ as well as X_{-1}^{η}, $X_1^{\eta^2}$, it follows that

$$\left.\begin{aligned} rs + sv &\equiv -s \\ -2r + s &\equiv -2r^2 - 2su + rs + sv \end{aligned}\right. \qquad \pmod{q-1}. \tag{3. 9}$$

s and $q-1$ are relatively prime by (3. 3), (3. 8). Cancelling s from the first congruence in (3. 9), we have then

$$r + v \equiv -1 \pmod{q-1} \tag{3. 10}$$

so that by (3. 4)

$$v \equiv 1 - \frac{3}{2}(1-t) \pmod{q-1}. \tag{3. 11}$$

The second congruence in (3. 9) can be simplified by (3. 10) to

$$2su \equiv 2r - 2r^2 - 2s \pmod{q-1}. \tag{3. 12}$$

Now (2. 4) and (3. 1) also give

$$\begin{aligned} h_2(\xi) &: x_1(\alpha)^{\eta^2} \longrightarrow x_1(\alpha\xi^{-2r-4u+s+2v})^{\eta^2} \\ h_2(\xi) &: x_2(\alpha)^{\omega_2\eta^2} \longrightarrow x_2(\alpha\xi^{s+2v})^{\omega_2\eta^2} \end{aligned}$$

Since $h_2(\xi)$ acts on $\mathscr{V}$ as multiplication by a scalar, it follows that

$$s + 2v \equiv -2r - 4u + s + 2v \pmod{q-1}$$

and so

$$(3.\ 13) \qquad 2r+4u\equiv 0 \pmod{q-1}.$$

Multiplying (3. 13) by s and using (3. 12) to eliminate the term $4su$, we find that

$$(3.\ 14) \qquad 2rs+4r-4r^2-4s\equiv 0 \pmod{q-1}.$$

But now (3. 3), (3. 4), (3. 8), (3. 14) give

$$(-1-p^i)(-p^i)-2-2p^i-(1+p^i)^2+4p^i\equiv 0 \pmod{q-1},$$

which simplifies to

$$(3.\ 15) \qquad p^i\equiv 3 \pmod{q-1}.$$

Since $(3, q-1)=1$, (3. 15) and (3. 8) show that $t\equiv 1 \pmod{q-1}$, and so $t=1$, as $1\leqslant t\leqslant q-1$. It now follows by (3. 3), (3. 4), and (3. 11) that $r\equiv -2$, $s\equiv -3$, $v\equiv 1 \pmod{q-1}$. That $u\equiv 1 \pmod{q-1}$ can be proved as for case (A). This completes the proof.

(3*B*) *In case* (*A*) *the automorphism* σ *appearing in* $\mathfrak{B}$ *is trivial. In case* (*B*), $p=3$ *and* $q=3^n$. *If* $q=3^n>3$, *then the automorphisms* ρ *and* σ *appearing in* E *and* $\mathfrak{B}$ *are respectively the mappings* $\alpha\longrightarrow\alpha^3$ *and the identity. If* $q=3$, *then* ρ *and* σ *are the identy. The subspaces of* $\mathscr{V}$ *determined by* X_{-2}^{η}, $X_{-2}^{\eta^2}$, $X_{1}^{\eta^2}$, X_{-1}^{η} *modulo* X_2 *are* $\mathscr{L}_1$, $\mathscr{L}_2$, $\mathscr{L}_3$, $\mathscr{L}_4$ *respectively.*

Proof. We use the notation and calculations of the preceding proof. From the congruences for r, s, u, v given in (3A), we have that

$$(3.\ 16) \qquad h_1(\xi):\begin{cases} x_2(\alpha)^{\omega_2\eta}\longrightarrow x_2(\alpha\xi^3)^{\omega_2\eta} \\ x_2(\alpha)^{\omega_2\eta^2}\longrightarrow x_2(\alpha\xi^{-3})^{\omega_2\eta^2} \\ x_1(\alpha)^{\eta^2}\longrightarrow x_1(a\xi)^{\eta^2} \\ x_1(\alpha)^{\omega_1\eta}\longrightarrow x_1(\alpha\xi^{-1})^{\omega_1\eta}. \end{cases}$$

In case (A) the subspace of $\mathscr{V}$ determined by X_{-2}^{η} modulo X_2 is $\mathscr{L}_1$. Since $\mathfrak{B}=\Gamma^{(3)\sigma}$ in case (A), it follows from (1. 1) and (3. 16) that σ is trivial.

In case (B) we proceed as follows. Since p is odd and $0<i\leqslant n$, we have $3\leqslant p^i\leqslant q$. On the other hand, $p^i\equiv 3 \pmod{q-1}$ by (3. 15), and so $p^i=3$ and $p=3$. Suppose $q>3$. It then follows from (3. 16) that the subspaces of $\mathscr{V}$ determined by X_{-2}^{η}, $X_{-2}^{\eta^2}$, $X_{1}^{\eta^2}$, X_{-1}^{η} modulo X_2 are characteristic subspaces for $h_1(\xi)$ corresponding to four distinct characteristic values.

These subspaces must then coincide up to order with the lines $\mathscr{L}_1$, $\mathscr{L}_2$, $\mathscr{L}_3$, $\mathscr{L}_4$. Since $\mathfrak{B} = E^{\sigma}$, it follows by (1. 2) and (3. 16) that ρ is non-trivial. By (2B) the subspace of $\mathscr{V}$ determined by $X_{-2}^{\eta 2}$ is $\mathscr{L}_2$; the subspace determined by X_{-2}^{η} is then $\mathscr{L}_2^{\omega_1}$, which is $\mathscr{L}_1$. Since $[X_{-1}^{\eta}, X_1] \leqslant X_{-2}^{\eta 2} X_2$ by [5] (7C), the subspace of $\mathscr{V}$ determined by X_{-1}^{η} can only be $\mathscr{L}_4$, and thus the subspace determined by $X_1^{\eta 2}$ is $\mathscr{L}_3$. It now follows from (1. 2) and (3. 16) that σ is trivial and ρ is the mapping $\alpha \longrightarrow \alpha^3$. If $q = 3$, then ρ and σ can only be the identity automorphism. By (3. 16) the line $\mathscr{L}_4$ of $\mathscr{V}$ must be contained in the subspace of $\mathscr{V}$ determined by $\langle X_{-2}^{\eta 2}, X_{-1}^{\eta} \rangle$ modulo X_2. If $\mathscr{L}_4$ is not X_{-1}^{η} modulo X_2, then a non-zero vector v in $\mathscr{L}_4$ can be represented in the form

$$v \equiv x_{-1}(\alpha)^{\eta} x_{-2}(\beta)^{\eta^2} \pmod{X_2},$$

where α, β are non-zero elements in F_3. But $\mathscr{L}_4$ admits D, and so the three distinct vectors

$$v^j, \quad v^{j1}, \quad v^{j2}$$

are also in $\mathscr{L}_4$. This is clearly impossible, and so $\mathscr{L}_4$ is X_{-1}^{η} modulo X_2. The proof can now be completed as before. This completes the proof of (3B).

Suppose now that case (C) holds. $H = H_1 \times H_0$ and so $h_1(\theta)^{\eta}$ and $h_0(\xi)^{\eta}$ can be expressed as products of powers of $h_1(\theta)$ and $h_0(\xi)$. Since $h_0(\xi)^{\eta}$ has order dividing $q-1$, we see that there are integers r, s modulo $q^3 - 1$, and u, v modulo $q-1$, such that

$$\begin{aligned} h_1(\theta)^{\eta} &= h_1(\theta^r) h_0(\theta^s) \\ h_0(\xi)^{\eta} &= h_1(\xi^u) h_0(\xi^v) . \end{aligned} \tag{3. 17}$$

The field element θ^s is necessarily in F_q, and so we may choose s so that $s = s_0(q^2 + q + 1)$ and $\theta^s = \xi^{s_0}$.

(3C) *In case* (C) *the integer* t *of* (2E) *is* $q-2$. *Moreover*, $r \equiv -q^2 - q$, $s \equiv -q^2 - q - 1 \pmod{q^3 - 1}$, *and* $u \equiv v \equiv 1 \pmod{q-1}$ *if* $q \not\equiv 1 \pmod 3$. *The same congruences hold if* $q \equiv 1 \pmod 3$ *and* θ *is chosen suitably.*

Proof. By (2E) there exists an isomorphism f of $\hat{G}/K_0$ onto $PGL(3, q)$ such that $f(h_1(\theta)) = b^t$, $f(h_0(\xi)) = ab^{(1-t(q^2+q+1))/2}$, and $f(\eta) = \tilde{\eta}$, where a, b, $\tilde{\eta}$ have the meaning given in (2E). We represent elements of $\hat{G}/K_0$ and $PGL(3, q)$ by elements in the corresponding cosets of $\hat{G}$ and $GL(3, q)$. Since

$\tilde{\eta} : a \longrightarrow (ab)^{-1}$ and $\tilde{\eta} : b \longrightarrow a$, it follows that

$$f(h_1(\theta^r)h_0(\theta^s)) = \tilde{\eta}^{-1}f(h_1(\theta))\tilde{\eta} = a^t$$

and so

$$\begin{aligned} &s_0 \equiv t \\ &rt + \frac{1}{2}(1 - t(q^2 + q + 1))s_0 \equiv 0 \end{aligned} \qquad (\mathrm{mod}\ q-1) \tag{3. 18}$$

Since t and $q-1$ are relatively prime, the second congruence can be expressed as

$$r \equiv -\frac{1}{2}(1 - t(q^2 + q + 1)) \quad (\mathrm{mod}\ q-1) \tag{3. 19}$$

By (2B) the subspaces of $\mathscr{V}$ determined by $X_{-2}^{\eta 2}$, X_{-2}^{η}, and $X_1^{\eta 2}$ modulo X_2 are the subspaces $\mathscr{L}_4$, $\mathscr{L}_1$, and $\mathscr{L}_2$ respectively. Using (2. 4) and (3. 17) we see that

$$h_1(\theta) : \begin{cases} x_2(\alpha)^{\omega_2\eta^2} \longrightarrow x_2(\alpha\theta^s)^{\omega_2\eta^2} \\ x_2(\alpha)^{\omega_2\eta} \longrightarrow x_2(\alpha\theta^{rs+sv})^{\omega_2\eta} \\ x_1(\alpha)^{\eta^2} \longrightarrow x_1(\alpha\theta^{s-2r})^{\eta^2} . \end{cases}$$

It now follows from (1. 3) that $s \equiv -rs - sv$ $(\mathrm{mod}\ q^3 - 1)$, and so

$$r + v \equiv -1 \ (\mathrm{mod}\ q-1) \tag{3. 20}$$

Moreover, (1. 3) shows that $\theta^{rs+sv} = N(\theta^{s-2r})$, where N is the relative norm of the extension F_{q^3}/F_q, so that

$$-s_0 \equiv s - 2r \ (\mathrm{mod}\ q-1). \tag{3. 21}$$

Thus by (3. 21) and (3. 18) we have

$$2r \equiv s + s_0 \equiv s_0(q^2 + q + 2) \equiv 4t \ \ (\mathrm{mod}\ \ q-1)$$

On the other hand, we have by (3. 19) that

$$2r \equiv -1 + 3t \ (\mathrm{mod}\ q-1).$$

These last two congruences show that $t \equiv -1$ $(\mathrm{mod}\ q-1)$. Since t is an integer with $1 \leqslant t < q-1$, it follows that $t = q-2$ as claimed.˙ Also, $s = s_0(q^2 + q + 1)$ so that $s \equiv -q^2 - q - 1$ $(\mathrm{mod}\ q^3 - 1)$ by (3. 18).

Now (3. 19) and $t = q-2$ imply that

$$2r \equiv -1 + (q-2)(q^2+q+1) \pmod{2(q-1)}.$$

But $-1+(q-2)(q^2+q+1) = (q-1)(q^2-1)-4 \equiv -4 \pmod{2(q-1)}$, and so

$$r \equiv -2, \quad v \equiv 1 \pmod{q-1}, \tag{3. 22}$$

the last congruence following from (3. 20). Again (2. 14) and (3. 17) give

$$h_2(\xi) : \begin{cases} x_2(\alpha)^{\omega_2\eta^2} \longrightarrow x_2(\alpha\xi^{s+2v})^{\omega_2\eta^2} \\ x_1(\alpha)^{\eta^2} \longrightarrow x_1(\alpha\xi^{s+2v-4u-2r})^{\eta^2}. \end{cases}$$

Since $h_2(\xi)$ acts on $\mathscr{V}$ as multiplication by a scalar, it follows that

$$s+2v \equiv s+2v-2r-4u \pmod{q-1}$$

and so by (3. 22)

$$4u \equiv 4 \pmod{q-1}.$$

Thus

$$h_0(\xi)^\eta = h_1(\xi)h_0(\xi)c, \tag{3. 23}$$

where c is an element in H_1 of order dividing 4. Using (3. 23), (3. 17), and the congruences $r \equiv -2$, $s \equiv -3$, $v \equiv 1 \pmod{q-1}$, we can compute that

$$h_1(\xi)^{\eta^3} = h_1(\xi)c^3(c^{-3})^\eta.$$

But $\eta^3 \in H$ and so centralizes $h_1(\xi)$. Thus $(c^3)^\eta = c^3$, and η must centralize c. Since η centralizes no involution in H, it follows that $c=1$ and $u \equiv 1 \pmod{q-1}$.

The subgroup $K_0 = (H_1)^{q-1}$ is central in $\hat{G}$. In particular, we have from (3. 17) that

$$h_1(\theta)^{q-1} = h_1(\theta)^{\eta(q-1)} = h_1(\theta^{r(q-1)}),$$

and so

$$r \equiv 1 \pmod{q^2+q+1}.$$

Let $r = 1 + r_0(q^2+q+1)$; using (3. 22) we see that $3r_0 \equiv -3 \pmod{q-1}$. If $q \not\equiv 1 \pmod 3$, then $r_0 \equiv -1 \pmod{q-1}$, and so $r \equiv -q^2-q \pmod{q^3-1}$ as claimed. If $q \equiv 1 \pmod 3$ and $r_0 \not\equiv -1 \pmod{q-1}$, then

$$r \equiv -q^2-q+\frac{1}{3}(q^3-1) \quad \text{or} \quad -q^2-q+\frac{2}{3}(q^3-1) \pmod{q^3-1}.$$

Let ζ accordingly be $\theta^{2(q^3-1)/3}$ or $\theta^{(q^3-1)/3}$. Since $q^2+q+1\equiv 0 \pmod 3$, we have that $N(\theta\zeta)=\xi$, and since $q\equiv 1 \pmod 3$, we have that $h_1(\zeta)$ belongs to K_0 and hence commutes with η. If θ is replaced by $\theta\zeta$, the integer s (mod q^3-1) and the integers u, v (mod $q-1$) of (3. 17) are unaffected by this change by what we have already proved. On the other hand, r is changed to $-q^2-q$ (mod q^3-1). This completes the proof.

(3D) *In case* (C) *the automorphism σ appearing in $\mathfrak{V}$ is trivial.*

Proof. Using the calculations of the preceding proof and the congruences for s in (3C), we see that

$$h_1(\theta) : x_{-2}(\alpha)^{\eta^2} \longrightarrow x_{-2}(\alpha\theta^{-q^2-q-1})^{\eta^2}.$$

Since the subspace of $\mathscr{V}$ determined by $X_{-2}^{\eta^2}$ modulo X_2 is $\mathscr{L}_4$, it follows from (1. 3) that σ is trivial.

(3E) *There exists an element η_0 in ηH such that*

$$\eta_0{}^3=1,\ \ \omega_1^{-1}\eta_0\omega_1=\eta_0{}^2j,\ \ \omega_2^{-1}\eta_0\omega_2=\eta_0{}^2j_2,$$

provided a possible relabeling of L_1 by $L_1{}^{h_0(\xi)}$ is made. In particular, $N(H)$ has a unique multiplication table.

Proof. Suppose first that case (A) or (B) holds. Since $\eta : j\longrightarrow j_1\longrightarrow j_2$ and $j=h_1(-1)$, it follows from (2D) and (3A) that

$$j_1=h_0(-1),\ \ j_2=h_1(-1)h_0(-1) \tag{3. 24}$$

Now

$$\eta^3=1,\ \ \omega_2^{-1}\eta\omega_2=\eta^2j_2, \tag{3. 25}$$

since the corresponding equations hold in $f(\hat{G})$. Set then

$$\omega_1^{-1}\eta\omega_1=\eta^2h_1(\alpha)h_0(\beta).$$

The square of the right-hand side can be computed from (3A) and (3. 25); we have

$$\omega_1^{-1}\eta^2\omega_1=\eta h_1(\alpha^2\beta^{-1})h_0(\alpha^3\beta^{-1}),$$

and so

$$\omega_1^{-1}\eta\omega_1 = \eta^2 j h_0(\beta).$$

We may assume β is a square in F_q by relabeling L_1 by $L_1^{h_0(\xi)}$, since the transform of η by $\omega_1^{h_0(\xi)}$ is $\eta^2 j h_0(\xi^3\beta)$. If γ is an element in F_q such that $\beta\gamma^2 = 1$, and if we set

$$\eta_0 = \eta h_1(\gamma) h_0(\gamma),$$

then η_0 satisfies the equations of (3E). The multiplication table of $N(H)$ is then unique by (3A).

Suppose now that case (C) holds. Since $\eta : j \longrightarrow j_1 \longrightarrow i_2$, $j = h_1(-1)$, and $\frac{1}{2}(1-(q-2)(q^2+q+1))$ is even, we have by (2E) and (3C) that (3. 24) holds. Moreover,

$$\eta^3 \equiv 1, \quad \omega_2^{-1}\eta\omega_2 = \eta^{-1}j_2 \pmod{K_0},$$

since the corresponding equations hold in $f(\hat{G})$. Thus $\eta^3 = \kappa$, $\omega_2^{-1}\eta\omega_2 = \eta^{-1}j_2\lambda$, where κ, λ are elements in K_0, and κ has order a power of 3. Since $K_0 \leqslant Z(\hat{G})$, it follows that

$$\kappa = \eta^3 = \omega_2^{-1}\eta^3\omega_2 = (\eta^{-1}j_2\lambda)^3 = \eta^{-3}\lambda^3,$$

and so $\lambda^3 = \kappa^2$. κ has order a power of 3, so there exists an integer i such that $\lambda^{3i} = \kappa$. Since

$$(\eta\lambda^{-i})^3 = \eta^3\lambda^{-3i} = \kappa\kappa^{-1} = 1,$$

we may assume $\eta^3 = 1$ by replacing η by $\eta\lambda^{-i}$. It then follows from (3C) that $(\eta h)^3 = 1$ as well, where h is any element in H of the form $h_1(\alpha)h_0(\beta)$ with α, β in F_q. Let $\omega_2^{-1}\eta\omega_2 = \eta^{-1}j_2\mu$, where μ belongs to K_0. Since $\eta^3 = 1$, the cube of this last equation gives $\mu^3 = 1$. If $\mu \neq 1$, then q^2+q+1 and $q-1$ are divisible by 3, and it then follows that μ is in $H_1^{q^2+q+1}$. Replacing η by $\eta\mu$, we may henceforth assume that (3. 25) holds.

Suppose

$$\omega_1^{-1}\eta\omega_1 = \eta^2 h_1(\alpha) h_0(\beta),$$

where $\alpha \in F_{q^3}$ and $\beta \in F_q$. The square of the right-hand side can be computed by (3C); we find

$$\omega_1^{-1}\eta^2\omega_1 = \eta h_1(\alpha^2\beta^{-1}) h_0(\alpha^{q^2+q+1}\beta^{-1})$$

and so

$$\omega_1^{-2}\eta\omega_1^{2} = \eta h_1(\alpha)h_0(\alpha^{q^2+q+1}).$$

Since $\omega_1^{2} = j$ and $j^{-1}\eta j = \eta j_2$, it follows by (3. 24) that $\alpha = -1$ so that

$$\omega_1^{-1}\eta\omega_1 = \eta^2 j h_0(\beta).$$

The proof can now be completed exactly as in the cases (A) and (B).

4. In this section we shall show that the subgroup $B = HP$ has a unique multiplication table. We fix a choice of the elements η_0 and $h_0(\xi)$ so that (3E) holds. To simplify notation, we shall write η_0 as η; η will always have this meaning for the remainder of the paper.

(A) *Suppose case* (A) *holds. If* v_1, v_2, v_3, v_4 *are the vectors in* $\mathscr{V}$ *determined by* $x_{-2}(-1)^{\eta}$, $x_1(3^{-1})^{\eta^2}$, $x_{-1}(3^{-1})^{\eta}$, $x_{-2}(1)^{\eta^2}$ *modulo* X_2 *respectively, then* $\{v_1, v_2, v_3, v_4\}$ *is a basis for* $\mathscr{V}$ *such that the corresponding matrix form of* $\mathfrak{V}$ *is* $\Gamma^{(3)}$.

Proof. The lines generated in $\mathscr{V}$ by v_1, v_2, v_3, v_4 are by (2B) the lines $\mathscr{L}_1, \mathscr{L}_2, \mathscr{L}_3, \mathscr{L}_4$ respectively. Thus there exists a basis $\mathscr{B}$ of $\mathscr{V}$ consisting of suitable scalar multiples of the v_i such that the matrix form of $\mathfrak{V}$ with respect to $\mathscr{B}$ is $\Gamma^{(3)}$. Using (3E) we calculate that

$$\omega_1 : v_4 \longrightarrow -v_1, \quad v_3 \longrightarrow v_2.$$

If we compare this with (1. 1), we see that we may assume that $\mathscr{B}$ consists of the vectors

$$v_1, \ \alpha v_2, \ \alpha v_3, \ v_4, \tag{4. 1}$$

where α is a scalar in F_q. Consider the representation $\mathfrak{U}$ of L_2^{η} constructed in the proof of (3A). There it was proved that if u_1 is the vector determined by $x_1(1)^{\eta^2}$ modulo U_0, and if $u_2 = u_1^{\omega_2\eta}$, then $\{u_1, u_2\}$ is a basis of U/U_0 such that the corresponding matrix form of $\mathfrak{U}$ is Γ^{τ}, where τ is a field automorphism of F_q. (The η appearing in (3A) has been changed to η_0, but it is clear that the above considerations apply.) Using (3E) we see that $\omega_2^{\eta} : x_1(1)^{\eta^2} \longrightarrow x_1(1)$, so that u_2 is the vector determined by $x_1(1)$ modulo U_0. In particular, it follows that

$$[x_{-2}(\beta)^{\eta}, x_1(\gamma)] \equiv x_1(-\beta^{\tau}\gamma)^{\eta^2} \pmod{U_0}$$

On the other hand, (4. 1) and (1. 1) imply that

$$[x_{-2}(\beta)^{\eta}, x_1(\gamma)] \equiv x_1(-\alpha\beta\gamma)^{\eta^2} \pmod{U_0}.$$

Thus $\beta^{\tau}\gamma = \alpha\beta\gamma$ for all β, γ in F_q. Setting $\beta = \gamma = 1$, we get that $\alpha = 1$, and so $\mathscr{B}$ is as claimed.

(4B) *Suppose case* (B) *holds. If v_1, v_2, v_3, v_4 are the vectors in $\mathscr{V}$ determined by $x_{-2}(-1)^{\gamma}$, $x_{-2}(1)^{\gamma^2}$, $x_1(-1)^{\gamma^2}$, $x_{-1}(1)^{\gamma}$ modulo X_2 respectively, then $\{v_1, v_2, v_3, v_4\}$ is a basis for $\mathscr{V}$ such that the corresponding matrix form of $\mathfrak{B}$ is E.*

Proof. The lines generated in $\mathscr{V}$ by v_1, v_2, v_3, v_4 are by (3B) the lines $\mathscr{L}_1$, $\mathscr{L}_2$, $\mathscr{L}_3$, $\mathscr{L}_4$ respectively. Thus there exists a basis $\mathscr{B}$ of $\mathscr{V}$ consisting of suitable scalar multiples of the v_i such that the matrix form of $\mathfrak{B}$ with respect to $\mathscr{B}$ is E. Using (3E) we find that

$$\omega_1 : v_4 \longrightarrow -v_3, \quad v_2 \longrightarrow -v_1.$$

If we compare this with (1. 2), we see that we may assume that $\mathscr{B}$ consists of the vectors

$$v_1, \ v_2, \ \alpha v_3, \ \alpha v_4, \tag{4. 2}$$

where α is a scalar in F_q. Since the matrix form of $\mathfrak{B}$ with respect to $\{v_1, v_2, v_3, v_4\}$ has essentially the same properties as E, differing only in the entries $*$ of (1. 2), we may change E so that (4B) holds.

(4C) *Suppose case* (C) *holds. If $v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8$ are the vectors in $\mathscr{V}$ determined by $x_{-2}(-1)^{\gamma}$, $x_1(-1)^{\gamma^2}$, $x_1(-\theta^2)^{\gamma^2}$, $x_1(-\theta)^{\gamma^2}$, $x_{-1}(-1)^{\gamma}$, $x_{-1}(-\theta)^{\gamma}$, $x_{-1}(-\theta^2)^{\gamma}$, $x_{-2}(1)^{\gamma^2}$ modulo X_2 respectively, then the v_i form a basis for $\mathscr{V}$ such that the corresponding matrix form of $\mathfrak{B}$ is Γ_0.*

Proof. The subspaces of $\mathscr{V}$ spanned over F_q by v_1; v_2, v_3, v_4; v_5, v_6, v_7; v_8 respectively are by (2B) the subspaces $\mathscr{L}_1$, $\mathscr{L}_2$, $\mathscr{L}_3$, $\mathscr{L}_4$. There thus exists a basis $\mathscr{B} = \{u_1, u_2, u_3, u_4, u_5, u_6, u_7, u_8\}$ of $\mathscr{V}$ with u_1 in $\mathscr{L}_1$, u_2, u_3, u_4 in $\mathscr{L}_2$, u_5, u_6, u_7 in $\mathscr{L}_3$, u_8 in $\mathscr{L}_4$ such that the matrix form of $\mathfrak{B}$ with respect to $\mathscr{B}$ is Γ_0. We can calculate using (3E) that $\omega_1 : v_8 \longrightarrow -v_1$. Comparing this with (1. 5), we see that we may assume

$$u_1 = v_1, \quad u_8 = v_8, \quad u_2 = x_1(\alpha)^{\gamma^2},$$

where α is a scalar in F_{q^3}. Now $q^2 + q - 1$ and $q^3 - 1$ are relatively prime, so there exists an integer i such that $\theta^{i(q^2+q-1)} = \theta$. By (1. 3) and (1. 6), we then have that $h_1(\theta^i) : u_2 \longrightarrow u_3 \longrightarrow u_4$. Using (3C) and (3E) we compute that $h_1(\theta^i) : x_1(\alpha)^{\gamma^2} \longrightarrow x_1(\theta\alpha)^{\gamma^2}$, and thus

$$u_2 = x_1(\alpha)^{\gamma^2}, \quad u_3 = x_1(\theta\alpha)^{\gamma^2}, \quad u_4 = x_1(\theta^2\alpha)^{\gamma^2}. \tag{4. 2}$$

Since $\omega_1 : x_1(\alpha)^{\eta^2} \longrightarrow x_{-1}(-\alpha)^\eta$, it now follows by (1. 5), (1. 6) that

$$u_5 = x_{-1}(a)^\eta,\ u_6 = x_{-1}(\theta\alpha)^\eta,\ u_7 = x_{-1}(\theta^2\alpha)^\eta. \tag{4. 3}$$

To evaluate α, we proceed as in the proof of (4A). Let $U = X_1X_1^{\eta^2}X_{-1}^\eta X_{-2}^{\eta^2}X_2$, $U_0 = X_{-1}^\eta X_{-2}^{\eta^2}X_2$. X_{-2}^η normalizes U_0 and $X_1^{\eta^2}X_{-1}^\eta X_{-2}^{\eta^2}X_2$, since the subgroup M/X_2 is abelian. The subspaces of $\mathscr{V}$ determined by X_{-2}^η, $X_1^{\eta^2}$, X_{-1}^η, $X_{-2}^{\eta^2}$ modulo X_2 are respectively $\mathscr{L}_1$, $\mathscr{L}_2$, $\mathscr{L}_3$, $\mathscr{L}_4$, and so it follows by (1. 4) that X_{-2}^η normalizes U as well. Since U and U_0 admit ω_2^η, L_2^η then has a representation $\mathfrak{U}$ on the factor group $\mathscr{U} = U/U_0$. Now $[L_2^\eta, H_1^\eta] = 1$, and using (3C) we can calculate that $h_1(\theta)^\eta$ acts on $\mathscr{U}$ as multiplication by the scalar θ^{q^2+q-1}. Since θ^{q^2+q-1} is a primitive root of unity of order q^3-1, we see that $\mathscr{U}$ can be considered as a 2-dimensional vector space over F_{q^3} with L_2^η as an irreducible group of linear transformations. With respect to a suitable basis, $\mathfrak{U}$ then has the form Γ^τ for some field automorphism τ of F_q, and an element a^η of L_2^η is then represented by the matrix a^τ. Since $X_1^{\eta^2}U_0/U_0$ and X_1U_0/U_0 admit H_2^η, $[X_1^{\eta^2}, X_{-2}^\eta] \leqslant X_2$, and $\omega_2^\eta : x_1(1)^{\eta^2} \longrightarrow x_1(1)$, it follows that the vectors of U determined by $x_1(1)^{\eta^2}$, $x_1(1)$ modulo U_0 form such a basis. In particular, we have that

$$[x_{-2}(\beta)^\eta,\ x_1(\theta)] \equiv x_1(-\beta^\tau\theta)^{\eta^2} \pmod{U_0}.$$

On the other hand, (4. 2), (1. 4), and (1. 6) imply that

$$[x_{-2}(\beta)^\eta,\ x_1(\theta)] \equiv x_1(\alpha\beta\theta)^{\eta^2} \pmod{U_0}.$$

Thus $-\beta^\tau\theta = \alpha\beta\theta$ for all β in F_q. Setting $\beta = 1$ and cancelling θ, we get that $\alpha = -1$, and thus the v_i and u_i coincide. This completes the proof.

(4D) $[x_{-2}(\alpha)^\eta, x_{-2}(\beta)^{\eta^2}] = x_2(-\alpha\beta)$ *for all* α, β *in* F_q.

Proof. Since $[X_{-2}^\eta, X_{-2}^{\eta^2}] = X_2$ by [5] (7B), it follows that X_{-2}^η normalizes the elementary abelian subgroup $Y = X_2X_{-2}^{\eta^2}$. Y also admits ω_2^η, and so L_2^η has a representation $\mathfrak{Y}$ on Y in which j^η inverts Y. Now $[L_2^\eta, H_1^\eta] = 1$ and H_1^η is faithful on Y. It follows easily that Y can be considered as a 2-dimensional vector space over F_q on which L_2^η acts as an irreducible group of linear transformations. With respect to a suitable basis, $\mathfrak{Y}$ then has the form Γ^τ for some field automorphism τ of F_q. Since X_2 and $X_{-2}^{\eta^2}$ admit H_2^η, $[X_2, X_{-2}^\eta] = 1$, and $\omega_2^\eta : x_2(1) \longrightarrow x_{-2}(1)^{\eta^2}$, it follows that $x_2(1)$, $x_{-2}(1)^{\eta^2}$ form such a basis. In particular,

$$[x_{-2}(\alpha)^\eta,\ x_{-2}(\beta)^{\eta^2}] = x_2(-\alpha^\tau\beta)$$

for all α, β in F_q. Using (3C) or (3E) we can calculate that $h_2(\gamma)^\eta : x_2(\delta) \rightarrow (x_2(\gamma\delta)$, and so τ is the trivial automorphism.

(4E) $[x_1(\alpha)^{\eta^2}, x_{-1}(\beta)^\eta] = x_2(-3\alpha\beta)$ *for all* α, β *in* F_q *in cases* (A) *and* (B). $[x_1(\alpha)^{\eta^2}, x_{-1}(\beta)^\eta] = x_2(\alpha\beta + \bar{\alpha}\bar{\beta} + \bar{\bar{\alpha}}\bar{\bar{\beta}})$ *for all* α, β *in* F_{q^3} *in case* (C).

Proof. Suppose first that case (A) holds. We note by [5] (6. 3) that $X_1 X_{-1}^\eta X_{-2}^{\eta^2}$ is a subgroup, and so by (4A) and (1. 1)

$$(4.\ 4) \qquad [x_1(\alpha), x_{-1}(\beta)^\eta] = x_{-2}(-3\alpha\beta)^{\eta^2}.$$

The result now follows by conjugating this relation by $\omega_2\eta^2$. Suppose case (B) holds. If $[X_1^{\eta^2}, X_{-1}^\eta] \neq 1$, then (4D) and [5] (7B) imply that $X_1^{\eta^2} X_{-1}^\eta X_2$ and $X_{-2}^\eta X_{-2}^{\eta^2} X_2$ are the centralizers of each other in the subgroup M. Since $X_1^{\eta^2} X_{-1}^\eta X_2$ and M admit L_1, it would follow that $X_{-2}^\eta X_{-2}^{\eta^2} X_2$ admits L_1 as well, contradicting the indecomposability of $\mathfrak{B}$. Thus $[X_1^{\eta^2}, X_{-1}^\eta] = 1$, which implies (4E) since F_q has characteristic 3.

Suppose finally that case (C) holds. As in the case (A), we note that $X_1 X_{-1}^\eta X_{-2}^{\eta^2}$ is a subgroup, so that by (4C), (1. 4), (1. 6)

$$(4.\ 5) \qquad [x_1(\alpha), x_{-1}(\beta)^\eta] = x_{-2}(\alpha\beta + \bar{\alpha}\bar{\beta} + \bar{\bar{\alpha}}\bar{\bar{\beta}})^{\eta^2}.$$

Conjugating this by $\omega_2\eta^2$ then gives (4E).

As a result of (4D), (4E), and [5] (7B), it follows that M has a unique multiplication table in all cases (A), (B), and (C). The next lemmas will show that P has a unique multiplication table as well. Since the action of H on P has been determined in §3, the subgroup $B = HP$ will then have a unique multiplication table.

(4F) *The following commutator relations hold in case* (A).

(i) $[x_{-1}(\beta)^\eta, x_1(\alpha)] = x_{-2}(3\alpha\beta)^{\eta^2}$

(ii) $[x_1(\beta)^{\eta^2}, x_1(\alpha)] = x_{-1}(2\alpha\beta)^\eta x_{-2}(3\alpha^2\beta)^{\eta^2} x_2(3\alpha\beta^2)$

(iii) $[x_{-2}(\beta)^\eta, x_1(\alpha)] = x_1(-\alpha\beta)^{\eta^2} x_{-1}(-\alpha^2\beta)^\eta x_{-2}(-\alpha^3\beta)^{\eta^2} x_2(\alpha^3\beta^2)$

(iv) $[X_{-2}^{\eta^2}, X_1] = 1$

In particular, $P = X_1 M$ *has a unique multiplication table.*

Proof. We have already seen in the proof of (4E) that $X_1 X_{-1}^\eta X_{-2}^{\eta^2}$ is a subgroup. Since $[X_1, X_{-2}^{\eta^2}] \leqslant X_2$ by [5] (7C), it follows that $[X_1, X_{-2}^{\eta^2}] \leqslant X_2 \cap X_1 X_{-1}^\eta X_{-2}^{\eta^2} = 1$, which proves (iv). (i) follows from (4. 4). (4A) and (1. 1) imply that

$$
\text{(4. 6)} \qquad
\begin{aligned}
&[x_1(\beta)^{\eta^2},\ x_1(\alpha)] = x_{-1}(2\alpha\beta)^{\eta}x_{-2}(3\alpha^2\beta)^{\eta^2}x_2(f(\alpha,\beta))\\
&[x_{-2}(\beta)^{\eta},\ x_1(\alpha)] = x_1(-\ \alpha\beta)^{\eta^2}x_{-1}(-\ \alpha^2\beta)^{\eta}x_{-2}(-\ \alpha^3\beta)^{\eta^2}x_2(g(\alpha,\beta))
\end{aligned}
$$

where f, g are functions from $F_q\times F_q$ into F_q. If we conjugate these relations by the element $h_1(\lambda)h_0(\mu)$ and compare coefficients in x_2, we find that

$$
\text{(4. 7)} \qquad
\begin{aligned}
f(\alpha\lambda^{-2}\mu,\ \beta\lambda\mu^{-1}) &= \mu^{-1}f(\alpha,\beta)\\
g(\alpha\lambda^{-2}\mu, \beta\lambda^3\mu^{-2}) &= \mu^{-1}g(\alpha,\beta).
\end{aligned}
$$

Setting $\lambda=\mu$, $\lambda^2=\mu$ successively in the first equation of (4. 7) shows that $f(\alpha,\beta)=\alpha\beta^2\gamma$ for some γ in F_q; setting $\lambda=\nu^2$, $\mu=\nu^3$ and then $\mu=\lambda^2$ successively in the second equation shows that $g(\alpha,\beta)=\alpha^3\beta^2\delta$ for some δ in F_q. To evaluate γ and δ, we use the commutator identity

$$
\text{(4. 8)} \qquad [xy,z]=[x,z][x,z,y][y,z]
$$

Setting $x=x_1(\mu)^{\eta^2}$, $y=x_1(\nu)^{\eta^2}$, $z=x_1(\alpha)$ in (4. 8) and taking into account (4E) and the fact that X_{-1}^{η}, $X_{-2}^{\eta^2}$, and X_2 centralize one another, we find by comparing the coefficients in x_2 that

$$
\alpha\gamma(\mu+\nu)^2=\alpha\gamma\mu^2+\alpha\gamma\nu^2+6\alpha\mu\nu.
$$

Thus $\gamma=3$, which proves (ii). Setting $x=x_{-2}(\mu)^{\eta}$, $y=x_{-2}(\nu)^{\eta}$, $z=x_1(\alpha)$ in (4. 8) and using (4D) and (4E), we find by comparing the coefficients in x_2 that

$$
\delta\alpha^3(\mu+\nu)^2=\delta\alpha^3\mu^2+\delta\alpha^3\nu^2-\alpha^3\mu\nu+3\alpha^3\mu\nu.
$$

Thus $\gamma=1$, which proves (iii).

(4G) *The following commutator relations hold in case* (B).

(i) $[x_1(\beta)^{\eta^2},\ x_1(\alpha)]=x_{-1}(-\ \alpha\beta)^{\eta}$

(ii) $[x_{-2}(\beta)^{\eta},\ x_1(\alpha)]=x_{-2}(-\ \alpha^3\beta)^{\eta^2}x_1(-\ \alpha\beta)^{\eta^2}x_{-1}(-\ \alpha^2\beta)^{\eta}x_2(\alpha^3\beta^2)$

(iii) $[X_{-1}^{\eta},\ X_1]=[X_{-2}^{\eta^2},\ X_1]=1.$

In particular, $P=X_1M$ *has a unique multiplication table.*

Proof. By [5] (7C) we have that $[X_1,\ X_{-2}^{\eta^2}]\leqslant X_2$, and the argument given for (4F) (iv) now shows that $[X_{-2}^{\eta^2},\ X_1]=1$. By (4E) we also have $[X_1^{\eta^2},\ X_{-1}^{\eta}]=1$; conjugating this by $\omega_2\eta^2$ then gives $[X_1,X_{-1}^{\eta}]=1$, which proves (iii).

Let $\mathscr{B}$ be the basis of $\mathscr{V}$ given in (4B), so that by (3B) the matrix form of $\mathfrak{V}$ with respect to this basis is E. Taking into account (4G) (iii), we have in particular that

$$(4.\ 9) \qquad \mathfrak{V}(x_1(\alpha)) = \begin{pmatrix} 1 & \alpha^3 & * & * \\ & 1 & 0 & 0 \\ & & 1 & \alpha \\ & & & 1 \end{pmatrix}.$$

Thus

$$[x_1(\beta)^{\eta^2},\ x_1(\alpha)] = x_{-1}(-\alpha\beta)^{\eta} x_2(f(\alpha,\beta)),$$

where f is a function from $F_q \times F_q$ into F_q. As in the proof of (4F), we find that $f(\alpha,\beta) = \alpha\beta^2\gamma$ for some γ in F_q. Setting $x = x_1(\mu)^{\eta^2}$, $y = x_1(\nu)^{\eta^2}$, $z = x_1(\alpha)$ in (4. 8) and comparing the coefficients in x_2, we find that

$$\alpha\gamma(\mu+\nu)^2 = \alpha\gamma\mu^2 + \alpha\gamma\nu^2,$$

so that $\gamma = 0$. This proves (i).

By (4. 9) and (4B) we have that

$$(4.\ 10) \qquad [x_{-2}(\beta)^{\eta}, x_1(\alpha)] = x_{-2}(-\alpha^3\beta)^{\eta^2} x_1(f(\alpha,\beta))^{\eta^2}.$$
$$x_{-1}(g(\alpha,\beta))^{\eta} x_2(h(\alpha,\beta)),$$

where f, g, h are functions from $F_q \times F_q$ into F_q. If we conjugate this relation by $h_1(\lambda)h_0(\mu)$ and compare coefficients, we find that

$$f(\alpha\lambda^{-2}\mu,\ \beta\lambda^3\mu^{-2}) = \lambda\mu^{-1}f(\alpha,\beta)$$
$$(4.\ 11) \qquad g(\alpha\lambda^{-2}\mu,\ \beta\lambda^3\mu^{-2}) = \lambda^{-1}g(\alpha,\beta)$$
$$h(\alpha\lambda^{-2}\mu,\ \beta\lambda^3\mu^{-2}) = \mu^{-1}h(\alpha,\beta).$$

Setting $\lambda = \nu^2$, $\mu = \nu^3$ and then $\mu = \lambda^2$ successively in each of the equations of (4. 11) shows that

$$f(\alpha,\beta) = \gamma\alpha\beta,\ \ g(\alpha,\beta) = \delta\alpha^2\beta,\ \ h(\alpha,\beta) = \varepsilon\alpha^3\beta^2,$$

where γ, δ, ε are elements in F_q.

To evaluate ε, we set $x = x_{-2}(\mu)^{\eta}$, $y = x_{-2}(\nu)^{\eta}$, $z = x_1(\alpha)$ in (4. 8), and compare coefficients in x_2. This gives

$$\varepsilon\alpha^3(\mu+\nu)^2 = \varepsilon\alpha^3\mu^2 + \varepsilon\alpha^3\nu^2 - \alpha^3\mu\nu,$$

so that $2\varepsilon = -1$, and $\varepsilon = 1$. Now (4. 10) implies that X_{-2}^{η} normalizes $U = X_1 X_1^{\eta^2} X_{-1}^{\eta} X_{-2}^{\eta^2} X_2$, a group which already admits ω_2^{η}. Since X_{-2}^{η} and ω_2^{η}

normalize $U_0 = X^{\eta}_{-1}X^{\eta^2}_{-2}X_2$, it follows that L^{η}_2 is represented on U/U_0. As in the proofs of (3A) and (4A) we have then

$$[x_{-2}(\beta)^{\eta},\ x_1(\alpha)] \equiv x_1(-\alpha\beta^{\rho})^{\eta^2} \quad (\mathrm{mod}\ U_0),$$

where ρ is a field automorphism of F_q. Thus $-\alpha\beta^{\rho} = \gamma\alpha\beta$, and so $\gamma = -1$. Finally, to evaluate δ, we set $x = x_1(\mu)$, $y = x_1(\nu)$, $z = x_{-2}(\beta)^{\eta}$ in (4. 8), take into account (4G) (i), and compare coefficients in x_{-1}. This gives.

$$-\delta\beta(\mu+\nu)^2 = -\delta\beta\mu^2 - \delta\beta\nu^2 - \beta\mu\nu,$$

so that $2\delta = 1$ and $\delta = -1$. This completes the proof.

(4H) *The following commutator relations hold in case* (C).

(i) $[x_{-1}(\beta)^{\eta},\ x_1(\alpha)] = x_{-2}(-\alpha\beta - \bar{\alpha}\bar{\beta} - \bar{\bar{\alpha}}\bar{\bar{\beta}})^{\eta^2}$

(ii) $[x_1(\beta)^{\eta^2},\ x_1(\alpha)] = x_{-1}(\bar{\alpha}\bar{\bar{\beta}} + \bar{\bar{\alpha}}\bar{\beta})^{\eta}x_{-2}(-\bar{\alpha}\bar{\bar{\alpha}}\beta - \bar{\bar{\alpha}}\alpha\bar{\beta} - \alpha\bar{\alpha}\bar{\bar{\beta}})^{\eta^2}.$
$x_2(-\alpha\bar{\beta}\bar{\bar{\beta}} - \bar{\alpha}\bar{\bar{\beta}}\beta - \bar{\bar{\alpha}}\beta\bar{\beta})$

(iii) $[x_{-2}(\beta)^{\eta},\ x_1(\alpha)] = x_1(\alpha\beta)^{\eta^2}x_{-1}(\bar{\alpha}\bar{\bar{\alpha}}\beta)^{\eta}x_{-2}(-\alpha\bar{\alpha}\bar{\bar{\alpha}}\beta)^{\eta^2}x_2(\alpha\bar{\alpha}\bar{\bar{\alpha}}\beta^2)$

(iv) $[X^{\eta^2}_{-2},\ X_1] = 1.$

In particular, $P = X_1M$ *has a unique multiplication table.*

Proof. [5] (7C) implies that $[X_1, X^{\eta^2}_{-2}] \leqslant X_2$, so the argument given for (4F) (iv) is also valid for (4H) (iv). (i) follows from (4. 5). Now (4C), (1. 4), (1. 6) imply that modulo X_2

$$\begin{aligned}
&[x_1(1)^{\eta^2},\ x_1(\alpha)] \equiv x_{-1}(\bar{\alpha} + \bar{\bar{\alpha}})^{\eta}x_{-2}(-\bar{\alpha}\bar{\bar{\alpha}} - \bar{\bar{\alpha}}\alpha - \alpha\bar{\alpha})^{\eta^2}\\
(4.\ 12)\qquad &[x_1(\theta)^{\eta^2},\ x_1(\alpha)] \equiv x_{-1}(\bar{\alpha}\bar{\bar{\theta}} + \bar{\bar{\alpha}}\bar{\theta})^{\eta}x_{-2}(-\bar{\alpha}\bar{\bar{\alpha}}\theta - \bar{\bar{\alpha}}\alpha\bar{\theta} - \alpha\bar{\alpha}\bar{\bar{\theta}})^{\eta^2}\\
&[x_1(\theta^2)^{\eta^2},\ x_1(\alpha)] \equiv x_{-1}(\bar{\alpha}\bar{\bar{\theta}}^2 + \bar{\bar{\alpha}}\bar{\theta}^2)^{\eta}x_{-2}(-\bar{\alpha}\bar{\bar{\alpha}}\theta^2 - \bar{\bar{\alpha}}\alpha\bar{\theta}^2 - \alpha\bar{\alpha}\bar{\bar{\theta}}^2)^{\eta^2}.
\end{aligned}$$

An element β in F_{q^3} can be expressed in the form $\beta = b_0 + b_1\theta + b_2\theta^2$, where b_0, b_1, b_2 are elements in F_q. Using (4. 12) and (4. 8) twice, we find that

$$\begin{aligned}
(4.\ 13)\qquad &[x_1(\beta)^{\eta^2},\ x_1(\alpha)] = x_{-1}(\bar{\alpha}\bar{\bar{\beta}} + \bar{\bar{\alpha}}\bar{\beta})^{\eta}x_{-2}(-\bar{\alpha}\bar{\bar{\alpha}}\beta - \bar{\bar{\alpha}}\alpha\bar{\beta} - \alpha\bar{\alpha}\bar{\bar{\beta}})^{\eta^2}.\\
&x_2(f(\alpha, \beta)),
\end{aligned}$$

where f is a function from $F_{q^3}\times F_{q^3}$ into F_q. A similar argument shows that

$$\begin{aligned}
(4.\ 14)\qquad &[x_{-2}(\beta)^{\eta},\ x_1(\alpha)] = x_1(\alpha\beta)^{\eta^2}x_{-1}(\bar{\alpha}\bar{\bar{\alpha}}\beta)^{\eta}x_{-2}(-\alpha\bar{\alpha}\bar{\bar{\alpha}}\beta)^{\eta^2}.\\
&x_2(g(\alpha, \beta)),
\end{aligned}$$

where g is a function from $F_{q^3}\times F_q$ into F_q. Conjugating (4. 13) by $\omega_2\eta^2$ then gives

$$[x_1(-\beta),\ x_1(\alpha)^{\eta^2}] = x_{-1}(\bar{\alpha}\bar{\bar{\beta}} + \bar{\bar{\alpha}}\bar{\beta})^{\eta}x_2(-\bar{\alpha}\bar{\bar{\alpha}}\beta - \bar{\bar{\alpha}}\alpha\bar{\beta} - \alpha\bar{\alpha}\bar{\bar{\beta}}).$$
$$x_{-2}(-f(\alpha,\beta))^{\eta^2}.$$

If we interchange α and β in this and compare the result with (4. 13), we find that

$$f(\alpha,\beta) = -\alpha\bar{\beta}\bar{\bar{\beta}} - \bar{\alpha}\bar{\bar{\beta}}\beta - \bar{\bar{\alpha}}\beta\bar{\beta},$$

which proves (ii). If we conjugate (4. 14) by $h_1(\lambda)h_0(\mu)$, where λ is in F_{q^3} and μ is in F_q, and compare the coefficients in x_2, we find that

$$(4.\ 15) \qquad g(\alpha\lambda^{-2}\mu,\beta\lambda^{q^2+q+1}\mu^{-2}) = \mu^{-1}g(\alpha,\beta).$$

Setting $\lambda = \nu$, $\mu = \nu^2$ in (4. 15), where ν is in F_q, shows that $g(\alpha,\beta) = g(\alpha,1)\beta^2$. To evaluate $g(\alpha,1)$, we set $x = x_{-2}(\mu)^{\eta}$, $y = x_{-2}(\nu)^{\eta}$, $z = x_1(\alpha)$ in (4. 8). Using (4D) and (4E) in comparing the coefficients in x_2, we find that

$$g(\alpha,1)\,(\mu+\nu)^2 = g(\alpha,1)\mu^2 + g(\alpha,1)\nu^2 + 2\alpha\bar{\alpha}\bar{\bar{\alpha}}\mu\nu.$$

Thus $g(\alpha,1) = \alpha\bar{\alpha}\bar{\bar{\alpha}}$ and $g(\alpha,\beta) = \alpha\bar{\alpha}\bar{\bar{\alpha}}\beta^2$, which proves (iii).

5. The results of §§ **3**, **4** and [5] § **6** now imply that $\tilde{G}$ has a unique multiplication table. Now it is not difficult to verify from the presentation of the groups $G_2(q)$ and $D_4^2(q)$ in [2], [8] that these groups satisfy the conditions (*), (**), (***) of § **2**. Indeed, for $G_2(q)$ the required calculations can be found in [11], and the verification for $D_4^2(q)$ can be done along similar lines. In the case of $G_2(q)$, $q_1 = q_2 = q$; in the case of $D_4^2(q)$, $q_1 = q^3$, $q_2 = q$. Since $|\tilde{G}| = |G_2(q)|$ in cases (A) and (B), and $|\tilde{G}| = |D_4^2(q)|$ in case (C), we have the following result.

(5A) *In cases* (A) *and* (B) *the subgroup* $\tilde{G}$ *is isomorphic to* $G_2(q)$. *In case* (C) $\tilde{G}$ *is isomorphic to* $D_4^2(q)$.

(5B) *Suppose* $G > \tilde{G}$. *Then there exists a subgroup* V *of* $\tilde{G}$ *of odd order such that* $\tilde{G} = V\cdot C(i)$, *where* i *is any involution in* $\tilde{G}$. *In particular,*

$$|V| = |\tilde{G} : C(j)|\,|V\cap C(j)|.$$

Proof. By [6], Chapter 9, Theorem 2. 1, there exists a subgroup V of odd order such that $\tilde{G} = VC(j)$. Now $\tilde{G}$ has only one class of involutions, so that $\tilde{G} = VC(i)$ for any involution i in $\tilde{G}$. This is enough to complete the proof. We note that if

$$c = |V \cap C(i)|,$$

then c does not depend on the choice of i. We have $|V| = q^4(q^4 + q^2 + 1)c$ in cases (A) and (B), $|V| = q^8(q^8 + q^4 + 1)c$ in case (C).

(5C) *Suppose $G > \tilde{G}$, and set $Y = HL_1M$, $D = V \cap Y^g$, where $g \in \tilde{G}$. If π is the set of odd primes dividing $q^6 - 1$, and D_π is an S_π-subgroup of D, then $D_\pi \leqslant (H_2L_1)^k$ for some k in $\tilde{G}$.*

Proof. We first note that D is solvable, this being a direct consequence of the structure of Y and the oddness of $|D|$. Thus D_π exists, and we have

$$D_\pi \simeq D_\pi M^g/M^g \leqslant (H_2L_1M)^g/M^g \simeq (H_2L_1)^g,$$

the last group being the central product of $L_1{}^g$ and the cyclic subgroup $H_2{}^g$ of order $q-1$. Let π_1, π_2 be the set of odd primes dividing $q^3 - 1$, $q^3 + 1$ respectively, so that $\pi = \pi_1 \cup \pi_2$. Since $H_2L_1 \leqslant Y$, it follows that Y contains an abelian S_{π_1}-subgroup and a cyclic S_{π_2}-subgroup. If D_π is a π_1-group, then $D_\pi \leqslant (H_2L_1)^{gh}$ for some h in Y^g by a theorem of Wielandt [14]. Since g and h are in $\tilde{G}$, the result follows. If D_π is not a π_1-group, then $D_0 = D_\pi \cap (L_1M)^g$ must be a non-trivial normal S_{π_2}-subgroup of D_π. We have $D_0 \leqslant L_1{}^{gh}$ for some h in Y^g by the theorem of Wielandt. Let E^{gh} be the normalizer of D_0 in $L_1{}^{gh}$; E^{gh} is then a dihedral group of order $2(q_1 + 1)$. Since $(H_2L_1M)^g$ and M^g are normal subgroups of Y^g and $h \in Y^g$, it follows that

$$D_\pi \leqslant (H_2L_1M)^{gh} \cap N(D_0) \leqslant (H_2L_1M)^{gh} \cap N(D_0M^{gh}) = (H_2EM)^{gh}.$$

But H_2EM has an abelian S_π-subgroup, so by a third application of the theorem of Wielandt, $D_\pi \leqslant (H_2L_1)^{ghi}$ for some i in $(H_2EM)^{gh}$. Since g, h, i are in $\tilde{G}$, (5C) follows.

(5D) $\qquad G = \tilde{G}.$

Proof. Suppose otherwise. We consider first cases (A) and (B). Let $g \in \tilde{G}$, $D = V \cap Y^g$, and $d = |D|$. The number of elements in the complex VY^g is

$$(5.1) \qquad \frac{|V|\,|Y^g|}{|V \cap Y^g|} = \frac{q^4(q^4+q^2+1)c(q^2-1)(q-1)q^6}{d} = q^6(q^6-1)(q-1)\frac{q^4c}{d}$$

a number which cannot exceed $|\tilde{G}| = q^6(q^6-1)(q^2-1)$. Let $d = d_\pi d_p$ and

$c = c_\pi c_p$ be the factorizations of d and c into their π- and p-factors, π being as before the set of odd primes dividing $q^6 - 1$. By (5C) d_π divides c_π, so that necessarily $d_p \geqslant q^3 c_p$.

Suppose $c_p \neq 1$, so that $d_p > q^3$. Since M^g is a normal subgroup of Y^g of index q in every S_p-subgroup of Y^g, it follows that $|V \cap M^g| > q^2$. But $(X_{-2}^{\eta} X_{-2}^{\eta^2} X_2)^g$ has index q^2 in M^g, and so $V \cap (X_{-2}^{\eta} X_{-2}^{\eta^2} X_2)^g \neq 1$. In particular, by taking $g = 1$ and $g = \omega_2 \eta^2$, we find that

$$V \cap X_{-2}^{\eta} X_{-2}^{\eta^2} X_2 \neq 1, \quad V \cap X_2^{\eta} X_{-2}^{\eta^2} X_2 \neq 1,$$

and since the subgroup $X_{-2}^{\eta^2} X_2$ admits $\langle X_2, X_{-2} \rangle^{\eta} = L_2^{\eta}$, it follows by a theorem of Dickson, [6], Chapter 2, Theorem 8. 4, and the oddness of $|V|$ that

$$V \cap X_{-2}^{\eta^2} X_2 \neq 1. \tag{5. 2}$$

By taking $g = \omega_2 \eta$ and $g = 1$, we find that

$$V \cap X_2^{\eta^2} X_{-2}^{\eta} X_2 \neq 1, \quad V \cap X_{-2}^{\eta^2} X_{-2}^{\eta} X_2 \neq 1,$$

and since the subgroup $X_{-2}^{\eta} X_2$ admits $\langle X_2, X_{-2} \rangle^{\eta^2} = L_2^{\eta^2}$, it follows as before that

$$V \cap X_{-2}^{\eta} X_2 \neq 1 \tag{5. 3}$$

(5. 2), (5. 3), and (4D) then imply that $V \cap X_2 \neq 1$. The entire argument repeated with Y replaced by Y^{ω_2} yields $V \cap X_{-2} \neq 1$. This is a contradiction by the theorem of Dickson and the oddness of $|V|$, and thus $c_p = 1$.

An S_p-subgroup of V then has order q^4, and no non-trivial p-element in V centralizes an involution of $\tilde{G}$. Thus $P = X_1 M$ contains a subgroup S of order q^4 such that no non-trivial element in S centralizes an involution in $\tilde{G}$. If $|S \cap M| > q^3$, then $S \cap (X_{-1} X_{-2})^{\eta} \neq 1$ since $(X_{-1} X_{-2})^{\eta}$ has index q^3 in M, and this is impossible. Thus $|S \cap M| = q^3$. Suppose case (A) holds. Using (4A), (1. 1), the existence of elements in $S - M$, and the relation $S \cap M \neq X_{-1}^{\eta} X_{-2}^{\eta^2} X_2$, we can find elements s, t in $S \cap (X_{-2}^{\eta^2} X_2 - X_2), S \cap (X_{-1}^{\eta} X_{-2}^{\eta^2} X_2 - X_{-2}^{\eta^2} X_2)$ respectively. Then (4D), (4F) (iv), and the existence of s imply that no element of S, when expressed as a product of elements from each of the root subgroups of P, can involve a factor $x_{-2}^{\eta}(\alpha)$ with $\alpha \neq 0$. But then (4E) and the existence of t imply that $S \cap M \leqslant X_{-1}^{\eta} X_{-2}^{\eta^2} X_2$, which is impossible. Suppose case (B) holds. Using (4B), (4. 9), the existence of elements in $S - M$, and the relation $S \cap M \neq X_1^{\eta^2} X_{-1}^{\eta} X_2$, we can find an element s in $S \cap (X_{-2}^{\eta^2} X_1^{\eta^2} X_{-1}^{\eta} X_2 - X_1^{\eta^2} X_{-1}^{\eta} X_2)$. (4D), (4E) then imply thet $S \cap M$

$\leqslant X_{-2}^{\eta^2}X_1^{\eta^2}X_{-1}^{\eta}X_2$, so that $S\cap(X_1X_{-2})^{\eta^2}\neq 1$, which is impossible. Thus (5D) follows in cases (A) and (B).

Consider now the case (C). Let $g\in\tilde{G}$, $D=V\cap Y^g$, and $d=|D|$. The number of elements in the complex VY^g is

$$\begin{aligned}\frac{|V|\,|Y^g|}{|V\cap Y^g|}&=\frac{q^8(q^8+q^4+1)c(q^6-1)(q-1)q^{12}}{d}\\ &=q^{12}(q^8+q^4+1)(q^6-1)(q-1)\frac{q^8c}{d}\end{aligned}\tag{5. 4}$$

a number which cannot exceed $|\tilde{G}|=q^{12}(q^8+q^4+1)(q^6-1)(q^2-1)$. Again, if π is the set of odd primes dividing q^6-1 and $d=d_\pi d_p$, $c=c_\pi c_p$, then $d_p\geqslant q^7c_p$ by (5C). Suppose first that $c_p\neq 1$, so that $d_p>q^7$. Since M^g is a normal subgroup of Y^g of index q^3 in every S_p-subgroup of Y^g, it follows that $|V\cap M^g|>q^4$. If $V\cap X_2{}^g=1$, then $V\cap M^g$ is necessarily abelian by (4D), (4E). But (4D), (4E) also show that $\mathscr{V}^g=M^g/X_2{}^g$ is a symplectic space of dimension 8 over F_q, the inner product being the commutator. Since $V\cap X_2{}^g=1$, the image of $V\cap M^g$ in $\mathscr{V}^g$ is a subgroup of order greater than q^4, such that any two vectors in $(V\cap M^g)X_2{}^g/X_2{}^g$ are orthogonal. This is impossible, and thus $V\cap X_2{}^g\neq 1$. Taking $g=1$ and $g=\omega_2$, we find that $V\cap X_2\neq 1$, $V\cap X_{-2}\neq 1$, which is impossible. Hence $c_p=1$, and P then contains a subgroup S of order q^8 such that no non-trivial element in S centralizes an involution in $\tilde{G}$. If $|S\cap M|>q^5$, then $S\cap(X_{-1}X_{-2})^\eta\neq 1$ since $(X_{-1}X_{-2})^\eta$ has index q^5 in M, which is impossible. Thus $|S\cap M|=q^5$. Since $S\cap X_2=1$, it follows that $S\cap M$ is abelian, but as before, this leads to a contradiction. Thus $G=\tilde{G}$ in all cases.

6. As a consequence of the work in the preceding sections, it now follows that the theorem stated in the introduction holds if

(***) $|G|$ is divisible by $(q_1q_2)^3$.

As remarked in § **2**, (***) can only fail to hold in case $q_1=q_2\leqslant 11$. Thus we shall assume that $q_1=q_2=q$ throughout this section, and indicate how (***) can be seen to hold even if $q\leqslant 11$. We may moreover assume that $q\geqslant 5$ since the case $q=3$ has been done by Janko [7].

Let $\{\alpha,\beta\}=\{1,2\}$, and set $K_\beta=O(C(X_\beta))$. Since K_β/X_β is inverted by j and so is abelian, K_β has a unique S_p-subgroup M_β. If q^6 does not divide $|G|$, then one and only one of the following cases occurs by [5] (4E).

(I) $M_\beta = X_\beta$

(II) $|M_\beta/X_\beta| = q^2$

(6A) *Suppose q^6 does not divide $|G|$. If* (I) *holds for the index β, then X_1X_2 is an S_p-subgroup of $C(u)$ for every $u \neq 1$ in X_β.*

Proof. Let $N = O(C(u))$, so that by [5] (3C), we have $C(u) = L_\alpha N$, $L_\alpha \cap N = 1$, and $X_\beta \leqslant N$. Let S be an S_p-subgroup of $C(u)$ containing X_1X_2. $S \cap N$ is then an S_p-subgroup of N containing X_β. If $S \cap N > X_\beta$, then there exists a subgroup R such that $X_\beta \lhd R \leqslant S \cap N$. Since $\langle X_\alpha, R\rangle \leqslant S$, it follows that $\langle X_\alpha, R\rangle$ is a p-group of order exceeding q^2 which normalizes X_β. But $N(X_\beta) = HL_\alpha K_\beta$ by [5] (3B), so that X_1X_2 is an S_p-subgroup of $N(X_\beta)$. This is a contradiction and so $S \cap N = X_\beta$, which then proves (6A).

(6B) *Suppose q^6 does not divide $|G|$. If* (I) *holds for both indices α and β, then X_1X_2 is an S_p-subgroup of G.*

Proof. Suppose not, and let S be a p-subgroup of G with $X_1X_2 \lhd S$. Under the action of H, $(X_1X_2)^\# = X_1X_2 - \{1\}$ is partitioned into four orbits:

$$X_1^\#,\ X_2^\#,\ O_1,\ O_2.$$

Let $z \neq 1$ be chosen in $Z(S) \cap X_1X_2$; by (6A) we may assume that $z \in O_1$. Since X_1X_2 is an S_p-subgroup of $N(X_1)$ and $N(X_2)$, no element in $S - X_1X_2$ normalizes X_1 or X_2. By (6A) no element in $X_1^\# \cup X_2^\#$ is fused in G to an element of O_1. Thus it follows that some element in $X_1^\#$ is fused to an element in $X_2^\#$. In particular, we have by [5] (3C) that the S_2-subgroups of L_1 and L_2 are conjugate in G. But then these S_2-subgroups would be conjugate in $C(j)$, which is a contradiction.

(6C) *Suppose q^6 does not divide $|G|$. If* (II) *holds for the index β, then $R_\beta = X_\alpha M_\beta$ is an S_p-subgroup of G and $Z(R_\beta) = X_\beta$. Moreover,* (I) *holds for the index α.*

Proof. The 4-subgroup D normalizes R_β, and ω_α interchanges $M_\beta \cap C(j_1)$ and $M_\beta \cap C(j_2)$. Thus by the Brauer-Wielandt Theorem, we have that

$$M_\beta \cap C(j) = X_\beta,\quad |M_\beta \cap C(j_1)| = |M_\beta \cap C(j_2)| = q.$$

Moreover, [5] (4B) implies that

$$M_\beta \cap C(j_1) \leqslant (X_aX_b)^\gamma,\quad M_\beta \cap C(j_2) \leqslant (X_cX_d)^{\gamma^2},$$

where $a, c \in \{1, -1\}$, and $b, d \in \{2, -2\}$. Since $M_\beta \cap C(j_1)$ and $M_\beta \cap C(j_2)$ admit H, and $q > 3$, it follows by [5] (4C) that

$$M_\beta \cap C(j_1) = X_a^\eta \text{ or } X_o^\eta, \quad M_\beta \cap C(j_2) = X_c^{\eta^2} \text{ or } X_d^{\eta^2}.$$

Taking into account that ω_α interchanges $M_\beta \cap C(j_1)$ and $M_\beta \cap C(j_2)$, we see that one of the following cases must occur:

(1) $M_\beta = X_\beta X_{-\alpha}^\eta X_\alpha^{\eta^2}$

(2) $M_\beta = X_\beta X_\alpha^\eta X_{-\alpha}^{\eta^2}$

(3) $M_\beta = X_\beta X_\beta^\eta X_\beta^{\eta^2}$

(4) $M_\beta = X_\beta X_{-\beta}^\eta X_{-\beta}^{\eta^2}$

Suppose (1) holds. For any ω in $N(H)$, we note that $R_\beta \cap R_\beta^\omega$ admits D. Applying the Brauer-Wielandt Theorem with $\omega = \omega_\alpha \omega_\beta \eta$, we find that

$$R_\beta \cap R_\beta^\omega = X_{-\alpha}^\eta X_\alpha^{\eta^2} \text{ for } \omega = \omega_\alpha \omega_\beta \eta. \tag{6. 1}$$

Since M_β / X_β is abelian, (6. 1) implies that

$$[X_{-\alpha}^\eta, X_\alpha^{\eta^2}] \leqslant X_\beta \cap X_{-\alpha}^\eta X_\alpha^{\eta^2} = 1, \tag{6. 2}$$

so that M_β is abelian. Conjugating (6. 2) by $\omega_\beta \eta^2$ gives $[X_{-\alpha}^\eta, X_\alpha] = 1$, which implies that $X_{-\alpha}^\eta \leqslant Z(R_\beta)$. In particular, $R_\beta^{\omega_\alpha \eta} = X_{-\alpha}^\eta X_\beta^\eta X_\alpha X_{-\alpha}^{\eta^2}$ is contained as an S_p-subgroup in $C(X_\alpha) = L_\beta K_\alpha$, and so $R_\beta^{\omega_\alpha \eta} \geqslant M_\alpha$. Since $X_\beta^\eta \leqslant Z(R_\beta^{\omega_\alpha \eta})$, it follows that X_β^η induces trivial automorphisms on M_α / X_α, so that $X_\beta^\eta \leqslant M_\alpha$. Conjugating this last relation by ω_β yields $X_{-\beta}^{\eta^2} \leqslant M_\alpha$, so in particular, $X_{-\beta}^{\eta^2} \leqslant R_\beta^{\omega_\alpha \eta}$, and $X_{-\beta}^{\eta^2} \leqslant R_\beta$, which is a contradiction. Thus case (1) cannot occur, and a similar argument excludes case (2) as well.

Suppose (3) holds. X_β, X_β^η, $X_\beta^{\eta^2}$ are permuted transitively by η, so that η normalizes M_β. Since $X_\beta \leqslant Z(M_\beta)$, it follows that M_β is abelian. Now M_β can be considered as a representation space for L_α over F_p. Since $[L_\alpha, X_\beta] = 1$ and j inverts $X_\beta^\eta X_\beta^{\eta^2}$, the representations of L_α on X_β and M_β / X_β are in different p-blocks. Thus M_β is a completely reducible L_α-module. In particular, $T = C(X_\alpha) \cap M_\beta$ has order q^2. Now T admits H, and $T \cap C(j) = X_\beta$. Applying the Brauer-Wielandt Theorem and [5] (4B), (4C), we can deduce that

$$T = X_\beta X_\beta^{\eta^i}, \quad i = 1 \text{ or } 2.$$

Thus $X_\beta^{\eta^i} \leqslant C(X_\alpha) = L_\beta K_\alpha$. If $X_\beta^{\eta^i} \leqslant M_\alpha$, then case (1) or (2) would hold for M_α, which we have just seen to be impossible. Thus $X_\beta^{\eta^i} \nleqslant K_\alpha$, and since $X_\beta^{\eta^i}$ and K_α both admit H, this implies that $X_\beta^{\eta^i} \cap K_\alpha = 1$. But now $X_\beta^{\eta^i}$ centralizes X_β, and $L_\beta K_\alpha / K_\alpha$ is isomorphic to $SL(2, q)$. Thus $X_\beta^{\eta^i} K_\alpha = X_\beta K_\alpha$, which is impossible since $X_\beta K_\alpha \cap C(j) = X_\beta X_\alpha$, while $X_\beta^{\eta^i} K_\alpha \cap C(j) = X_\alpha$. Case (3) then does not occur.

Suppose finally that (4) holds. If $[X_{-\beta}^{\eta}, X_{-\beta}^{\eta^2}] = 1$, then conjugating this relation by $\omega_\beta \eta$ gives $[X_\beta, X_\beta^{\eta^2}] = 1$. Thus $L_\beta^{\eta^2} = \langle X_\beta, X_{-\beta} \rangle^{\eta^2} \leqslant C(X_\beta)$, which is impossible since j_2 inverts X_β. Hence $[X_{-\beta}^{\eta}, X_{-\beta}^{\eta^2}] \neq 1$, and since $X_{-\beta}^{\eta}$ and $X_{-\beta}^{\eta^2}$ admit H, we find that $[X_{-\beta}^{\eta}, X_{-\beta}^{\eta^2}] = X_\beta$. A similar type of argument shows that $Z(M_\beta) = X_\beta$. Thus $Z(R_\beta) = X_\beta$, so in particular, $N(R_\beta) \leqslant N(X_\beta)$, which is enough to show that R_β is an S_p-subgroup of G. If (II) holds for the index α, then X_α and X_β would necessarily be conjugate in G, which we showed to be impossible in the proof of (6B). This completes the proof.

(6D) *If* $|G|$ *is not divisible by* q^6 *then* $X_1 X_2$ *is an* S_p*-subgroup of* G.

Proof. $\langle j \rangle$ is an S_2-subgroup of $C(X_1 X_2, j)$, so by [5] (2B) $\langle j \rangle$ is also an S_2-subgroup of $C(X_1 X_2)$. In particular, $C(X_1 X_2)$ has a normal 2-complement T, and the Frattini argument gives

$$N(X_1 X_2) = (N(X_1 X_2) \cap C(j)) \cdot C(X_1 X_2).$$

Since $N(X_1 X_2) \cap C(j) = X_1 X_2 H$, it follows that $N(X_1 X_2) = TH$. If $X_1 X_2$ is not an S_p-subgroup of G, then $X_1 X_2$ is not an S_p-subgroup of T. Since $T \leqslant C(X_1 X_2)$, this is impossible by (6A) and (6C).

(6E) *If* $q = 5$ *or* 7, *then* q^6 *divides* $|G|$.

Proof. We use the notation of [5], § 5. Since $q = 5$ or 7, it follows that $q + \varepsilon = 6$, so that $|V| = 9$. If ζ centralizes V_α, where $\alpha = 1$ or 2, then $X = C(V_\alpha)/V_\alpha$ satisfies the conditions of [5] (3E). In particular, q^3 divides $|G|$, and so q^6 divides $|G|$ by (6D). We may assume then that ζ does not centralize V_1 or V_2. ζ must then fix exactly 3 elements in V, none of which belong to $V_1^\# \cup V_2^\#$. The remaining 6 elements of V thus lie in orbits of length 3 under the action of ζ, and a generator v_1 of V_1 is necessarily fused to a generator v_2 of V_2. Since $\langle a_1, b_1, n \rangle$ and $\langle a_2, b_2, n \rangle$ are S_2-subgroups of $C(V_2)$ and $C(V_1)$ respectively, these 2-groups are then conjugate in G. But then they would be conjugate in $C(j)$, which is impossible. This completes the proof of (6E).

(6F) *If* $q = 9$ *or* 11, *then* q^6 *divides* $|G|$.

Proof. We shall only outline the proof, since the calculations involved are lengthy. Suppose (6F) fails to hold for $q = 9$. If $\mathscr{D}$ is the set of all elements of $C(j)$ which are roots of j, 3-singular elements, or 5-elements in L_1 or L_2, then it is not difficult to show using (6D) and [5] (3E) that $\mathscr{D}$ is a union of classes of $C(j)$ which are special in the sense of [9]. Moreover, $C(j) \geqslant C^*(g)$ for every g in $\mathscr{D}$, where $C^*(g)$ is the extended centralizer of g in G. $C(j)$ has an irreducible character θ of degree 81 such that $1 - \theta$ vanishes on the elements of $C(j) - L_1L_2$ not in $\mathscr{D}$. $C(j)$ also has 8 irreducible characters Ξ_i, $1 \leqslant i \leqslant 8$, of degree 80 such that $1 - \theta + \Xi_i$ vanishes on the elements of $C(j)$ not in $\mathscr{D}$. Decomposing the induced characters $(1 - \theta + \Xi_i)^*$ and applying the Suzuki order formula [9], we find

$$|G| = 2^{14} \cdot 3^8 \cdot 5^3 \cdot 41^2 \frac{x(x+\delta)}{(x - \chi(j))^2}$$

where $\delta = \pm 1$, χ is an irreducible character of G, $x = \chi(1)$, and x, $x + \delta$ are divisors of $|G|$. In particular, $x - \chi(j)$ divides $2^7 \cdot 3^4 \cdot 5 \cdot 41$. Since $|C(j)| = (720)^2$, it follows that only a limited number of possibilities arise for $|G|$, all of which turn out to be impossible.

If $q = 11$, then $q \equiv 3 \pmod 8$. Now whenever $q \equiv \pm 3 \pmod 8$, an S_2-subgroup S of G has order 64. The fusion of 2-elements in G then is that designated as case I in [1]. By methods similar to those in [1], and indeed, using [1] (4. 1), (4. 2), we can write down all possible decomposition numbers for the principal 2-block of G. Up to this point, only the structure of S need be assumed known. If in addition we use the fact that $C(j)$ is known, we can obtain the order formula

$$|G| = q^4(q^2 - 1)^3(q^2 + 1)^2 \frac{x(x+1)}{(x + q^2)^2}$$

where $|x|$ is the degree of an irreducible character of G. Moreover, $x + q^2$ divides $q^2(q^2 - 1)(q^2 + 1)$, $x \equiv 27q^2 \pm 20q - 16 \pmod{64}$, and $(x + q^2)^2 - 4x(q^2+1)^2$ is a square. In particular, for $q = 11$, the limited number of possibilities which arise for $|G|$ turn out to be impossible except for the one case where q^6 divides $|G|$.

References

[1] R. Brauer and P. Fong, A characterization of the Mathieu group M_{12}, Transactions of the Amer. Math. Soc. **122** (1966), 18–47.

[2] C. Chevalley, Sur certains groupes simples, Tohoku Math. Journal (2), **7** (1955), 14–66.

[3] L.E. Dickson, Linear groups in an arbitrary field, Transactions of the Amer. Math. Soc. **2** (1901), 363–394.

[4] —————, A new system of simple groups, Math. Annalen, **60** (1905), 137–150.

[5] P. Fong and W.J. Wong, A characterization of the finite simple groups $PSp(4,q)$, $G_2(q)$, $D_4^2(q)$, I, Nagoya Math. Journal **36** (1969), 143-184.

[6] D. Gorenstein, *Finite groups*. Harper and Row, New York, 1968.

[7] Z. Janko, A characterization of the simple group $G_2(3)$, Journal of Algebra **12** (1969), 360-371.

[8] R. Steinberg, Variations on a theme of Chevalley, Pac. Jour. Math. **9** (1959), 875–891.

[9] M. Suzuki, Applications of group characters, Proc. Symposium Pure Math., Amer. Math. Soc. **1** (1959) 88–99.

[10] G. Thomas, A characterization of the groups $G_2(2^n)$, Journal of Algebra **13** (1969), 87-118.

[11] J.G. Thompson, Non-solvable finite groups all of whose local subgroups are solvable, to appear.

[12] J. Tits, Théorème de Bruhat et sous-groupes paraboliques, C.R. Acad. Sci. Paris, **254** (1962), 2910–2912.

[13] ————, Sur la trialité et certains groupes qui s'en déduisent, Institut des Hautes Études Scientifiques, **2** (1959).

[14] H. Wielandt, Zum Satz von Sylow, Math. Zeitschrift, **60** (1954), 407–409.

[15] W.J. Wong, A characterization of the finite projective symplectic groups $PSp_4(q)$, Transactions of the Amer. Math. Soc. **139** (1969), 1-135.

University of Illinois
Chicago, Illinois