

A CHARACTERIZATION OF THE FINITE SIMPLE GROUPS $\text{PSp}(4, q)$, $G_2(q)$, $D_4^2(q)$, I

PAUL FONG and W.J. WONG¹⁾

Suppose that G is the projective symplectic group $\text{PSp}(4, q)$, the Dickson group $G_2(q)$, or the Steinberg "triviality-twisted" group $D_4^2(q)$, where q is an odd prime power. Then G is a finite simple group, and G contains an involution j such that the centralizer $C(j)$ in G has a subgroup of index 2 which contains j and which is the central product of two groups isomorphic with $SL(2, q_1)$ and $SL(2, q_2)$ for suitable q_1, q_2 . We wish to show that conversely the only finite simple groups containing an involution with this property are the groups $\text{PSp}(4, q)$, $G_2(q)$, $D_4^2(q)$. In this first paper we shall prove the following result.

THEOREM. *Let G be a finite group with subgroups L_1, L_2 such that $L_1 \cong SL(2, q_1)$, $L_2 \cong SL(2, q_2)$, $[L_1, L_2] = 1$, $L_1 \cap L_2 = \langle j \rangle$, where j is an involution, and $|C(j) : L_1 L_2| = 2$. Suppose that $G \neq C(j)O(G)$. Then one of the following holds:*

- (a) $q_1 = q_2$, and L_1, L_2 are not normal in $C(j)$.
- (b) $q_1 = q_2$, and L_1, L_2 are both normal in $C(j)$.
- (c) One of the numbers q_1, q_2 is the cube of the other.

Furthermore, in each case, $C(j)$ is uniquely determined to within isomorphism.

Here $O(G)$ denotes the largest normal subgroup of odd order in G , and the condition $G \neq C(j)O(G)$ is obviously satisfied if G is simple. The groups $\text{PSp}(4, q)$, $G_2(q)$, $D_4^2(q)$ satisfy the hypotheses of the theorem, and belong to the cases (a), (b), (c) respectively. By the uniqueness statement of the theorem, $C(j)$ is isomorphic with the centralizer of an involution in $\text{PSp}(4, q)$, $G_2(q)$ or $D_4^2(q)$, where $q = \min\{q_1, q_2\}$. In case (a) it follows that G must be isomorphic with $\text{PSp}(4, q)$ [18]. In the sequel to this paper it will be shown that, in cases (b), (c), G must be isomorphic with $G_2(q)$, $D_4^2(q)$ respectively [12].

Received January 14, 1969.

¹⁾ Research partially supported by National Science Foundation grants GP-6539 and GP-8366.

The proof of the theorem is begun by a study of the possible fusions of involutions of $C(j)$ in G , which shows that either (a) holds and the structure of $C(j)$ is uniquely determined, or else L_1 and L_2 are both normal in $C(j)$ and the structure of $C(j)$ is again uniquely determined. In the latter case we use the Brauer-Wielandt theorem, a knowledge of the irreducible representations of $SL(2, q)$ over finite fields, and results and methods of Brauer concerning groups with prescribed S_2 -groups, first to show that q_1 and q_2 are powers of the same prime p , and then to show that (b) or (c) holds provided $(q_1q_2)^3$ divides the order of $C(X_b)$, where X_b is a S_p -group of L_b , $b = 1$ or 2 , $q_b = \min \{q_1, q_2\}$. By using the theory of blocks of group characters we show that if (b) does not hold then $(q_1q_2)^3$ divides the order of G , and hence $(q_1q_2)^3$ divides the order of $C(X_\beta)$, where X_β is a S_p -group of L_β , $\beta = 1$ or 2 . Finally, by forming a (B, N) -pair, we construct a subgroup \hat{G} of G of known order and show by means of a result of Brauer that \hat{G} induces a group of collineations of a Desarguesian projective plane of order q_β , containing the little projective group $PSL(3, q_\beta)$. This gives an inequality between orders which implies that $\beta = b$, completing the proof of the theorem.

§1. In this section we fix notation for $L = SL(2, q)$, where $q = p^\alpha$ for an odd prime p , and set down some facts about its automorphisms and representations. Let

$$q - \varepsilon = 2^\alpha u, \quad q + \varepsilon = 2v,$$

where $\varepsilon = \pm 1$, $\alpha \geq 2$, and u, v are odd. L contains elements ρ, σ of order $q - \varepsilon, q + \varepsilon$ respectively. Indeed, we may take

$$\rho = \begin{pmatrix} \gamma & \\ & \gamma^{-1} \end{pmatrix}, \quad \sigma = \begin{pmatrix} \lambda & \mu \\ -\delta\mu & \lambda \end{pmatrix} \text{ if } \varepsilon = 1,$$

and

$$\rho = \begin{pmatrix} \lambda & \mu \\ -\mu & \lambda \end{pmatrix}, \quad \sigma = \begin{pmatrix} \gamma & \\ & \gamma^{-1} \end{pmatrix} \text{ if } \varepsilon = -1.$$

Here γ is a primitive root of F_q , δ is a non-square in F_q , and $\lambda + \mu\sqrt{-\delta}$ or $\lambda + \mu\sqrt{-1}$ is a generator for the group of elements in F_{q^2} of F_q -norm 1 respectively in the cases $\varepsilon = 1, \varepsilon = -1$. Set

$$a = \rho^u, \quad \tau = a^{2^{\alpha-2}},$$

so that a and τ have orders 2^α and 4 respectively. The involution

$$j = \tau^2 = \begin{pmatrix} -1 & \\ & -1 \end{pmatrix}$$

generates the center of L . We have

$$(1.1) \quad C_L(\rho^i) = \langle \rho \rangle \quad \text{if } \rho^i \notin \langle j \rangle.$$

For $g \in L$ denote by $C_L^*(g)$ the projective centralizer of g in L , i.e.

$$C_L^*(g) = \{h \in L: g^h = g \text{ or } gj\}.$$

$C_L^*(g)$ is a subgroup of L with $C_L(g)$ as a subgroup of index 1 or 2. Then

$$(1.2) \quad C_L^*(\tau) = \langle \rho, b \rangle,$$

where b is an element satisfying the relations

$$b^2 = j, \quad \rho^b = \rho^{-1}.$$

Indeed, we may take

$$(1.3) \quad b = \begin{cases} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} & \text{if } \varepsilon = 1 \\ \begin{pmatrix} \lambda & \mu \\ \mu & -\lambda \end{pmatrix} & \text{if } \varepsilon = -1, \end{cases}$$

where in the case $\varepsilon = -1$, $\lambda^2 + \mu^2 = -1$. We have

$$(1.4) \quad N_L(\langle \rho^i \rangle) = \langle \rho, b \rangle \quad \text{if } \rho^i \notin \langle j \rangle.$$

The subgroup $Q = \langle a, b \rangle$ is a generalized quaternion group of order $2^{\alpha+1}$, and is an S_2 -subgroup of L . We also have

$$(1.5) \quad C_L(\sigma^i) = \langle \sigma \rangle \quad \text{if } \sigma^i \notin \langle j \rangle$$

and

$$\sigma^\tau = \sigma^{-1}, \quad \sigma^{\frac{1}{2}(q+\varepsilon)} = j,$$

so that

$$(1.6) \quad N_L(\langle \sigma^i \rangle) = \langle \sigma, \tau \rangle \quad \text{if } \sigma^i \notin \langle j \rangle.$$

The automorphism group $\text{Aut}(L)$ is isomorphic to the projective semili-

near group $PFL(2, q)$ by [11]. Thus the outer automorphism group $\text{Out}(L)$ is given by

$$\text{Out}(L) \simeq PFL(2, q)/PSL(2, q),$$

which is the direct product of the group $PGL(2, q)/PSL(2, q)$ of order 2 and a cyclic group of order n , where $q = p^n$ and p is the characteristic of the Galois field F_q . The latter group arises from the automorphisms of L induced by field automorphisms of F_q . Referring to elements of $\text{Out}(L)$ as automorphism classes, we have

(1A) If q is not a square, then L has exactly one automorphism class T_1 of order 2. If q is a square, then L has exactly three automorphism classes T_1, T_2, T_3 of order 2.

We denote the class of inner automorphisms of L by T_0 ; the identity automorphism θ_0 is a representative of this class. The class T_1 of outer automorphisms corresponding to elements of $PGL(2, q)$ not in $PSL(2, q)$ may be represented by the automorphism θ_1 of order 2 defined by

$$(1.7) \quad \theta_1: g \longrightarrow k^{-1}gk,$$

where

$$k = \begin{cases} \begin{pmatrix} & 1 \\ -\delta & \end{pmatrix} & \text{if } \varepsilon = 1, \\ \begin{pmatrix} -1 & \\ & 1 \end{pmatrix} & \text{if } \varepsilon = -1, \end{cases}$$

and δ is a non-square in F_q . If we choose $\delta = \gamma^u$, then in the case $\varepsilon = 1$

$$(1.8) \quad \theta_1: \rho \rightarrow \rho^{-1}, \quad a \rightarrow a^{-1}, \quad b \rightarrow ba.$$

In the case $\varepsilon = -1$, we find that $\theta_1: \rho \rightarrow \rho^{-1}, b \rightarrow b\rho^i$ for some integer i . Then $\theta_1: b\rho^m \rightarrow (b\rho^m)\rho^{i-2m}$, so that by replacing b by $b\rho^m$ for suitable m , we may assume that either $\theta_1: b \rightarrow ba$ or $\theta_1: b \rightarrow b$. The latter is impossible, since the element μ of (1.3) would be 0 so that $\lambda^2 = -1$, which is impossible. Hence we may assume that (1.8) holds in the case $\varepsilon = -1$ as well.

For any $\theta \in \text{Aut}(L)$, define

$$C_L(\theta) = \{g \in L: g^\theta = g\}, \\ C_L^*(\theta) = \{g \in L: g^\theta = g \text{ or } gj\}.$$

$C_L^*(\theta)$ is a subgroup of L containing $C_L(\theta)$ as a subgroup of index 1 or 2. We have

$$(1.9) \quad C_L(\theta_1) = \langle \sigma \rangle, \quad C_L^*(\theta_1) = \langle \sigma, \tau \rangle.$$

If q is a square, say $q = r^2$, then $\varepsilon = 1$. For $\beta \in F_q$ we write $\bar{\beta} = \beta^r$, so that $\beta \rightarrow \bar{\beta}$ is the automorphism of F_q of order 2. If $g = (\beta_{ij}) \in L$, let $\bar{g} = (\bar{\beta}_{ij})$. Then

$$(1.10) \quad \theta_2: g \rightarrow \bar{g}$$

defines an automorphism of L of order 2 belonging to an automorphism class T_2 distinct from T_0 and T_1 . We have

$$(1.11) \quad \theta_2: a \rightarrow a^r, \quad b \rightarrow b,$$

where we note that $a^r = ja$ or ja^{-1} according as to whether $r \equiv 1 \pmod{4}$ or $r \equiv -1 \pmod{4}$. Also

$$(1.12) \quad C_L(\theta_2) \simeq SL(2, r), \quad C_L^*(\theta_2) = \langle C_L(\theta_2), g \rangle,$$

where g is an element whose square may be taken to be j .

Finally we represent the class T_3 by the automorphism θ_3 of L which is θ_2 followed by θ_1 . $(\theta_3)^2$ is then the inner automorphism

$$(1.13) \quad (\theta_3)^2: g \rightarrow a^{\frac{1}{2}(r-1)} g a^{-\frac{1}{2}(r-1)},$$

and

$$(1.14) \quad \theta_3: a \rightarrow a^{-r}, \quad b \rightarrow ba.$$

(1B) All automorphisms of order 2 in T_1 are conjugate in $\text{Aut}(L)$.

Proof. This is the well-known fact that all involutions in $PGL(2, q)$, but not in $PSL(2, q)$, are conjugate.

(1C) Let q be a square. Then all automorphisms of order 2 in T_2 are conjugate in $\text{Aut}(L)$.

Proof. For $z \in L$ denote by θ_z the automorphism of L given by

$$\theta_z: g \rightarrow z^{-1}(g^{\theta_2})z.$$

Let $\Omega = \{z \in L: (\theta_z)^2 = 1\}$. If $y \in GL(2, q)$ induces the automorphism η on L , then

$$\eta^{-1}\theta_z\eta = \theta_w,$$

where $w = (\det y)^{\frac{1}{2}(r-1)} \bar{y}^{-1}zy \in L$. Thus

$$z^y = (\det y)^{\frac{1}{2}(r-1)} \bar{y}^{-1}zy$$

determines an action of $GL(2, q)$ on Ω , and it is sufficient to show this action is transitive. Now $\Omega = \Omega_1 \cup \Omega_2$, where $\Omega_1 = \{z \in L : \bar{z}z = 1\}$, $\Omega_2 = \{z \in L : \bar{z}z = j\}$.

If $y \in GL(2, q)$ and $\det y$ is a non-square, then $\bar{z}^y z^y = (\det y)^{\frac{1}{2}(q-1)} \bar{z}z = -\bar{z}z = j\bar{z}z$, so that y interchanges Ω_1 and Ω_2 . Ω_1 is invariant under the subgroup L , and thus it suffices to show L acts transitively on Ω_1 .

The stabilizer in L of the element 1 in Ω_1 is $\{y \in L : \bar{y} = y\}$, a group isomorphic to $SL(2, r)$. Since $|L| = q(q^2-1) = r^2(q^2-1)$ and $|SL(2, r)| = r(r^2-1) = r(q-1)$, the orbit of 1 under L contains $r(q+1)$ elements. Now $z \in \Omega_1$ if and only if

$$z = \begin{pmatrix} \lambda & \mu \\ \nu & \bar{\lambda} \end{pmatrix}, \quad \lambda\bar{\lambda} - \mu\nu = 1, \quad \bar{\mu} = -\mu, \quad \bar{\nu} = -\nu.$$

Since $\bar{\nu} = -\nu$ if and only if $\nu\gamma^{\frac{1}{2}(r+1)} \in F_r$, there are r possibilities for ν . Similarly there are r possibilities for μ . For $r-1$ choices of μ, ν , we have $\mu\nu = -1, \lambda = 0$. In the remaining $r^2 - r + 1$ cases, $\lambda\bar{\lambda} = 1 + \mu\nu \in F_r$, and there are $r+1$ choices for λ . Hence

$$|\Omega_1| = r - 1 + (r^2 - r + 1)(r + 1) = r^3 + r = r(q + 1).$$

Hence L acts transitively on Ω_1 as asserted.

(1D) There are no automorphisms of order 2 in T_3 .

Proof: For $z \in L$, denote by φ_z the automorphism of L given by

$$\varphi_z: g \rightarrow z^{-1}(g^\theta)z.$$

Then φ_z^2 is the inner automorphism of L corresponding to the element $a^{-\frac{1}{2}(r-1)}(z^\theta)z$. If $\varphi_z^2 = 1$, then $z^\theta = \pm a^{\frac{1}{2}(r-1)}z^{-1}$. If $z = \begin{pmatrix} \lambda & \mu \\ \nu & \pi \end{pmatrix}$, this is equivalent to the equations

$$\bar{\lambda} = \eta\delta^{-\frac{1}{2}(r-1)}\lambda, \quad \bar{\mu} = \eta\delta^{-\frac{1}{2}(r+1)}\nu,$$

$$\bar{\nu} = \eta \delta^{\frac{1}{2}(r+1)} \mu, \quad \bar{\pi} = \eta \delta^{\frac{1}{2}(r-1)} \pi,$$

where $\eta = \pm 1$. Now

$$\begin{aligned} \lambda = \bar{\bar{\lambda}} &= \eta \bar{\delta}^{-\frac{1}{2}(r-1)} \bar{\lambda} = (\delta \bar{\delta})^{-\frac{1}{2}(r-1)} \lambda, \\ \mu = \bar{\bar{\mu}} &= \eta \bar{\delta}^{-\frac{1}{2}(r+1)} \bar{\nu} = (\delta \bar{\delta}^{-1})^{\frac{1}{2}(r+1)} \mu. \end{aligned}$$

Since $(\delta \bar{\delta})^{-\frac{1}{2}(r-1)} = (\delta \bar{\delta}^{-1})^{\frac{1}{2}(r+1)} = \delta^{-\frac{1}{2}(q-1)} = -1$, we have $\lambda = \mu = 0$, which is impossible.

(1E) Let V be a vector space over F_p of dimension m on which L acts irreducibly and nontrivially. Then $m \geq 2n$. If moreover L is faithfully represented on V , then $m = 2n$, $m = \frac{8}{3}n$, or $m \geq 4n$. The second case occurs only if 3 divides n .

Proof. Let Γ be the natural representation of L as 2×2 matrices over F_q . For any integer k , where $0 \leq k \leq p-1$, let $\Gamma^{(k)}$ be the representation of L induced from Γ on forms of degree k ; the degree of the representation $\Gamma^{(k)}$ is $k+1$. Let θ be the field automorphism of F_q defined by $\theta: x \rightarrow x^p$ for $x \in F_q$. It is known [6] that every irreducible representation of L over an algebraic closure of F_q is equivalent to one and only one of the form

$$(1.15) \quad \Gamma^{(k_0)} \times \Gamma^{(k_1)\theta} \times \cdots \times \Gamma^{(k_{n-1})\theta^{n-1}},$$

where $0 \leq k_i \leq p-1$, $0 \leq i \leq n-1$, and $\Gamma^{(k_i)\theta^i}$ is the representation of L obtained by applying θ^i to the matrix coefficients of $\Gamma^{(k_i)}$.

Suppose \mathfrak{B} is a non-trivial absolutely irreducible representation of L of form (1.15): the corresponding n -tuple $(k_0, k_1, \dots, k_{n-1}) \neq (0, 0, \dots, 0)$. Let s be the smallest positive integer such that \mathfrak{B} and \mathfrak{B}^{θ^s} are equivalent. Since s divides n , we have $n = st$ for some integer t . k_0, k_1, \dots, k_{s-1} can be arbitrary subject to the requirement not all of them are zero; the remaining k_i are then uniquely determined. The degree of \mathfrak{B} is then $\prod_{i=0}^{s-1} (k_i + 1)^t$. An irreducible representation of L over F_p containing \mathfrak{B} as an absolutely irreducible constituent thus has degree $s \prod_{i=0}^{s-1} (k_i + 1)^t \geq s2^t \geq 2st = 2n$. \mathfrak{B} is faithful if and only if t is odd and the number of odd k_i for $0 \leq i \leq s-1$ is odd. Since $s \prod_{i=0}^{s-1} (k_i + 1)^t < 4st$ holds only if $t = 1, 2$, or 3, this completes the proof of (1E).

(1F) Let V be a vector space over F_l of dimension m , where l is an odd prime different from p . If L acts irreducibly and non-trivially on V , then $m \geq \frac{1}{2}(q-1)$. If l^b is the full power of l in $|L|$, then $m \geq 4b$.

Proof. By [16] the irreducible characters of L have degrees $1, q, q \pm 1, \frac{1}{2}(q \pm 1)$. The four characters of degree $\frac{1}{2}(q \pm 1)$ are irrational, their irrationalities being of the form $\frac{1}{2}(\varepsilon \pm \sqrt{\varepsilon q})$. Since the S_l -subgroups of L are cyclic, we can apply the results of Dade [9]. If D is any non-trivial l -subgroup of L , then $|N_L(D): C_L(D)| = 2$ by (1.4), (1.6). Thus the tree associated with an l -block of positive defect has at most two edges. Every irreducible Brauer character of L with respect to the prime l is then the restriction of an ordinary irreducible character to l -regular elements of L . Thus $m \geq \frac{1}{2}(q-1)$.

Let \mathfrak{B} be an absolutely irreducible constituent of the representation of L on V . If s is the number of non-equivalent algebraic conjugates of \mathfrak{B} over F_l , then $m = s \cdot \deg \mathfrak{B}$. Now $2l^b$ divides $q-1$ or $q+1$. Hence if $\deg \mathfrak{B} \geq q-1$, then $m \geq 2l^b - 2 \geq 4b$. Suppose then that $\deg \mathfrak{B} = \frac{1}{2}(q \pm 1)$. If $s \geq 2$, the preceding argument applies. If $s = 1$, the argument fails in the case $l^b = 3$ and $q = 5$ or 7 . Since $s = 1$, εq must be a quadratic-residue modulo l . Since 5 and -7 are non-residues modulo 3 , these last cases do not occur.

§2. Throughout this section we shall assume G is 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 $|C(j): L_1 L_2| = 2$.

Clearly $j \in Z(L_1) \cap Z(L_2)$, so that q_1, q_2 are odd, and $Z(L_1) = Z(L_2) = \langle j \rangle$. The considerations of §1 apply to L_1 and L_2 . In particular, we can speak of automorphisms of L_1 and L_2 of class T_0, T_1, T_2 , or T_3 . We fix isomorphisms ϕ_i from $SL(2, q_i)$ onto L_i , and attach a subscript i to the symbols used in §1 for various objects defined for $SL(2, q)$ to denote the corresponding objects for $SL(2, q_i)$. Thus we have

$$q_i - \varepsilon_i = 2^{\alpha_i} u_i, \quad q_i + \varepsilon_i = 2v_i, \quad i = 1, 2,$$

where $\varepsilon_i = \pm 1$, $\alpha_i \geq 2$, and u_i, v_i are odd. Suppressing the symbol ϕ_i for

the moment, we have that $Q_i = \langle a_i, b_i \rangle$ is an S_2 -subgroup of L_i of order 2^{e_i+1} . j is the central involution of Q_1 and of Q_2 .

We shall prove the following result:

(2A) Let G be a finite group with property (*). Then one of the following holds:

- (i) $G = C(j)O(G)$.
- (ii) $C(j) = L_1L_2\langle n \rangle$, where $n^2 = 1$, $L_1^n = L_2$, $q_1 = q_2$.
- (iii) $C(j) = L_1L_2\langle n \rangle$, where $n^2 = 1$, $L_1^n = L_1$, $L_2^n = L_2$, n induces automorphisms of class T_1 on L_1 and L_2 , $\alpha_1 = \alpha_2$, and G has only one class of involutions.

We remark that in cases (ii) and (iii) the structure of $C(j)$ is uniquely determined. In case (ii) either (i) holds or $G \simeq PSp(4, q)$ with $q = q_1 = q_2$, [18]. In case (iii) the structure of $C(j)$ is uniquely determined by (1B), (i) cannot hold, and $G \simeq G_2(q)$ or $D_4^2(q)$, [12].

Condition (*) allows a number of possibilities for the structure of $C(j)$. The proof of (2A) involves examination of the fusion of involutions of an S_2 -subgroup of G . We write $g \sim h$ if g and h are fused in G , $g \not\sim h$ if not. We begin with a simple remark.

(2B) If $H \leq G$, T is an S_2 -subgroup of $H \cap C(j)$, and $\langle j \rangle$ is characteristic in T , then T is an S_2 -subgroup of H . In particular, an S_2 -subgroup S of $C(j)$ is one of G .

Proof. Since $\langle j \rangle$ is characteristic in T , $N(T) \leq N(\langle j \rangle) = C(j)$. If U is an S_2 -subgroup of H containing T , then $N_U(T) \leq C(j) \cap U = T$, so that $U = T$. If S is an S_2 -subgroup of $C(j)$ containing Q_1Q_2 , then $|S : Q_1Q_2| = 2$, so that $S' \leq Q_1Q_2$. Since $Z(Q_1Q_2) = \langle j \rangle$, it follows that $\langle j \rangle = S' \cap Z(S)$ is characteristic in S . Taking $H = G$ in the first part of the lemma, we see that S is an S_2 -subgroup of G .

We define

$$(2.1) \quad x = \tau_1\tau_2, \quad y = b_1b_2.$$

Since $\tau_1^2 = \tau_2^2 = b_1^2 = b_2^2 = j$, x and y are involutions of L_1L_2 distinct from j .

(2C) L_1L_2 has exactly two classes of involutions, represented by j and x .

Proof. If $g \in L_1$, $h \in L_2$, $(gh)^2 = 1$, then $g^2 = h^{-2} \in L_1 \cap L_2 = \langle j \rangle$. If $g^2 = h^{-2} = 1$, then g and h are j or 1 , and $gh = 1$ or j . If $g^2 = h^{-2} = j$, then $gh \sim x$ in L_1L_2 , since L_1, L_2 each have only one conjugacy class of elements of order 4.

(2D) $C(j) = L_1L_2\langle n \rangle$, where one of the following holds:

- (i) $L_1^n = L_1$ and $L_2^n = L_2$.
- (ii) $L_1^n = L_2$, $n^2 = 1$ or j , and $q_1 = q_2$.

Proof: Choose $n \in C(j) - L_1L_2$, so that $C(j) = L_1L_2\langle n \rangle$. Since $L_i/\langle j \rangle \simeq PSL(2, q_i)$ is an indecomposable group with a trivial center, it follows by the Krull-Schmidt Theorem that $L_1^n = L_1$, $L_2^n = L_2$, or $L_1^n = L_2$, $L_2^n = L_1$. In the first case, (i) holds. In the second case, $L_1 \simeq L_2$ so that $q_1 = q_2$. Since $n_2 \in L_1L_2$, we have $n^2 = gh$ with $g \in L_1$, $h \in L_2$. Since $n^{-1}hn \in L_1$, $ng^{-1}n^{-1} \in L_2$, we also have

$$\begin{aligned}(ng^{-1})^2 &= n^{-1}n^2g^{-1}ng^{-1} = (n^{-1}hn)g^{-1} \in L_1, \\ (ng^{-1})^2 &= ng^{-1}n^{-1}n^2g^{-1} = (ng^{-1}n^{-1})h \in L_2,\end{aligned}$$

and so $(ng^{-1})^2 \in L_1 \cap L_2 = \langle j \rangle$. Replacing n by ng^{-1} , we have $n^2 \in \langle j \rangle$, which completes the proof of (ii).

(2E) If $C(j) = L_1L_2\langle n \rangle$, $L_1^n = L_2$, and $n^2 = j$, then $G = C(j)O(G)$.

Proof. We may assume the isomorphisms ϕ_i of $SL(2, q_i)$ onto L_i are chosen so that $a_1^n = a_2$, $b_1^n = b_2$, etc. Suppose $(ghn)^2 = 1$ for some $g \in L_1$, $h \in L_2$. Then

$$1 = ghn^2g^n h^n = jgh^n h g^n.$$

Since $jgh^n \in L_1$, $hg^n \in L_2$, and $L_1 \cap L_2 = \langle j \rangle$, it follows that $gh^n = 1$, $hg^n = j$, or $gh^n = j$, $hg^n = 1$. But $(gh^n)^{q^n} = hg^n$, so both cases are impossible. Thus $C(j) - L_1L_2$ contains no involutions, and every involution in $C(j) - \langle j \rangle$ is conjugate to x by (2C).

Now (1. 1), (1. 2), (2. 1) imply that

$$C(x, j) = \langle \rho_1, \rho_2, y, n \rangle,$$

which has the S_2 -subgroup

$$T = \langle a_1, a_2, y, n \rangle.$$

$|T| = 2^{2\alpha+1}$, where $\alpha = \alpha_1 = \alpha_2$; T is defined by the relations

$$\begin{aligned} j^2 &= 1, \quad a_1^{2^{\alpha-1}} = a_2^{2^{\alpha-1}} = j, \quad [a_1, a_2] = 1, \quad a_1^y = a_1^{-1}, \\ a_2^y &= a_2^{-1}, \quad y^2 = 1, \quad a_1^n = a_2, \quad y^n = y, \quad n^2 = j. \end{aligned}$$

In particular $Z(T) = \langle x, j \rangle$.

For any element g of a group X , let $r_X(g)$ be the number of roots of g in X , i.e. the number of elements in X having g as a power. We compute that

$$\begin{aligned} r_T(j) &= \frac{1}{3} (2^{2\alpha-2} - 1) + 2^{2\alpha-2} + 2^{\alpha+1}, \\ r_T(x) &= r_T(xj) = \frac{1}{3} (2^{2\alpha-2} - 1) + 2^{2\alpha-1} - 2^\alpha. \end{aligned}$$

These two numbers differ by $2^\alpha(2^{\alpha-2} - 3) \neq 0$, so that $\langle j \rangle$ is characteristic in T .

By (2B) T is an S_2 -subgroup of $C(x)$ and thus $x \neq j$. In particular, j is conjugate to no other involution of S . The Z^* -theorem of Glauberman [13] implies that $jO(G) \in Z(G/O(G))$, and so $G = C(j)O(G)$.

(2F) Suppose $C(j) = L_1L_2\langle n \rangle$, $L_1^n = L_1$, $L_2^n = L_2$, and $G \neq C(j)O(G)$. Then

- (i) n may be chosen as an involution inducing automorphisms of class T_1 on both L_1 and L_2 , and $\alpha_1 = \alpha_2$;
- (ii) G has only one class of involutions.

Proof. Since $n^2 \in L_1L_2$, the class of the automorphism of L_i induced by n is an element of order 1 or 2 in $\text{Out}(L_i)$, $i = 1, 2$. Let n induce an automorphism of class T_a on L_1 and one of class T_b on L_2 , where $0 \leq a, b \leq 3$. Since n may be changed by an element of L_1L_2 , we may assume n induces the automorphisms $\theta_{a,1}, \theta_{b,2}$ on L_1, L_2 respectively, where these correspond to the automorphisms θ_a, θ_b of $SL(2, q)$ defined in §1. n^2 is an element of L_1L_2 inducing the inner automorphisms $\theta_{a,1}^2$ on L_1 , $\theta_{b,2}^2$ on L_2 . There are two such elements, differing by a factor of j , and these are easily found (see (1. 13)).

Suppose $x \neq j$. Since $G \neq C(j)O(G)$, it follows by (2C) and Glauberman's Z^* -theorem that there exists an involution $t \in C(j) - L_1L_2$ such that $t \sim j$. Using (1B), (1C), (1. 9), (1. 12), we can compute an S_2 -subgroup U

of $C(t, j)$. Except in the case $a = b = 1$, we find that $U' = Z_1 Z_2 \neq 1$, where Z_i is a cyclic subgroup of L_i , $i = 1, 2$. Thus $\langle j \rangle = (U')^m$ for a suitable integer m . U is then an S_2 -subgroup of $C(t)$ by (2B), so U is even an S_2 -subgroup of G . The proof of (2B) shows that $\langle j \rangle$ is characteristic in $N(U)$, so that $j \nmid t$ in $N(U)$. But then $j \nmid t$ in G by Burnside's Theorem. In the case $a = b = 1$, we may assume $n = t$. The involutions of the S_2 -subgroup $S = Q_1 Q_2 \langle n \rangle$ of $C(j)$ which are not in $Q_1 Q_2$ are of the form $a_1^r a_2^s n$. Since $a_1^r a_2^s n = n^g$ with $g = (nb_1)^r (a_1^r nb_2)^s$, all involutions in $C(j) - L_1 L_2$ are conjugate in $C(j)$. The elementary abelian subgroup $V = \langle n, x, j \rangle$ is an S_2 -subgroup of $C(n, j)$. Choose $h \in G$ such that $n^h = j$, $V^h \leq C(j)$. The three subgroups of index 2 in V containing n are $\langle n, j \rangle$, $\langle n, x \rangle$, $\langle n, xj \rangle$; one of these must be transformed by h into a subgroup of $L_1 L_2$. Thus nj , nx , or nxj is fused to an element of $L_1 L_2 - \langle j \rangle$ and hence to x by (2C). Thus $n \sim x \sim j$, which is a contradiction. Hence $x \sim j$ in G .

Now (1. 8), (1. 11), (1. 14) show that an S_2 -subgroup T of $C(x, j)$ is given by

$$T = \langle a_1, a_2, y, n \rangle \text{ or } \langle a_1, a_2, y, nb_1 \rangle.$$

If $\{a, b\} \not\subseteq \{1, 3\}$, then $T' = \langle a_1, a_2 \rangle$, $\langle a_1, a_2^2 \rangle$, $\langle a_1^2, a_2 \rangle$, or $\langle a_1^2, a_2^2 \rangle$, and $\langle j \rangle = (T')^m$ for some integer m . But then $\langle j \rangle$ is characteristic in T , so by (2B) T is an S_2 -subgroup of $C(x)$. This is impossible since $x \sim j$. Hence $\{a, b\} \subseteq \{1, 3\}$, and $T' = \langle a_1^2, a_1 a_2 \rangle$. If $\alpha_1 \neq \alpha_2$, then $\langle j \rangle = \langle T' \rangle^m$ for some m , and again this is impossible. Hence $\{a, b\} \subseteq \{1, 3\}$ and $\alpha_1 = \alpha_2$. A calculation readily shows that if (i) fails, then $r_T(j)$ is different from $r_T(x)$, $r_T(xj)$, so that $\langle j \rangle$ is characteristic in T . This is again impossible, and so (i) holds.

$T = \langle a_1, a_2, y, n \rangle$ is an S_2 -subgroup of $C(x, j)$. Since $x \sim j$, we may choose $g \in G$ such that $x^g = j$, $T^g \leq C(j)$. $X = \langle a_1, a_2, y \rangle$ is generated by $a_1 y$, $a_2 y$, y , which are involutions conjugate to x . If $n \nmid j$, then necessarily $X^g \leq L_1 L_2$. In particular, $j^g \in L_1 L_2 - \langle j \rangle$; by (2C) we may assume $j^g = x$. Since X is an S_2 -subgroup of $C_{L_1 L_2}(x)$, we may even assume $X^g = X$. But $X' = \langle a_1^2, a_2^2 \rangle$, and so $\langle j \rangle = (X')^m$ for a suitable integer m . Thus $\langle j \rangle$ is characteristic in X , and $j^g = j$. This contradiction shows that $n \sim j$, and (ii) holds.

The results (2D), (2E), (2F) together prove (2A). Summarizing our calculations, we see that if $C(j)$ satisfies the assumptions of (2F), then

$$C(x, j) = \langle \rho_1, \rho_2, y, n \rangle, \quad C(n, j) = \langle \sigma_1, \sigma_2, x, n \rangle.$$

Moreover, $\langle a_1, a_2, y, n \rangle$, $\langle j, x, n \rangle$ are S_2 -subgroups of $C(x, j)$, $C(n, j)$ respectively.

§3. From now on we assume that G satisfies condition (*) and case (iii) of (2A). In this section we shall prove that q_1 and q_2 are powers of the same prime p .

(3A) Let D be a 4-subgroup of G . Then D is conjugate to $\langle x, j \rangle$ or $\langle n, j \rangle$. Moreover, $N(D)/C(D)$ is isomorphic to S_3 , the symmetric group on 3 symbols.

Proof. We may assume $j \in D$ by (2A), so that $D \leq C(j)$. Since all involutions in $C(j) - \langle j \rangle$ are conjugate in $C(j)$ to x or n by (2C) and the proof of (2F), it follows that D is conjugate to $\langle x, j \rangle$ or $\langle n, j \rangle$. Now $x \sim xj$ and $n \sim nj$ in $C(j)$. Since G has one class of involutions, it readily follows that $|N(D):C(D)| = 6$ and $N(D)/C(D) \simeq S_3$.

It will be convenient to introduce the following notation: let the images of $\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix}$, $\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ under the isomorphism ϕ_i of $SL(2, q_i)$ onto L_i be denoted by $x_i(\alpha)$, $x_{-i}(\alpha)$, $h_i(\alpha)$, ω_i respectively, $i = 1, 2$. Moreover, let X_i , X_{-i} , H_i be the subgroups of L_i generated by elements of the form $x_i(\alpha)$, $x_{-i}(\alpha)$, $h_i(\alpha)$ respectively. We note that $L_i = X_i H_i \cup X_i H_i \omega_i X_i$, $i = 1, 2$. Let δ_1, δ_2 be non-squares of order a power of 2 in F_{q_1}, F_{q_2} respectively. We may assume n acts on L_i as conjugation by $\begin{pmatrix} 0 & 1 \\ -\delta_i & 0 \end{pmatrix}$ if $\varepsilon_i = 1$, and by $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ if $\varepsilon_i = -1$. Set

$$h_0 = nd_1 d_2,$$

where $d_i = \varphi_i \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ if $\varepsilon_i = 1$, $d_i = 1$ if $\varepsilon_i = -1$. Then $C(j) = \langle L_1 L_2, h_0 \rangle$, where h_0 acts on L_i as conjugation by $\begin{pmatrix} 1 & \\ & \delta_i \end{pmatrix}$. Moreover,

$$(3.1) \quad h_0^2 = h_1(\delta_1^{-1}) h_2(\delta_2^{-1}).$$

In particular, h_0 centralizes $H_1 H_2$, $h_0^2 \in H_1 H_2$. Thus

$$(3.2) \quad H = \langle H_1 H_2, h_0 \rangle$$

is abelian of order $(q_1 - 1)(q_2 - 1)$.

(3B) Let $\{a, b\} = \{1, 2\}$, and let $K = O(C(X_b))$. Then the following hold:

- (i) An S_2 -subgroup of L_a is one of $C(X_b)$.

- (ii) $C(X_b) = L_a K$, $N(X_b) = HL_a K$, and $K \cap L_a = 1$.
- (iii) K/X_b is abelian, and j inverts K/X_b .

Proof. Since $C(X_b) \cap C(j) = L_a X_b$, the subgroup Q_a of L_a is an S_2 -subgroup of $C(X_b) \cap C(j)$. Since $\langle j \rangle$ is characteristic in the generalized quaternion group Q_a , it follows by (2B) that Q_a is then an S_2 -subgroup of $C(X_b)$, which proves (i). Now $K \cap L_a$ is a normal subgroup of odd order in L_a , so that necessarily $K \cap L_a = 1$. Now the Brauer-Suzuki Theorem [7] implies that $K\langle j \rangle \triangleleft C(X_b)$, so by the Frattini argument

$$C(X_b) = K(C(j) \cap C(X_b)) = KX_b L_a = KL_a.$$

Since $K\langle j \rangle$ is characteristic in $C(X_b)$, we have $K\langle j \rangle \triangleleft N(X_b)$ so again by the Frattini argument

$$N(X_b) = K(C(j) \cap N(X_b)) = KL_a H,$$

which proves (ii). If j centralizes $kX_b \pmod{X_b}$ for some $k \in K$, then $k^{-1}jk \in jX_b$, and necessarily $k \in C(j)$. Thus $k \in C(X_b) \cap C(j) = L_a X_b$. Write $k = mu$ with $m \in L_a$, $u \in X_b$. Then $m = ku^{-1} \in L_a \cap K = 1$, and so $k = u \in X_b$. Thus j inverts K/X_b , which proves (iii).

(3C). Let $u \neq 1$ be in X_b , and let $M = O(C(u))$. Then

- (i) $X_b \leq M$.
- (ii) $C(u) = ML_a$, $M \cap L_a = 1$.
- (iii) $C(j) \cap M = X_b$.

Proof. Since $C(u) \cap C(j) = L_a X_b$, it follows as in the proof of (3B) (i) that Q_a is an S_2 -subgroup of $C(u)$. By the Brauer-Suzuki Theorem, $M\langle j \rangle \triangleleft C(u)$, and so $C(u) = M(C(j) \cap C(u)) = MX_b L_a$. But L_a normalizes MX_b . Thus $MX_b \triangleleft MX_b L_a = C(u)$ and so $X_b \leq M$, $C(u) = ML_a$. Since $M \cap L_a \triangleleft L_a$, clearly $M \cap L_a = 1$, which completes the proof of (i), (ii). Suppose $m \in C(j) \cap M$. Since m has odd order, we may write $m = g_1 g_2$, where g_i is an element of odd order in L_i , $i = 1, 2$. m and g_a centralize u , so that $g_b \in C(u) \cap L_b = \langle j \rangle X_b$. But since g_b has odd order, $g_b \in X_b \leq M$. But now $g_a = mg_b^{-1} \in M \cap L_a = 1$, and so $m = g_b$, which proves (iii).

(3D) If $q_1 - \varepsilon_1 > q_2 - \varepsilon_2$, then $(q_1 - \varepsilon_1)q_2^3$ divides $|G|$.

Proof. $C(x, j) = \langle \rho_1, \rho_2, y, n \rangle$ has a normal abelian 2-complement consisting of the 2^α -th powers of elements in $\langle \rho_1, \rho_2 \rangle$, where $\alpha = \alpha_1 = \alpha_2$. The

subgroup $R = \langle \rho_1^{q_2 - \varepsilon_2} \rangle$ is characteristic in $C(x, j)$, since R consists of all $\frac{1}{2^\alpha} (q_2 - \varepsilon_2)$ -th powers of elements in the normal 2-complement. Moreover, $R \neq 1$ since $q_1 - \varepsilon_1 > q_2 - \varepsilon_2$.

By (1. 1), (1. 8),

$$(3. 3) \quad C(R, j) = \langle \rho_1, nb_1 \rangle L_2,$$

which has as an S_2 -subgroup $T = \langle nb_1, a_2, b_2 \rangle$. T has order $2^{2\alpha+1}$ with relations

$$\begin{aligned} (nb_1)^{2^\alpha} &= a_2^{2^\alpha - 1} = b_2^2 = j, \\ a_2^{nb_1} &= a_2^{-1}, \quad b_2^{nb_1} = b_2 a_2, \quad a_2^{b_2} = a_2^{-1}. \end{aligned}$$

If we set

$$s_1 = a_2 nb_1 b_2, \quad s_2 = nb_1 b_2, \quad t = (nb_1)^{2^\alpha - 1} b_2,$$

then $T = \langle s_1, s_2, t \rangle$, where

$$s_1^{2^\alpha} = s_2^{2^\alpha} = t^2 = [s_1, s_2] = 1, \quad s_1^t = s_2.$$

Thus T is the wreath product of Z_{2^α} by Z_2 . Since $T' = \langle a_2 \rangle$, $\langle j \rangle$ is characteristic in T . T is then an S_2 -subgroup of $C(R)$ by (2B).

The Frattini argument implies that

$$N(R) = C(R) (N(R) \cap N(T)) = C(R) (N(R) \cap C(j)).$$

Choose $g \in N(\langle x, j \rangle)$ such that $x^g = j$; this is possible by (3A). Since R is characteristic in $C(x, j)$, it follows that $g \in N(R)$, so that $g = cd$, where $c \in C(R)$, and $d \in N(R) \cap C(j)$. Thus $x^g = x^c = j$, and $x \sim j$ in $C(R)$. Now we can verify that Theorem 2 of [4] applies to $C(R)$ with $\beta = a_2$, $J = j$. Using (3. 3) we can compute that

$$\begin{aligned} c(R, j) &= (q_1 - \varepsilon_1) q_2 (q_2^2 - 1), \\ c(R, a_2) &= (q_1 - \varepsilon_1) (q_2 - \varepsilon_2), \\ c(R, j, t) &= (q_1 - \varepsilon_1) (q_2 - \varepsilon_2), \\ c(R, a_2, t) &= q_1 - \varepsilon_1. \end{aligned}$$

The numbers in [4] denoted by a, c, t, ε, f are readily computed to be $1, q_1 - \varepsilon_1, 1, \varepsilon_2, \varepsilon_2 q_2$ respectively. It then follows that

$$|C(R)| = (q_1 - \varepsilon_1) q_2^3 (q_2^2 - 1) (q_2^2 + \varepsilon_2 q_2 + 1),$$

which proves (3D).

We shall prove another similar result, for which we need the following:

(3E) Let X be a finite group with an involution i such that $C(i) = Z \times L \langle t \rangle$, where $L \simeq SL(2, q)$, Z is a cyclic group of order dividing $\frac{1}{2}(q + \varepsilon)$ with $\varepsilon = \pm 1$, $q \equiv \varepsilon \pmod{4}$, and t is an involution inducing an automorphism of class T_1 on L . Suppose moreover that $t \sim i$ in X . Then $|X|$ is divisible by $|Z|q^3$ unless $q = 3$ and $X \simeq M_{11}$, the Mathieu group of order 7920. If $q = 3$ and $X \not\simeq M_{11}$, then $X \simeq SL(3, 3)$. Finally, if $Z = 1$, then $q = 3, 5$, or 7 .

Proof. This is essentially a result of Brauer. The case $\varepsilon = -1$ is treated in Sections 4, 9, 10 of [3], II. We indicate in §8 the modifications needed to treat the case $\varepsilon = 1$.

(3F) If $q_1 + \varepsilon_1 > q_2 + \varepsilon_2$, then $(q_1 + \varepsilon_1)q_2^3$ divides $|G|$. If $q_1 > q_2 = 3$, then L_1 has a cyclic subgroup R of order $\frac{1}{2}(q_1 + \varepsilon_1)$ such that $C(R) = R \times M$, $C(R, j) = RL_2 \langle n \rangle$, and $M \simeq SL(3, 3)$.

Proof. $C(n, j) = \langle \sigma_1, \sigma_2, x, n \rangle$ has a normal abelian 2-complement $\langle \sigma_1^2, \sigma_2^2 \rangle$. If $R = \langle \sigma_1^{q_1 + \varepsilon_1} \rangle$, then R is characteristic in $C(n, j)$, and since $q_1 + \varepsilon_1 > q_2 + \varepsilon_2$, $R \neq 1$. By (1.5), $C(R, j) = \langle \sigma_1, n \rangle L_2 = \langle \sigma_1^2 \rangle \times L_2 \langle n \rangle$. The same arguments as in (3D) show that $\langle a_2, b_2, n \rangle$ is an S_2 -subgroup of $C(R)$ and that $n \sim j$ in $C(R)$. If we set $X = C(R)/R$, the conditions of (3E) are satisfied with $Z = \langle \sigma_1^2 \rangle / R$. Since $x \in N(R)$, x induces an automorphism of X . If this automorphism were inner, the 2-group $\langle a_2, b_2, n, x \rangle$ obtained by adjoining x to the S_2 -subgroup $\langle a_2, b_2, n \rangle$ of $C(R)$ would have a center of order at least 4. But $Z(\langle a_2, b_2, n, x \rangle) = \langle j \rangle$. Thus $X \not\simeq M_{11}$ since all automorphisms of M_{11} are inner [15]. By (3E), $|X|$ is divisible by $|Z|q_2^3$, so that $|C(R)|$ is divisible by $|R| |Z|q_2^3 = \frac{1}{2}(q_1 + \varepsilon_1)q_2^3$.

If $q_1 > q_2 = 3$, then $R = \langle \sigma_1^2 \rangle$ is cyclic of order $\frac{1}{2}(q_1 + \varepsilon_1)$. By (3E), $C(R)/R \simeq SL(3, 3)$. A modification of the method of [17] shows that $SL(3, 3)$ has trivial Schur multiplier. Hence $C(R) = R \times M$, where $M \simeq SL(3, 3)$. This proves (3F).

(3G) Let q_1, q_2 be powers of the prime numbers p_1, p_2 respectively. If $q_1 > q_2$ and $p_1 \neq p_2$, then an S_{p_2} -subgroup of $C(j)$ is not an S_{p_2} -subgroup of G .

Proof. We note $q_1 + \varepsilon_1 > q_2 + \varepsilon_2$ and $q_1 - \varepsilon_1 > q_2 - \varepsilon_2$ both hold except in the case $q_1 = q_2 + 2$. Since the order of an S_{p_2} -subgroup of $C(j)$ divides $(q_1 - \varepsilon_1)q_2$ or $(q_1 + \varepsilon_1)q_2$, the result follows from (3D) and (3F).

(3H) If $q_1 > q_2$ and $p_1 \neq p_2$, then $q_1 = 5$, $q_2 = 3$.

Proof. Let P be an S_{p_2} -subgroup of L_1 , X_2 the S_{p_2} -subgroup of L_2 introduced at the beginning of §3, and $K = O(C(X_2))$. By (3B), we have $C(X_2) = KL_1$. Now PX_2 is an S_{p_2} -subgroup of $C(j)$, and $C(PX_2) \cap C(j) = C_{L_1}(P)X_2$. An S_2 -subgroup T of this subgroup is cyclic or generalized quaternion, so by (2B), T is an S_2 -subgroup of $C(PX_2)$. The Frattini argument then implies

$$N(PX_2) = C(PX_2)(N(PX_2) \cap N(T)) = C(PX_2)(N(PX_2) \cap C(j)),$$

so that $N(PX_2)/C(PX_2) \cong (N(PX_2) \cap C(j))/(C(PX_2) \cap C(j))$. But PX_2 is an abelian S_{p_2} -subgroup of $C(j)$, so that p_2 does not divide $|N(PX_2)/C(PX_2)|$. Since PX_2 is not an S_{p_2} -subgroup of G and so not one of $N(PX_2)$ by (3G), it follows that PX_2 is not an S_{p_2} -subgroup of $C(PX_2)$, and hence not one of $C(X_2)$. It follows that p_2 divides $|K/X_2|$.

Set $t = x$ if $\varepsilon_2 = 1$, $t = n$ if $\varepsilon_2 = -1$, and $D = \langle t, j \rangle$. By the definition of x , n , and (1.7), D normalizes X_2 and hence K . Since j inverts K/X_2 by (3B), we have

$$K/X_2 = C_{K/X_2}(t) \times C_{K/X_2}(tj),$$

and indeed, since $|X_2|$ is odd,

$$(3.4) \quad K/X_2 = C_K(t)C_K(tj)X_2/X_2.$$

For any group Y , let $m(Y)$ be the minimum number of generators of an S_{p_2} -subgroup of Y . If $q_2 = p_2^n$, then $m(X_2) = n$. Since P is cyclic and t, tj are conjugate to j , it follows that

$$m(C(t)) = m(C(tj)) = m(C(j)) \leq n + 1.$$

By (3.4), we have

$$(3.5) \quad m(K/X_2) \leq 2m(C(j)) \leq 2(n + 1).$$

Let M be a normal subgroup of $C(X_2)$ such that $K > M \geq X_2$, K/M is a p_2 -group, and M is maximal subject to these conditions. Then K/M is an elementary abelian p_2 -group admitting L_1 as an irreducible group of operators. By (1F),

$$m(K/M) \geq \frac{1}{2} (q_1 - 1).$$

Since $m(K/M) \leq m(K/X_2)$ and $q_1 \geq q_2 + 2$, we find from

(3.5) that

$$(3.6) \quad \frac{1}{2} (q_2 + 1) \leq \frac{1}{2} (q_1 - 1) \leq 2m(C(j)) \leq 2(n + 1).$$

Since $q_2 = p_2^n$, we have in particular

$$p_2^{\frac{1}{4}(q_2-3)} \leq q_2.$$

By calculus,

$$\begin{aligned} 11^{\frac{1}{4}(x-3)} &> x \quad \text{for } x \geq 7, \\ 7^{\frac{1}{4}(x-3)} &> x \quad \text{for } x > 7, \\ 5^{\frac{1}{4}(x-3)} &> x \quad \text{for } x \geq 11, \\ 3^{\frac{1}{4}(x-3)} &> x \quad \text{for } x \geq 15. \end{aligned}$$

The only possibilities are

$$\begin{aligned} p_2 = q_2 = 7, \\ p_2 = q_2 = 5, \\ p_2 = 3, \quad q_2 = 3 \quad \text{or } 9. \end{aligned}$$

If $q_2 = 7$, then (3.6) gives $4 \leq \frac{1}{2} (q_1 - 1) \leq 2m(C(j)) \leq 4$, so that $q_1 = 9$, $m(C(j)) = 2$. This is impossible since 7 does not divide $|L_1|$ so that $m(C(j)) = 1$.

If $q_2 = 5$, then (3.6) gives $3 \leq \frac{1}{2} (q_1 - 1) \leq 4$, so that $q_1 = 7$ or 9. This contradicts the assumption (2A) (iii) is the case, since $\alpha_1 = 3$, $\alpha_2 = 2$ in this situation.

If $q_2 = 9$, then (3.6) gives $5 \leq \frac{1}{2} (q_1 - 1) \leq 6$, so that $q_1 = 11$ or 13. Again this contradicts the assumption that (2A) (iii) holds, since then $\alpha_1 = 2$, $\alpha_2 = 3$.

If $q_2 = 3$, then (3.6) gives $2 \leq \frac{1}{2} (q_1 - 1) \leq 4$, so that $q_1 = 5, 7$, or 9. Since $p_1 \neq 3$, we have $q_1 \neq 9$. Since $\alpha_1 = \alpha_2 = 2$, $q_1 \neq 7$. Hence $q_1 = 5$ and (3H) is proved.

(3I) In any faithful representation of $SL(2,5)$ as a subgroup of the symplectic group $Sp(4,3)$, the vectors fixed by an element of order 3 in $SL(2,5)$ form a singular subspace of dimension 2.

Proof. $SL(2,5)$ is given by generators α, β, γ satisfying the relations

$$(3.7) \quad \alpha^5 = \beta^4 = 1, \quad \gamma^2 = \beta^2, \quad \alpha^\beta = \alpha^{-1}, \quad \beta^\gamma = \beta^{-1}, \quad (\alpha\gamma)^3 = 1.$$

(We may take $\alpha = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, $\beta = \begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix}$, $\gamma = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.) Thus we look for elements of $Sp(4,3)$ satisfying these relations.

Choose a basis e_1, e_2, e_3, e_4 of the 4-dimensional symplectic vector space over F_3 , satisfying

$$\begin{aligned} (e_1, e_2) &= (e_3, e_4) = 1, \\ (e_1, e_3) &= (e_1, e_4) = (e_2, e_3) = (e_2, e_4) = 0, \end{aligned}$$

and identify elements of $Sp(4,3)$ with their matrices with respect to this basis.

$Sp(4,3)$ has only one conjugacy class of elements of order 5. Hence we can take

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

Since $\langle \alpha \rangle$ is self-centralizing modulo $\langle -I \rangle$, the elements of $Sp(4,3)$ inverting α are all conjugate modulo $\langle -I \rangle$. Since the relations (3.7) are unchanged if β is replaced by β^{-1} , we may assume that

$$\beta = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}.$$

Now a computation shows there are only two possibilities for the element γ satisfying (3.7):

$$\gamma = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 0 & -1 & 0 & -1 \\ -1 & 0 & -1 & 0 \\ 0 & -1 & 0 & 1 \\ -1 & 0 & 1 & 0 \end{pmatrix}.$$

The element $\alpha\gamma$ of order 3 is

$$\begin{pmatrix} -1 & -1 & 1 & -1 \\ -1 & 0 & 1 & 1 \\ -1 & -1 & -1 & 1 \\ 1 & -1 & 1 & 0 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 0 & -1 & -1 & 0 \\ 0 & -1 & -1 & -1 \\ 1 & 0 & 0 & 1 \\ -1 & 1 & 0 & -1 \end{pmatrix},$$

and its space of fixed vectors has basis

$$\{(1, 0, 0, 1), (0, 1, 1, 0)\} \quad \text{or} \quad \{(1, 1, 1, 0), (-1, 1, 0, 1)\}.$$

In both cases the subspace is singular. Since $SL(2, 5)$ has only one conjugacy class of elements of order 3, we have the result. (The calculation that $Sp(4, 3)$ has two conjugacy classes of subgroups isomorphic to $SL(2, 5)$ is due to Dickson [10]).

(3J) The case $q_1 = 5$, $q_2 = 3$ cannot occur.

Proof. Suppose $q_1 = 5$, $q_2 = 3$. As in the proof of (3H), we consider $C(X_2)$. $L_1 \simeq SL(2, 5)$ is represented irreducibly and faithfully on the elementary abelian 3-group K/M . Since 5 does not divide $|GL(3, 3)|$, it follows that $m(K/M) \geq 4$. By (3.5), $m(K/X_2) \leq 4$ and thus $m(K/M) = m(K/X_2) = 4$. The S_3 -subgroups of $C(j)$ are elementary abelian of order 9, and since $t \sim tj \sim j$ in G , it follows by (3.4) that the S_3 -subgroup of K/X_2 is elementary abelian of order 81. Since L_1 has no subgroups of order 15, an S_3 -subgroup of $C(j)$ is contained in no larger subgroup of odd order in $C(j)$. The same is true for $C(t)$ and $C(tj)$. Since K contains S_3 -subgroups of $C(t)$ and $C(tj)$, it follows that $C_K(t)$, $C_K(tj)$ are S_3 -subgroups of $C(t)$, $C(tj)$ respectively. Hence K/X_2 is a 3-group of order 3^4 , and $M = X_2$.

By (3F), L_1 has a subgroup R of order 3 such that

$$C(R) = R \times N, \quad C(R, j) = RL_2\langle n \rangle$$

where $N \simeq SL(3, 3)$. Since $L_2\langle n \rangle \simeq GL(2, 3)$, a group with no normal subgroup of index 3, $L_2\langle n \rangle \leq N$. Now N has two conjugacy classes of subgroups of order 3, whose centralizers in N have orders 9 or 54. Since $j \in C_N(X_2)$, we must have $|C_N(X_2)| = 54$. Let Z be an S_3 -subgroup of $C_N(X_2)$. Z is an S_3 -subgroup of N and so $Z' \neq 1$. Since $RC_Z(j) \leq C(j)$ and $C_Z(j) \geq X_2$, we necessarily have $C_Z(j) = X_2$. Thus j has no fixed-points on Z/X_2 , and j inverts Z/X_2 . Since j centralizes $C(X_2)/K$, K contains all elements of odd

order in $C(X_2)$ which are inverted by j modulo X_2 . In particular, $Z \leq K$ and K is non-abelian.

It now follows that

$$Z(K) = K' = D(K) = X_2,$$

since L_1 acts irreducibly on K/X_2 , and so K is extra special of order 3^5 [14]. Since $[L_1, X_2] = 1$, we have a faithful representation of $L_1 \simeq SL(2, 5)$ on the 4-dimensional symplectic space K/X_2 . The subgroup R fixes the elements of Z/X_2 , which is a non-singular subspace of dimension 2 in K/X_2 since Z is non-abelian. But this contradicts (3I).

Together with (3H), this proves

(3K) If G is a finite group with property (*) and (2A) (iii) holds, then q_1 and q_2 are powers of the same prime p .

§4. From now on we may assume $q_1 = p^{n_1}$, $q_2 = p^{n_2}$. Thus $\varepsilon_1 = \varepsilon_2 = \varepsilon$, and the group H of (3. 2) is the direct product of two cyclic subgroups of orders $q_1 - 1$ and $q_2 - 1$. Let D be the 4-subgroup contained in H , and denote the involutions in D by

$$j = j_0, j_1, j_2.$$

By (3A) and the final remark of §2, we have $|C(D)| = 2(q_1 - 1)(q_2 - 1)$. Since $\omega_1\omega_2$ inverts H and H is abelian, it follows that

$$(4. 1) \quad C(D) = \langle H, \omega_1\omega_2 \rangle.$$

By (3A) there exists an element $\eta \in N(D)$ permuting the involutions of D cyclically. We may assume that η has order a power of 3 and that

$$\eta: j_0 \rightarrow j_1 \rightarrow j_2 \rightarrow j_0.$$

Since $\omega_1, \omega_2, \eta \in N(D)$, it follows that

$$(4. 2) \quad N(D) = \langle C(D), \omega_1, \eta \rangle.$$

Since D is characteristic in H , $N(H) \leq N(D)$. Suppose $D < H$. Then H is the unique subgroup of its isomorphism type in $C(D)$ by (4. 1), so that H is characteristic in $C(D)$ and hence normal in $N(D)$. Thus $N(H) = N(D)$ in all cases. η and $\omega_1\omega_2$ commute modulo H , so $W = N(H)/H$ is dihedral of order 12. If $D \neq H$, then (4. 1) implies that $C(H) = H$. We have thus proved

(4A) Let D be the 4-subgroup of H . Then $N(D) = N(H) = \langle H, \omega_1, \omega_2, \eta \rangle$, and $W = N(H)/H$ is dihedral of order 12. If $D \neq H$, then $C(H) = H$.

(4B) Let π be a p -element of $C(j)$ inverted by j_1 or j_2 . Then $\pi \in X_a X_b$, where $a \in \{1, -1\}$, $b \in \{2, -2\}$. If P is a p -subgroup of $C(j)$ inverted by j_1 or j_2 , then $P \leq X_a X_b$, where $a \in \{1, -1\}$, $b \in \{2, -2\}$.

Proof. Since $\pi \in L_1 L_2$, we may express $\pi = \pi_1 \pi_2$ with $\pi_i \in L_i$. Every conjugate of X_i in L_i different from X_i is of the form $u^{-1} X_{-i} u$ for a suitable u in X_i . Thus if $\pi_i \notin X_i$, then

$$(4.3) \quad \pi_i = u^{-1} v u$$

for some $u \in X_i$, $v \in X_{-i}$, $v \neq 1$. Now j_1, j_2 invert X_i and X_{-i} . Conjugating (4.3) by j_1 or j_2 then gives $\pi_i^{-1} = u v^{-1} u^{-1}$. Since π_i^{-1} is also $(u^{-1} v u)^{-1} = u^{-1} v^{-1} u$, it follows that u^2 and v^{-1} commute. But $u^2 \in X_i$ whereas $v \in X_{-i}$, and $v \neq 1$. Thus $u^2 = 1$, and $u = 1$, which proves the first part of (4B). The second follows from the fact that if $g \neq 1$, $h \neq 1$, and $g \in X_i$, $h \in X_{-i}$, then $\langle g, h \rangle$ is not a p -group.

(4C) Let $\pi \neq 1$ be in $X_a X_b$, with $a \in \{1, -1\}$, $b \in \{2, -2\}$.

(i) If $\pi \notin X_a \cup X_b$, then the number of conjugates of π under H is $\frac{1}{2}(q_1 - 1)(q_2 - 1)$; these all belong to $X_a X_b - X_a - X_b$.

(ii) If $\pi \in X_a$ or X_b , then the conjugates of π under H consist of all non-identity elements of X_a or X_b respectively.

Proof. We note from the definition of H that H normalizes X_i, X_{-i} for $i = 1, 2$. The result is an easy consequence of the action of H on X_i, X_{-i} .

(4D) Suppose $q_1 = q_2 = 3$ is not the case. Then one of the following holds:

(i) Some element $\pi \neq 1$ in $X_1 X_2$ is in the center of an S_p -subgroup of G .

(ii) For some $\pi \neq 1$ in X_1 or X_2 , $c(\pi) = 0 \pmod{q_1^3 q_2^3}$.

Proof. Let $\{a, b\} = \{1, 2\}$, and let $K = O(C(X_b))$. By (3B), K admits HL_a and j inverts K/X_b . As an L_a -group, K/X_b has composition factors which are faithful irreducible L_a -modules over prime fields. In particular,

a factor which is a p -group has order m , where $m = q_a^2$, $m = q_a^{8/3}$, or $m \geq q_a^4$ by (1G). Since D normalizes L_a and K , the Brauer-Wielandt Theorem [3], II, (6E) implies that $|K|_p \leq q_a^2 q_b^3$.

Arrange notation so that $q_1 \geq q_2$. Let $b = 2$ in the preceding paragraph, and let M/X_2 be the S_p -subgroup of K/X_2 . If $M = X_2$, then $X_1 X_2$ is an S_p -subgroup of $C(X_2)$. If P is then an S_p -subgroup of G containing $X_1 X_2$ then $Z(P) \leq C(X_2)$ so that $Z(P) \leq L_1 K$. By Sylow's Theorem, $Z(P)^g \leq X_1 X_2$ for some $g \in L_1 K$. Thus (i) holds since $Z(P) \neq 1$.

Suppose then that $M > X_2$. Since D normalizes M and X_1 , we have that $|M| \leq q_1^2 q_2^3$, $|M/X_2| \leq q_1^2 q_2^2$. If $q_1^4 \leq |M/X_2|$, then $q_1^4 \leq q_1^2 q_2^2$ and necessarily $q_1 = q_2$, so that $c(X_2) \equiv 0 \pmod{q_1^3 q_2^3}$. In this case, (ii) holds for any $\pi \neq 1$ in X_2 . By (1G) and the discussion in the first paragraph, we may assume that L_1 is irreducible, faithful on M/X_2 , and that $|M/X_2| = q_1^2$ or $q_1^{8/3}$.

We define $M_i = M \cap C(j_i)$ for $i = 0, 1, 2$. M_0 is then X_2 . Since $\omega_1 \in N(M)$ and $\omega_1: j_1 \rightarrow j_2 \rightarrow j_1$, it follows that ω_1 interchanges M_1 and M_2 . In particular, $|M_1| = |M_2|$, and since $M > X_2$, M_1 and M_2 are not trivial. Since j inverts M_1 and M_2 , $\eta M_1 \eta^{-1}$ and $\eta^2 M_2 \eta^{-2}$ are p -subgroups of $C(j)$ inverted by j_2 and j_1 . Thus by (4B)

$$(4.4) \quad M_1 \leq (X_a X_b)^\eta, \quad M_2 \leq (X_c X_d)^{\eta^2}$$

where $a, c \in \{1, -1\}$, $b, d \in \{2, -2\}$. We note that H normalizes each M_i , $i = 0, 1, 2$, by the definition of M_i .

Suppose $|M/X_2| = q_1^{8/3}$. Since $|M_1| = q_1^{4/3} > q_1 \geq q_2$, and $M_1^{\eta^{-1}} \leq X_a X_b$, we have that $|M_1^{\eta^{-1}}| |X_a| > |X_a X_b| \geq |M_1^{\eta^{-1}} X_a|$, and so $M_1^{\eta^{-1}} \cap X_a > 1$. A similar argument shows that $M_1^{\eta^{-1}} \cap X_b > 1$. Conjugating these relations by H then implies that X_a and X_b are both in $M_1^{\eta^{-1}}$. Thus

$$M_1 = (X_a X_b)^\eta, \quad M_2 = (X_c X_d)^{\eta^2}$$

so that $q_1^{4/3} = q_1 q_2$, and $q_1 = q_2^3$. $q_1^3 q_2^3$ then divides $c(X_2)$, and (ii) holds for any $\pi \neq 1$ in X_2 .

Suppose $|M/X_2| = q_1^2$. Let P be an S_p -subgroup of G containing $X_1 M$. If $z \neq 1$ is in $Z(P)$, then $z \in C(X_2)$ so that $z \in X_1 M$, and we may write

$$z = \pi z_0 z_1 z_2$$

where $\pi \in X_1$, $z_i \in M_i$ for $i = 0, 1, 2$. If $z_1 = z_2 = 1$, then $z = \pi z_0 \in X_1 X_2$ and (i) holds. Assume then that $z_1 \neq 1$ or $z_2 \neq 1$. Since z , z_0 , and π centralize $X_1 X_2$, it follows that $z_1 z_2 = z_0^{-1} \pi^{-1} z \in C(X_1 X_2)$. Conjugating this

inclusion by j_1 and j_2 then gives $z_1 z_2^{-1} \in C(X_1 X_2)$, $z_1^{-1} z_2 \in C(X_1 X_2)$ respectively. Thus $z_1^2, z_2^2 \in C(X_1 X_2)$, so that $z_1, z_2 \in C(X_1 X_2)$.

Now $M_1, X_a^\gamma, X_b^\gamma$ are normalized by H . By (4C) it follows that if $X_a^\gamma \cap M_1 > 1$ or $X_b^\gamma \cap M_1 > 1$, then $X_a^\gamma \leq M_1$ or $X_b^\gamma \leq M_1$ respectively. A similar remark holds for $M_2, X_c^{\gamma^2}$ and $X_d^{\gamma^2}$. If the projection of M_1 into X_a^γ were 1-1, then $|M_1| \leq q_2$. If $q_1 > q_2$, then necessarily $M_1 \cap X_a^\gamma > 1$ and $X_a^\gamma \leq M_1$. If the projection of M_1 into X_b^γ is not 1-1, then $M_1 \cap X_b^\gamma > 1$ and $X_b^\gamma \leq M_1$. A comparison of orders then gives $M_1 = X_a^\gamma$. If $q_1 = q_2 = q$ and if $M_1 \cap X_a^\gamma = M_1 \cap X_b^\gamma = 1$, then M_1 contains an element of $(X_a X_b - X_a - X_b)^\gamma$ and hence $\frac{1}{2}(q-1)^2$ such elements by (4C). Since $\frac{1}{2}(q-1)^2 > q-1$ for $q > 3$, this is impossible if $q > 3$. Similar comments apply to M_2 . Thus

$$(4.5) \quad \begin{aligned} M_1 &= X_a^\gamma, M_2 = X_c^{\gamma^2} \quad \text{if } q_1 > q_2, \\ M_1 &= X_a^\gamma \quad \text{or } X_b^\gamma, M_2 = X_c^{\gamma^2} \quad \text{or } X_d^{\gamma^2} \quad \text{if } q_1 = q_2 > 3. \end{aligned}$$

Suppose $z_1 \neq 1$, so that $z_1 \in M_1 \cap C(X_1 X_2)$. Since M_1 and $C(X_1 X_2)$ admit H , it follows by (4C) and (4.5) that $M_1 \leq C(X_1 X_2)$. If $M_1 = X_a^\gamma$, then $X_a^\gamma X_1 X_2$ is an abelian group. $(X_a^\gamma X_1 X_2)^\alpha = X_1 (X_1 X_2)^\alpha$ is then abelian as well, where $\alpha = \gamma^{-1}$ if $a = 1$, and $\alpha = \omega_1 \gamma$ if $a = -1$. In particular, $(X_1 X_2)^\alpha \leq C(X_1) \cap C(j_1)$. Let $\tilde{K} = O(C(X_1))$, and let \tilde{M} be the S_p -subgroup of \tilde{K} . $C(X_1) = L_2 \tilde{K}$ by (3B). If $g \in (X_1 X_2)^\alpha$, then $g = hk$, where h is a p -element in L_2 and $k \in \tilde{K}$. Since $j_1^{-1} g j_1 = g$, we have

$$h^{-1} j_1^{-1} h j_1 = k j_1^{-1} k^{-1} j_1 \in \tilde{K} \cap L_2 = 1,$$

so that $h \in C(j, j_1) = C(D)$. But $|C(D)|$ is not divisible by p , so that $h = 1$. Thus $(X_1 X_2)^\alpha \leq \tilde{M}$. Define $\tilde{M}_i = \tilde{M} \cap C(j_i)$ for $i = 0, 1, 2$. As in the proof that $|M_1| = |M_2|$, it follows that $|\tilde{M}_1| = |\tilde{M}_2|$. But we have just shown that $\tilde{M}_1 \geq (X_1 X_2)^\alpha$, so that $|X_2 \tilde{M}| \geq q_1^2 q_2^2$. Thus (ii) holds for any $\pi \neq 1$ in X_1 . If $M_1 = X_b^\gamma$, then $X_2 (X_1 X_2)^\beta$ is an abelian group, where $\beta = \gamma^{-1}$ if $b = 2$, $\beta = \omega_2 \gamma$ if $b = -2$. Thus $(X_1 X_2)^\beta \leq C(X_2) \cap C(j_1)$. If $g \in (X_1 X_2)^\beta$, then $g = hk$, where h is a p -element in L_1 and $k \in K$. As before, h must be trivial so that $(X_1 X_2)^\beta \leq K$. Thus $M_1 \geq (X_1 X_2)^\beta$, contradicting the assumption that $|M_1| = q_1$.

A similar argument applies if $z_2 \neq 1$, which completes the proof of (4D). As a corollary of the proof, we have

(4E) Let $q_1 \geq q_2$. One of the following holds:

(i) X_2 is an S_p -subgroup of $K = O(C(X_2))$, $M = X_2$.

(ii) $|M/X_2| = q_1^4$, $q_1 = q_2$, and $c(X_2) \equiv 0 \pmod{q_1^3 q_2^3}$.

(iii) $|M/X_2| = q_1^{3/2}$, $q_1 = q_2^3$, and $c(X_2) \equiv 0 \pmod{q_1^3 q_2^3}$.

(iv) $|M/X_2| = q_1^2$. If (ii) of (4D) fails, then there is an S_p -subgroup P of G containing $X_1 M$, such that $Z(P) \cap X_1 X_2 \neq 1$.

(4F) If $q_1^3 q_2^3$ divides $|G|$, then $c(\pi) \equiv 0 \pmod{q_1^3 q_2^3}$ for some $\pi \neq 1$ in X_1 or X_2 .

Proof. We choose $q_1 \geq q_2$ and let K, M be defined as in (4D), (4E). If (ii) or (iii) of (4E) holds, then we are done. If (iv) of (4E) holds and (4F) fails, then there exists an S_p -subgroup P of G such that $P \geq X_1 M$ and $Z(P) \cap X_1 X_2 \neq 1$. Choose $\pi \neq 1$ in $Z(P) \cap X_1 X_2$, and write $\pi = \pi_1 \pi_2$ with $\pi_i \in X_i$. Since $X_2 \leq Z(M)$, π and π_1 induce the same automorphism on M/X_2 . Since π centralizes M , π_1 acts trivially on M/X_2 so that $\pi_1 = 1$. But then $\pi = \pi_2 \in X_2$ and (4F) holds.

Suppose (i) of (4E) holds and (4F) fails. By (4D) there exists an element $\pi \neq 1$ in $X_1 X_2$ such that $\pi \in Z(P)$ for some S_p -subgroup P of G . Let $\pi = \pi_1 \pi_2$, where $\pi_i \in X_i$. Since we are assuming (4F) fails, $\pi_1 \neq 1$, $\pi_2 \neq 1$. Now $\langle j \rangle$ is an S_2 -subgroup of $C(\pi, j)$ so by (2B), $\langle j \rangle$ is an S_2 -subgroup of $C(\pi)$. Thus $C(\pi) = \langle j \rangle O(C(\pi))$, moreover D normalizes $O(C(\pi))$ since j_1 and j_2 invert π . Let R be an S_p -subgroup of $O(C(\pi))$ admitting D ; by assumption $|R| \geq q_1^3 q_2^3$. On the other hand, the Brauer-Wielandt Theorem shows that $|R| = q_1^3 q_2^3$. If $R_i = R \cap C(j_i)$ for $i = 0, 1, 2$, then $|R_0| = |R_1| = |R_2| = q_1 q_2$. By (4B) $R_0 = X_a X_b$ where $a \in \{1, -1\}$, $b \in \{2, -2\}$. Since $\langle \pi \rangle \leq O(C(\pi))$, π belongs to R_0 . Since the S_p -subgroups of L_1 and L_2 are T.I. sets, it follows that $R_0 = X_1 X_2$. An argument already used several times gives

$$R_1 = (X_a X_b)^c, \quad R_2 = (X_c X_d)^{c^2},$$

where $a, c \in \{1, -1\}$, $b, d \in \{2, -2\}$. Thus R contains the abelian subgroup $\langle \pi \rangle \times (X_c X_d)^{c^2}$ of order greater than $q_1 q_2$. Since X_2 and $X_d^{c^2}$ are conjugate in G , we have that $c(X_2) \equiv 0 \pmod{p q_1 q_2}$, contrary to the assumption that (i) of (4E) holds.

In the next two lemmas we shall assume $|G|$ is divisible by $q_1^3 q_2^3$. By (4F) there exists an element $\pi \neq 1$ in X_1 or X_2 such that $c(\pi) \equiv 0 \pmod{q_1^3 q_2^3}$. Set $\{\alpha, \beta\} = \{1, 2\}$, and choose β to be that subscript such that $\pi \in X_\beta$.

(4G) If $q_1^3 q_2^3$ divides $|G|$, then $q_1^3 q_2^3$ divides $c(X_\beta)$, where β is chosen as above.

Proof. Choose $\pi \neq 1$ in X_β so that $c(\pi) \equiv 0 \pmod{q_1^3 q_2^3}$, and let $M = O(C(\pi))$. Since D normalizes M , we may choose an S_p -subgroup R of M which admits D . By (3C), $C(\pi) = L_\alpha M$ and $L_\alpha \cap M = 1$, so that $|R| \geq q_\alpha^2 q_\beta^3$. We define $R_i = R \cap C(j_i)$ for $i = 0, 1, 2$, and note that $R_0 \leq C(j) \cap M \leq X_\beta$ by (3C) (iii), so that $|R_0| \leq q_\beta$. Since $|R_1|$ and $|R_2|$ are not greater than $q_\alpha q_\beta$, it must be the case that $R_0 = X_\beta$ and $|R_1| = |R_2| = q_\alpha q_\beta$. Moreover, by an earlier argument we may conclude that

$$R_0 = X_\beta, \quad R_1 = (X_a X_b)^\eta, \quad R_2 = (X_c X_d)^\eta,$$

where $a, c \in \{1, -1\}$, $b, d \in \{2, -2\}$. But now H normalizes R_0, R_1 , and R_2 , and so H normalizes $R = R_0 R_1 R_2$ as well. Conjugating the inclusion $\pi \in Z(R) \cap X_\beta$ by H then gives $X_\beta \leq Z(R)$, so that $X_\beta \leq Z(X_\alpha R)$. This completes the proof.

(4H) Suppose the hypothesis of (4G) holds. Let $K = O(C(X_\beta))$, and $P = X_\alpha M$, where M is the S_p -subgroup of K . Then the following hold:

- (i) M/X_β is elementary abelian of order $q_1^2 q_2^2$.
- (ii) With a suitable choice of notation

$$P = (X_\alpha X_\beta) (X_{-\alpha} X_\beta)^\eta (X_\alpha X_\beta)^{\eta^2} \quad \text{or}$$

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

Proof. M/X_β is abelian of order $q_1^2 q_2^2$ by (3B), (4G). Let $M_i = M \cap C(j_i)$ for $i = 0, 1, 2$; we have $M_0 = X_\beta$ and $[M_1, M_2] \leq X_\beta$. Since M_1 and M_2 are elementary abelian, it follows that M/X_β is as well, which proves (i). Now

$$M_1 = (X_\alpha^a X_\beta^b)^\eta, \quad M_2 = (X_\alpha^c X_\beta^d)^{\eta^2},$$

where $a, c \in \{1, \omega_\alpha\}$, $b, d \in \{1, \omega_\beta\}$. Since $X_\beta \leq Z(P)$, we see that $X_\beta^{\eta^{-1}} \leq C(X_\alpha^a)$, $X_\beta^{\eta^{-2}} \leq C(X_\alpha^c)$, so that $\langle X_\beta^{\eta^{-1}a}, X_\beta^{\eta^{-2}c} \rangle \leq C(X_\alpha)$. Suppose $a = c$, so that $\langle X_\beta^{\eta^{-1}a}, X_\beta^{\eta^{-2}c} \rangle = \langle X_\beta^\eta, X_\beta^{\eta^2} \rangle$. Then $\langle X_\beta, X_\beta^\eta, X_\beta^{\eta^2} \rangle \leq C(X_\alpha)$, and so in turn, $\langle X_\alpha, X_\alpha^\eta, X_\alpha^{\eta^2} \rangle \leq C(X_\beta)$. Conjugating this last inclusion by ω_α then gives $\langle X_{-\alpha}, X_{-\alpha}^\eta, X_{-\alpha}^{\eta^2} \rangle \leq C(X_\beta)$. In particular, $\langle X_\alpha, X_{-\alpha} \rangle^\eta \leq C(X_\beta)$, which is impossible since $j_1 \notin C(X_\beta)$. Thus $a \neq c$. By a suitable choice of notation,

we may assume $a = \omega_\alpha$, $c = 1$. Now $\langle X_\beta^{b\eta}, X_\beta^{d\eta^2} \rangle \leq C(X_\beta)$. Conjugating this inclusion by ω_α then gives $\langle X_\beta^{b\eta^2}, X_\beta^{d\eta} \rangle \leq C(X_\beta)$. If $b \neq d$, then $\langle X_\beta, X_{-\beta} \rangle^? \leq C(X_\beta)$; which is again impossible since $j_1 \notin C(X_\beta)$. Thus $b = d$, and the proof of (4H) is complete.

§5. We shall prove in this section that $q_1^3 q_2^3$ divides $|G|$ if it is not the case that $q_1 = q_2 \leq 11$. Set $E = \langle n, j \rangle$. By the final remark of §2, $C(E) = \langle \sigma_1, \sigma_2, x, n \rangle$, which has the normal abelian 2-complement $\langle \sigma_1^2, \sigma_2^2 \rangle$. Set

$$V = \langle \sigma_1^2, \sigma_2^2 \rangle, \quad V_1 = \langle \sigma_1^2 \rangle, \quad V_2 = \langle \sigma_2^2 \rangle.$$

Since $N(E)/C(E)$ is isomorphic to S_3 by (3A), there exists an element ζ of order a power of 3 in $N(E)$ permuting n, nj, j cyclically. By (1.9) the elements $\tau_1, \tau_2 \in N(E)$, and indeed, τ_1 inverts V_1 and centralizes V_2 , τ_2 inverts V_2 and centralizes V_1 . Since $x = \tau_1 \tau_2$, x inverts V . Thus

$$(5.1) \quad N(E) = \langle V \times E, \tau_1, \tau_2, \zeta \rangle.$$

Let \hat{V} be the character group of V . We define the following subsets of \hat{V} :

$$\begin{aligned} \hat{V}_1 &= \{ \lambda \in \hat{V} : \lambda|_{V_2} = 1 \}, \\ \hat{V}_2 &= \{ \lambda \in \hat{V} : \lambda|_{V_1} = 1 \}, \\ \hat{M} &= \hat{V} - \hat{V}_1 - \hat{V}_2, \\ \hat{N} &= \hat{V}_1 \cup \hat{V}_2 - \{1\}, \end{aligned}$$

where 1 stands for the trivial character of V . The union $\hat{V} = \hat{M} \cup \hat{N} \cup \{1\}$ is disjoint, and

$$(5.2) \quad \begin{aligned} |\hat{M}| &= v_1 v_2 - v_1 - v_2 + 1 = (v_1 - 1)(v_2 - 1), \\ |\hat{N}| &= (v_1 - 1) + (v_2 - 1), \end{aligned}$$

where $q_i + \varepsilon = 2v_i$. An element h of $N(E)$ induces an action on \hat{V} by the equation $\lambda^h(g^h) = \lambda(g)$, $g \in V$.

(5A) Suppose there exists an orbit of length 3 in \hat{V} under the action of ζ contained in \hat{M} . Then $|G|$ is divisible by $q_1^3 q_2^3$.

Proof. If λ is a character in this orbit, then the hypothesis implies that the orbit of λ under $N(E)$ has 12 distinct characters. As a character of VE/E , λ induces a character λ^* of $C(E)/E$ of degree 2 with 6 conjugates

in $N(E)/E$, which by [1] corresponds to a block B of G with defect group E . In $N(E) \cap C(j)$ these conjugates form 3 orbits of 2 characters each, which then correspond to blocks B_1, B_2, B_3 of $C(j)$ with E as defect group, and by [5], $B_i^c = B$ for $i = 1, 2, 3$. It is easily seen from the structure of $C(j)$ that each B_i has four irreducible characters of degree $(q_1 - \varepsilon)(q_2 - \varepsilon)$. Since $n \sim nj$ in $C(j)$, there exist blocks b_{i1}, b_{i2} of $C(n, j) = C(E)$ such that $b_{i1}^{c_{i1}^{(j)}} = b_{i2}^{c_{i2}^{(j)}} = B_i$. In particular, B_i has one column of decomposition numbers from each of the sections of $C(j)$ represented by 1 and j , and two columns from the section of n . The degrees of the corresponding modular characters are $(q_1 - \varepsilon)(q_2 - \varepsilon), (q_1 - \varepsilon)(q_2 - \varepsilon), 2, 2$ respectively. B itself has one column from the section of 1, and 3 columns from the section of j . The corresponding degrees are $f, (q_1 - \varepsilon)(q_2 - \varepsilon), (q_1 - \varepsilon)(q_2 - \varepsilon), (q_1 - \varepsilon)(q_2 - \varepsilon)$, where f is an integer. We can assume that the matrices of decomposition numbers for B_i, B are

1	j	n		1	j		
1	1	1	δ_i	1	1	1	δ
1	1	-1	$-\delta_i$	1	1	-1	$-\delta$
1	-1	1	$-\delta_i$	1	-1	1	$-\delta$
1	-1	-1	δ_i	1	-1	-1	δ

where $\delta = \pm 1, \delta_i = \pm 1, i = 1, 2, 3$.

Apply now the formula of [2] III (2A) to the groups G and $C(j)$ with $\pi = y_1 = y_2 = j$ and the column of decomposition numbers of the modular character of $C(j)$ in B_i . A computation then gives

$$|G| = (q_1 q_2)^3 (q_1 + \varepsilon)(q_2 + \varepsilon)f.$$

Thus $q_1^3 q_2^3$ divides $|G|$.

(5B) Let $\{\alpha, \beta\} = \{1, 2\}$. Suppose $V_\beta \neq 1$ and ζ centralizes V_β . Then $q_\alpha \leq 7$.

Proof. As in the proof of (3F), we can verify that the conditions of (3E) are satisfied in $X = C(V_\beta)/V_\beta$. The corresponding Z and L are V_β/V_β and $L_\alpha V_\beta/V_\beta$ respectively, and so $q_\alpha \leq 7$.

(5C) $|G|$ is divisible by $(q_1 q_2)^3$ unless one of the following cases holds:

- (i) $q_1 = q_2 = 11$.
- (ii) $q_1 = q_2 = 9$.

(iii) $\min\{q_1, q_2\} = 3, 5$ or 7 .

Proof. If $V_1 = V_2 = 1$, then necessarily $q_1 = q_2 = 3$, a case contained in (iii). If $V \neq 1$, and ζ centralizes V , then necessarily V_1 or V_2 is non-trivial, and the result is implied by (5B). Thus we may suppose that $V \neq 1$, and moreover, ζ does not centralize V . In particular, ζ does not centralize \hat{V} . If ζ has an orbit of length 3 in \hat{V} contained in \hat{M} , then $(q_1 q_2)^3$ divides $|G|$ by (5A). Thus we may suppose that no orbit of length 3 of ζ in \hat{V} is contained in \hat{M} .

Let r be the number of characters in \hat{M} fixed by ζ . The remaining $(v_1 - 1)(v_2 - 1) - r$ characters in \hat{M} then belong to s orbits of ζ which meet \hat{N} . Let t be the number of orbits of length 3 of ζ contained in \hat{N} , and let w be the number of characters in \hat{N} fixed by ζ . The fixed-points of ζ in \hat{V} form a subgroup $\hat{W} < \hat{V}$ of order $1 + r + w$. Since there are a total of $s + t$ orbits of ζ of length 3 in \hat{V} , we have

$$(5.3) \quad |\hat{W}| = |\hat{V}| - 3(s + t).$$

Moreover, each such orbit contains one or more characters in \hat{N} , so by

$$(5.2)$$

$$(5.4) \quad s + t \leq v_1 + v_2 - 2$$

$|\hat{W}|$ divides $|\hat{V}| - |\hat{W}|$, and since $|\hat{V}|$ and $|\hat{W}|$ are odd, it follows that $2|\hat{W}|$ divides $|\hat{V}| - |\hat{W}|$. This together with (5.3) then gives

$$(5.5) \quad 3(s + t) \equiv 0 \pmod{2|\hat{W}|}.$$

In particular, $|\hat{W}| \leq \frac{3}{2}(s + t)$, and so $|\hat{V}| \leq \frac{9}{2}(s + t)$ by (5.3). Using (5.4), we then obtain the inequality

$$(5.6) \quad 2v_1 v_2 \leq 9(v_1 + v_2 - 2).$$

Suppose $v_1 > 5$ and $v_2 > 5$. (5.6) then implies that $v_1 \leq 9$, $v_2 \leq 9$. If $v_1 = v_2 = 9$, then $s + t \leq 16$ by (5.4). But (5.3) and (5.5) cannot simultaneously be satisfied. If $v_1 = v_2 = 7$, then $s + t \leq 12$ by (5.4), and $s + t = 12$ must be the case; otherwise $2|\hat{W}| > 3(s + t)$. But if $s + t = 12$, then $2|\hat{W}| = 26$, which does not divide 36. If $\{v_1, v_2\} = \{7, 9\}$, then (3K) would be contradicted. By a relabeling of indices, we may thus assume $v_2 \leq 5$. If $v_2 = 5$, then $v_1 \leq 27$ by (5.6), and (2A), (3K) then imply that $q_1 = q_2 = 9$ or $q_1 = q_2 = 11$. If $v_2 < 5$, then $q_2 \leq 7$. This completes the proof of (5C).

(5D) Suppose $\min\{q_1, q_2\} \leq 7$. If $q_1 \neq q_2$, then $|G|$ is divisible by $(q_1q_2)^3$.

Proof. We choose notation so that $q_1 > q_2 = p$, where p is 3, 5 or 7. If $p = 3$, let R be the subgroup of L_1 given by (3F); if $p = 5$ or 7, so that $v_2 = 3$, let $R = (V_1)^3$. The proof of (3F) shows that in every case, $|C(R)|$ is divisible by p^3 . Let P then be an S_p -subgroup of $C(R)$ containing X_2 , so that $Z(P) \leq C(X_2)$. Since $C(X_2) = L_1K$, where $K = O(C(X_2))$, any element π in $Z(P)$ may be written in the form $\pi = cd$, where c is a p -element in L_1 and $d \in K$. Now $P \leq C(R)$ and so $[\pi, R] = 1$. On the other hand $[\pi, R] \equiv [c, R] \pmod{K}$. Thus $[c, R] \leq L_1 \cap K = 1$, and indeed, $c = 1$ since c is a p -element. We have thus shown that $Z(P) \leq M$, where M is the S_p -subgroup of K . If $Z(P) \cap X_2 = 1$, then certainly $M > X_2$, and R has non-trivial fixed-points on M/X_2 . If $Z(P) \cap X_2 > 1$, then $X_2 \leq Z(P)$ since X_2 has prime order. In this case, $P \leq C(X_2)$, and the above argument showing that $Z(P) \leq M$ can be applied to yield $P \leq M$. Again $M > X_2$, and R has non-trivial fixed-points on M/X_2 . Thus (ii), (iii) or (iv) of (4E) must hold. (iv) is impossible by the proof of (1E) and the fact that R has fixed-points on M/X_2 , and so $(q_1q_2)^3$ divides $|G|$.

§6. We assume from now on that $|G|$ is divisible by $(q_1q_2)^3$. Choosing notation as specified in (4G), we have the two cases

$$(6.1) \quad \begin{aligned} \text{Case A: } & P = (X_\alpha X_\beta)(X_{-\alpha} X_\beta)^\eta (X_\alpha X_\beta)^{\eta^2}. \\ \text{Case B: } & P = (X_\alpha X_\beta)(X_{-\alpha} X_{-\beta})^\eta (X_\alpha X_{-\beta})^{\eta^2}. \end{aligned}$$

$$(6A) \quad P \cap P^{\sigma_1 \sigma_2} = 1.$$

Proof. Let $P^- = P^{\sigma_1 \sigma_2}$. Since H normalizes P and P^- , it follows that H , and in particular D , normalizes $P \cap P^-$. Since $P \cap P^- \cap C(j_i) = 1$ for $i = 0, 1, 2$, it follows by the Brauer-Wielandt Theorem that $P \cap P^- = 1$.

For each w in $W = N(H)/H_t$, let $\omega(w)$ be a coset representative of w in $N(H)$. We define the subgroups

$$(6.2) \quad \begin{aligned} P'_w &= P \cap \omega(w)^{-1} P \omega(w), \\ P''_w &= P \cap \omega(w)^{-1} P^- \omega(w). \end{aligned}$$

Clearly P'_w and P''_w are well-defined and admit H . If $r \in N(H)$ and $w = Hr$, we shall occasionally write P'_r, P''_r in place of P'_w, P''_w . We shall call a

subgroup of the form $X_\gamma^{\eta^i}$, $\gamma \in \{\pm 1, \pm 2\}$, $i = 0, 1, 2$, appearing in (6. 1) a root subgroup of P .

(6B) Let $w \in W$. Each root subgroup of P is contained in P'_w or P''_w . P'_w, P''_w are the products of the root subgroups of P contained in them, the root subgroups being ordered from left to right in the order they appear in (6. 1). $P = P'_w P''_w = P''_w P'_w$, and $P'_w \cap P''_w = 1$.

Proof. It is clear from (6. 2) that each root subgroup of P is in P'_w or P''_w . Moreover, $P'_w \cap P''_w = 1$ by (6A). Since P'_w and P''_w admit D , P'_w and P''_w can be factored as required by the Brauer-Wielandt Theorem. Finally, $|P'_w| \cdot |P''_w| = (q_1 q_2)^3$, so that $P = P'_w P''_w = P''_w P'_w$.

(6C) With suitable notation, case B of (6. 1) holds.

Proof. Suppose case A of (6. 1) holds, so that

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

Since $[X_\alpha^{\eta^2}, X_\beta] = 1$, we have $[X_\alpha, X_\beta^\eta] = 1$ by conjugating by η . Conjugating the last relation by ω_β , we have as well $[X_\alpha, X_\beta^{\eta^2}] = 1$. Now $P''_w = X_\alpha X_{-\alpha}^\eta X_\alpha^{\eta^2}$, where $\omega(w) \equiv \omega_\alpha \eta^2 \pmod{H}$, so in particular

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

Thus $[X_{-\alpha}^\eta, X_\alpha^{\eta^2}] = 1$, from which we conclude that $[X_{-\alpha}^{\eta^2}, X_\alpha] = 1$ by conjugating by η . Conjugating the latter by ω_β gives $[X_{-\alpha}^\eta, X_\alpha] = 1$ as well. We have thus shown that

$$\langle X_\beta, X_\beta^\eta, X_{-\beta}^{\eta^2}, X_{-\alpha}^{\eta^2}, X_{-\alpha}^\eta \rangle \leq C(X_\alpha).$$

Let g be any element in $X_\beta^\eta, X_{-\beta}^{\eta^2}, X_{-\alpha}^{\eta^2}$, or $X_{-\alpha}^\eta$. If $\tilde{K} = 0(C(X_\alpha))$, then $C(X_\alpha) = L_\beta \tilde{K}$ by (3B), so we may express $g = cd$, where c is a p -element in L_β and $d \in \tilde{K}$. Let $j_i, i = 1$ or 2 , be the involution in D commuting with g . Since D normalizes \tilde{K} , it follows that $[j_i, c] \in \tilde{K}$. On the other hand, D normalizes L_β , and so $[j_i, c] \in L_\beta$. Thus $[j_i, c] = 1$, since $L_\beta \cap \tilde{K} = 1$. The element c then centralizes $D = \langle j, j_i \rangle$, which implies that $c = 1$. We have now shown that

$$\langle X_\beta^\eta, X_{-\alpha}^\eta, X_{-\beta}^{\eta^2}, X_{-\alpha}^{\eta^2} \rangle \leq \tilde{M},$$

where \tilde{M} is the S_p -subgroup of \tilde{K} . If $\tilde{M}_i = \tilde{M} \cap C(j_i)$ for $i = 0, 1, 2$, then

$$\tilde{M}_0 \geq X_\alpha, \tilde{M}_1 \geq \langle X_\beta, X_{-\alpha} \rangle^\eta, \tilde{M}_2 \geq \langle X_{-\beta}, X_{-\alpha} \rangle^{\eta^2}$$

and necessarily these inclusions are equalities by the Brauer-Wielandt Theorem. If we define $\tilde{P} = X_\beta \tilde{M}$, then $|\tilde{P}| = (q_1 q_2)^3$ and $X_\alpha \leq Z(\tilde{P})$. Replacing X_α by $X_{-\alpha}$ and \tilde{P} by $\tilde{P}^{\omega_\alpha}$ then gives case B for \tilde{P} in $C(X_\alpha)$.

We may henceforth assume that case B in (6.1) holds. The following table gives the factorization of P''_w for $w \in W$ in this case.

	$\omega(w)$	P''_w
	1	1
	ω_α	X_α
	$\omega_\beta \eta^2$	$X_{-\beta}^\eta$
	$\omega_\alpha \omega_\beta \eta$	$X_\alpha X_{-\beta}^{\eta^2}$
	$\omega_\alpha \omega_\beta \eta^2$	$X_{-\beta}^\eta X_\alpha^{\eta^2}$
(6.3)	$\omega_\alpha \eta$	$X_\beta X_{-\beta}^\eta X_\alpha^{\eta^2}$
	$\omega_\beta \eta$	$X_\alpha X_{-\alpha}^\eta X_{-\beta}^{\eta^2}$
	η	$X_\beta X_{-\alpha}^\eta X_{-\beta}^\eta X_\alpha^{\eta^2}$
	η^2	$X_\alpha X_\beta X_{-\alpha}^\eta X_{-\beta}^{\eta^2}$
	$\omega_\alpha \eta^2$	$X_\alpha X_\beta X_{-\alpha}^\eta X_\alpha^{\eta^2} X_{-\beta}^{\eta^2}$
	ω_β	$X_\beta X_{-\alpha}^\eta X_{-\beta}^\eta X_\alpha^{\eta^2} X_{-\beta}^{\eta^2}$
	$\omega_\alpha \omega_\beta$	P

We define the subgroup $B = HF$. Since $H \leq N(P)$ and $H \cap P = 1$, the order of B is $(q_1 - 1)(q_2 - 1)q_1^3 q_2^3$.

(6D) For $w \in W$, $|B\omega(w)B| = |B| |P''_w|$.

Proof. By the definition of B and (6B) we have $B\omega(w)B = B\omega(w)HP'_w P''_w$. Since the transform of HP'_w by $\omega(w)^{-1}$ is contained in B , it follows that $B\omega(w)B = B\omega(w)P''_w$. Now suppose $b\omega(w)u = b_1\omega(w)u_1$ for elements $b, b_1 \in B$ and $u, u_1 \in P''_w$. Then $b_1^{-1}b = \omega(w)u_1 u^{-1} \omega(w)^{-1}$. Since $b_1^{-1}b$ is a p -element of B and $P \triangleleft B$, it follows that $b_1^{-1}b \in P$. On the other hand, $\omega(w)u_1 u^{-1} \omega(w)^{-1} \in \omega(w)P''_w \omega(w)^{-1} \leq P^-$. Thus $b_1^{-1}b \in P \cap P^- = 1$, and so $b_1 = b, u_1 = u$. This completes the proof.

(6E) Let $r \in \{\omega_\alpha, \omega_\beta \eta^2\}$, and $w \in W$. Then

- (i) $rB\omega(w) \subseteq B\omega(w)B \cup Br\omega(w)B,$
- (ii) $\omega(w)Br \subseteq B\omega(w)B \cup B\omega(w)rB.$

Proof. It suffices to prove (i), since (ii) follows from (i) by taking inverses of the subsets in question. Now $rB\omega(w) = rHP\omega(w) = HrP_r'R_r''\omega(w) \subseteq BrP_r''\omega(w)$. If $(P_r'')^{\omega(w)} \leq P$, then $BrP_r''\omega(w) \subseteq Br\omega(w)B$ and (i) holds. Assume then that $(P_r'')^{\omega(w)} \leq P^-$. Since $P_r'' = X_\alpha$ if $r = \omega_\alpha$ and $P_r'' = X_{-\beta}^{\eta}$ if $r = \omega_\beta\eta^2$, it easily follows that $(P_r'')^{r\omega(w)} \leq P$. But now $BrP_r''\omega(w) = BrP_r''r^{-1} \cdot r\omega(w)$, and so it will be sufficient to show that $rP_r''r^{-1} \subseteq BrP_r''$. This, however, is a consequence of the corresponding double coset decomposition in the groups $SL(2, q_1)$ and $SL(2, q_2)$.

(6F) Let $\tilde{G} = BN(H)B$. Then \tilde{G} is a subgroup of G of order $(q_1q_2)^3(q_1^2 - 1)(q_2^2 - 1)(1 + q_1q_2 + q_1^2q_2^2)$. \tilde{G} is the disjoint union of double cosets $B\omega(w)B$, where $w \in W$.

Proof. \tilde{G} is closed under group multiplication by (6E), so \tilde{G} is a subgroup of G . We claim that $B \cap N(H) = H$. Since $H \leq B \cap N(H)$ and $B = HP$, it follows that if $B \cap N(H) > H$, then there exists an element $\pi \neq 1$ in P such that $\pi \in B \cap N(H)$. But then $[\pi, H] \leq P \cap H = 1$, so that $\pi \in C(H) \leq C(D)$, which is impossible by (4. 1). This together with the preceding facts is enough to show that \tilde{G} is the disjoint union of the double cosets $B\omega(w)B$ with $w \in W$, (see [8]). The order of \tilde{G} then is immediate from (6D) and (6. 3).

§7. We continue with the notation of §6.

(7A) Let D normalize the p -subgroup A of G , and define $A_i = A \cap C(j_i)$ for $i = 0, 1, 2$. If $A_i \leq Z(A)$ for some i in $\{0, 1, 2\}$, then $[A_{i-1}, A_{i+1}] \leq A_i$, where the indices are reduced modulo 3.

Proof. This is a restatement of [3] II (7E).

(7B) The root subgroups of P contained in M satisfy the following commutator relations:

- (i) $[X_\alpha^\eta, X_\alpha^{\eta^2}] = 1$ or X_β , $[X_{-\beta}^\eta, X_{-\beta}^{\eta^2}] = X_\beta$.
- (ii) All other commutator relations between root subgroups in M are trivial.

Proof. We have $[X_{-\beta}^\eta, X_\alpha^{\eta^2}] = [X_\beta, X_\alpha^{\eta^2}]^{\omega_\beta \eta} = 1$, and $[X_{-\beta}^{\eta^2}, X_{-\alpha}^\eta] = [X_\beta, X_{-\alpha}^\eta]^{\omega_\beta \eta^2} = 1$. The remaining commutator relations between root subgroups in M not of type (i) are clearly trivial, so (ii) is proved. Since H is transitive on the non-identity elements of X_β , it will be sufficient to show $[X_{-\beta}^\eta, X_{-\beta}^{\eta^2}] \neq 1$ in order to prove (i). But if $[X_{-\beta}^\eta, X_{-\beta}^{\eta^2}] = 1$, then $[X_\beta, X_\beta^{\eta^2}] = [X_{-\beta}^\eta, X_{-\beta}^{\eta^2}]^{\omega_\beta \eta} = 1$, so that $\langle X_\beta, X_{-\beta} \rangle^{\eta^2} \leq C(X_\beta)$. This is impossible since $j_2 \notin C(X_\beta)$.

(7C) X_α stabilizes the following chain of subgroups:

$$P \triangleright X_{-\beta}^\eta X_\alpha^{\eta^2} X_{-\alpha}^\eta X_{-\beta}^{\eta^2} X_\beta \triangleright X_\alpha^{\eta^2} X_{-\alpha}^\eta X_{-\beta}^{\eta^2} X_\beta \triangleright X_{-\alpha}^\eta X_{-\beta}^{\eta^2} X_\beta \triangleright X_{-\beta}^{\eta^2} X_\beta \triangleright X_\beta \triangleright 1.$$

Proof. The second term of this chain is M , which is normal in P . Since M/X_β is abelian, the remaining terms are clearly normal in their predecessor. The chain is then a normal one. Now $[X_\alpha^{\eta^2}, X_\beta] = 1$; conjugating this by $\omega_\beta \eta^2$ gives $[X_\alpha, X_{-\beta}^{\eta^2}] = 1$. Thus X_α even centralizes $X_{-\beta}^{\eta^2} X_\beta$. The complex $X_\alpha X_{-\alpha}^\eta X_{-\beta}^{\eta^2} X_\beta$ is a subgroup by (6. 3) and the factor group $X_\alpha X_{-\alpha}^\eta X_{-\beta}^{\eta^2} X_\beta / X_\beta$ admits D . Since $X_{-\beta}^{\eta^2} X_\beta / X_\beta$ is central in this factor group, we have by (7A) that $[X_\alpha, X_{-\alpha}^\eta] \leq X_{-\beta}^{\eta^2} X_\beta$, so that $[X_\alpha, X_{-\alpha}^\eta X_{-\beta}^{\eta^2} X_\beta] \leq X_{-\beta}^{\eta^2} X_\beta$. $X_\alpha X_\alpha^{\eta^2} X_{-\alpha}^\eta X_{-\beta}^{\eta^2} X_\beta$ is a subgroup by (6. 3) and the factor group of this by $X_{-\beta}^{\eta^2} X_\beta$ admits D . Since $[X_\alpha^{\eta^2}, X_{-\alpha}^\eta] \leq X_\beta$ and $[X_\alpha, X_{-\alpha}^\eta] \leq X_{-\beta}^{\eta^2} X_\beta$, (7A) implies that $[X_\alpha, X_\alpha^{\eta^2}] \leq X_{-\alpha}^\eta X_{-\beta}^{\eta^2} X_\beta$ so that $[X_\alpha, X_\alpha^{\eta^2} X_{-\alpha}^\eta X_{-\beta}^{\eta^2} X_\beta] \leq X_{-\alpha}^\eta X_{-\beta}^{\eta^2} X_\beta$. Finally, $P / X_{-\alpha}^\eta X_{-\beta}^{\eta^2} X_\beta$ admits D , and the image of $X_\alpha^{\eta^2}$ in this factor group is central. A third application of (7A) gives $[X_\alpha, X_{-\beta}^{\eta^2}] \leq X_\alpha^{\eta^2} X_{-\alpha}^\eta X_{-\beta}^{\eta^2} X_\beta$, which completes the proof.

We construct one other subgroup \hat{G} of G along lines similar to those for \tilde{G} . Define then

$$\hat{P} = X_\beta X_{-\beta}^\eta X_{-\beta}^{\eta^2}, \quad \hat{N} = \langle H, \omega_\beta, \eta \rangle, \quad \hat{W} = \hat{N} / H.$$

We note that H normalizes the subgroup \hat{P} and that $\hat{P} \cap \hat{P}^{\omega_\beta} = 1$. For each $w \in \hat{W}$, let

$$\begin{aligned} \hat{P}'_w &= \hat{P} \cap \omega(w)^{-1} \hat{P} \omega(w), \\ \hat{P}''_w &= \hat{P} \cap \omega(w)^{-1} \hat{P}^{\omega_\beta} \omega(w). \end{aligned}$$

\hat{P}'_w, \hat{P}''_w are well-defined subgroups of \hat{P} , and each root subgroup of P contained in \hat{P} is either in \hat{P}'_w or \hat{P}''_w . Moreover, $\hat{P}'_w \hat{P}''_w = \hat{P}''_w \hat{P}'_w$. The following table gives the factorization of \hat{P}''_w .

$$(7.1) \quad \begin{array}{ll} \omega(w) & \hat{P}''_w \\ 1 & 1 \\ \omega_\beta\eta & X_{-\beta}^{\eta^2} \\ \omega_\beta\eta^2 & X_{-\beta}^\eta \\ \eta & X_\beta X_{-\beta}^\eta \\ \eta^2 & X_\beta X_{-\beta}^{\eta^2} \\ \omega_\beta & \hat{P} \end{array}$$

Finally, define $\hat{B} = H\hat{P}$. \hat{B} is a subgroup of order $(q_1 - 1)(q_2 - 1)q_\beta^3$. The next three lemmas are the analogues of (6D), (6E), (6F), and are proved in much the same way.

(7D) $|\hat{B}\omega(w)\hat{B}| = |\hat{B}| |\hat{P}''_w|$ for $w \in \hat{W}$.

(7E) Let $r \in \{\omega_\beta\eta, \omega_\beta\eta^2\}$, and let $w \in \hat{W}$. Then

(i) $r\hat{B}\omega(w) \subseteq \hat{B}\omega(w)\hat{B} \cup \hat{B}r\omega(w)\hat{B}$.

(ii) $\omega(w)\hat{B}r \subseteq \hat{B}\omega(w)\hat{B} \cup \hat{B}\omega(w)r\hat{B}$.

(7F) Let $\hat{G} = \hat{B}\hat{N}\hat{B}$. Then \hat{G} is a subgroup of G of order $q_\beta^3(q_\beta^3 - 1)(q_\beta + 1)(q_\alpha - 1)$. \hat{G} is the disjoint union of double cosets $\hat{B}\omega(w)\hat{B}$, where $w \in \hat{W}$.

(7G) Let $\hat{C}(j) = \hat{G} \cap C(j)$. Then $\hat{C}(j) = L_\beta H$.

Proof. The inclusion $\hat{C}(j) \supseteq L_\beta H$ is clear. Suppose there exists an element c in $\hat{C}(j)$ not in $L_\beta H$. Since $C(j) = L_1 L_2 H$ and $L_\alpha = X_\alpha H_\alpha \cup X_\alpha H_\alpha \omega_\alpha X_\alpha$, we may express $c = uv$, where $u \in L_\beta H$, $v \in X_\alpha$ or $X_\alpha H_\alpha \omega_\alpha X_\alpha$, and $v \neq 1$. If $v \in X_\alpha$, then $v = u^{-1}c \in \hat{G} \cap X_\alpha$. Since $P \cap \hat{G} = \hat{P}$ is an S_p -subgroup of \hat{G} and $P \geq \langle \hat{P}, X_\alpha \rangle$, this is impossible. If $v \in X_\alpha H_\alpha \omega_\alpha X_\alpha$, then $v = u^{-1}c \in \hat{G} \cap B\omega_\alpha B$. By (6F) and (7F) we see that $\hat{G} \cap B\omega_\alpha B = \phi$. Thus $\hat{C}(j) = L_\beta H$.

Now $[X_\beta, X_{-\beta}^\eta] = 1$ and $[X_\beta, X_{-\beta}^{\eta^2}] = 1$. If we conjugate these relations by η and $\omega_\beta\eta$ respectively, we then have $[X_\beta^\eta, X_{-\beta}^{\eta^2}] = 1$ and $[X_{-\beta}^\eta, X_\beta^{\eta^2}] = 1$. The subgroups

$$(7.2) \quad U = X_\beta^\eta X_{-\beta}^{\eta^2}, \quad U^* = X_{-\beta}^\eta X_\beta^{\eta^2}$$

are thus abelian of order q_β^2 .

(7H) Let U, U^* be defined as in (7.2). Then the following hold:

- (I) $\hat{G} \geq \langle D, \eta \rangle$.
- (II) $|U| = |U^*| = q_\beta^2$; U and U^* are normalized by $\hat{C}(j)$;
 $U \cap U^* = U \cap \hat{C}(j) = U^* \cap \hat{C}(j) = 1$.
- (III) All involutions in $\hat{C}(j)$ different from j are conjugate in $\hat{C}(j)$.
- (IV) $[\hat{G}: U\hat{C}(j)] \leq q_\beta^2 + q_\beta + 1$.
- (V) Every class of $\hat{C}(j)$ -conjugate elements of U meets $\hat{C}(j_i) = C(j_i) \cap \hat{G}$.

Proof. (I) is obvious. By definition $|U| = |U^*| = q_\beta^2$. Now $[X_{-\beta}^\eta, X_{-\beta}^{\eta^2}] = X_\beta$; conjugating this by $\omega_\beta \eta^2$ then gives $[X_\beta^\eta, X_\beta] = X_{-\beta}^{\eta^2}$, which implies that $X_\beta \leq N(U)$. Since $\omega_\beta \in N(U)$ as well, it now follows that $L_\beta \leq N(U)$, and so $\hat{C}(j) = L_\beta H \leq N(U)$ by (7G). Since $\omega_\alpha \omega_\beta$ normalizes $\hat{C}(j) = L_\beta H$ and transforms U onto U^* , we have $\hat{C}(j) \leq N(U^*)$ as well. U and U^* are inverted by j , so necessarily $\hat{C}(j) \cap U = \hat{C}(j) \cap U^* = 1$. To complete the proof of (II), we note that $U \cap U^*$ admits D , $U \cap U^* \cap C(j_i) = 1$ for $i = 0, 1, 2$, and apply the Brauer-Wielandt Theorem. (IV) holds since $[\hat{G}: U\hat{C}(j)] = q_\beta^2 + q_\beta + 1$.

The group $\hat{C}(j) = L_\beta H$ can be described in the following manner. Let F_q be a Galois field containing both F_{q_1} and F_{q_2} as subfields. Since $q_1 - 1, q_2 - 1$ are divisible by the same powers of 2, we may choose an element δ in $F_{q_1} \cap F_{q_2}$ of order a power of 2 such that δ is a non-square in F_{q_1} and in F_{q_2} . If $\delta_1 = \delta_2 = \delta$ in the notation of the beginning of §3, then h_0 acts on L_β as $\begin{pmatrix} 1 & \\ & \delta \end{pmatrix}$, and $h_0^2 = h_1(\delta^{-1})h_2(\delta^{-1})$. Let $SL(2, q_\beta)$ be embedded in the natural way in $GL(2, q)$, and let Z be the subgroup of $GL(2, q)$ defined by

$$Z = \left\{ \begin{pmatrix} \mu & \\ & \mu \end{pmatrix}; \mu \in F_{q_\alpha}, \mu \neq 0 \right\}.$$

If ϕ is the inverse of the isomorphism ϕ_β of $SL(2, q_\beta)$ onto L_β , then ϕ can be extended to an isomorphism ψ from $L_\beta H_\alpha$ onto $SL(2, q_\beta)Z$ by defining

$$\psi: h_\alpha(v^{-1}) \rightarrow \begin{pmatrix} v & \\ & v \end{pmatrix}.$$

That ψ is an isomorphism follows from the relations $[L_\beta, H_\alpha] = 1, L_\beta \cap H_\alpha = \langle j \rangle$. Finally, ψ can be extended to an isomorphism Ψ from $L_\beta H$ onto $\langle SL(2, q_\beta), Z, \begin{pmatrix} 1 & \\ & \delta \end{pmatrix} \rangle$ by defining

$$\Psi: h_0 \rightarrow \begin{pmatrix} 1 & \\ & \delta \end{pmatrix}.$$

That ψ is an isomorphism follows from the fact that h_0 acts on L_β as $\begin{pmatrix} 1 & \\ & \delta \end{pmatrix}$, and that

$$h_0^2 = h_1(\delta^{-1})h_2(\delta^{-1}), \begin{pmatrix} 1 & \\ & \delta_2 \end{pmatrix} = \begin{pmatrix} \delta^{-1} & \\ & \delta \end{pmatrix} \begin{pmatrix} \delta & \\ & \delta \end{pmatrix}.$$

Suppose a, c are matrices in $\langle SL(2, q_\beta), \begin{pmatrix} 1 & \\ & \delta \end{pmatrix} \rangle$ and Z respectively such that $(ac)^2 = \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}$. Since $(ac)^2 = a^2c^2$, it follows that

$$c^2 = a^{-2} \in Z \cap \langle SL(2, q_\beta), \begin{pmatrix} 1 & \\ & \delta \end{pmatrix} \rangle.$$

But the intersection $Z \cap \langle SL(2, q_\beta), \begin{pmatrix} 1 & \\ & \delta \end{pmatrix} \rangle$ is easily seen to be

$$\left\{ \begin{pmatrix} \gamma & \\ & \gamma \end{pmatrix} : \gamma \text{ in } \langle \delta \rangle \right\}.$$

Thus c must be of the form $\begin{pmatrix} \mu & \\ & \mu \end{pmatrix}$, where $\mu \in \langle \delta \rangle$. Since $\begin{pmatrix} \mu & \\ & \mu \end{pmatrix} = \begin{pmatrix} \mu & \\ & \mu^{-1} \end{pmatrix} \begin{pmatrix} 1 & \\ & \mu^2 \end{pmatrix}$, we see that $ac \in \langle SL(2, q_\beta), \begin{pmatrix} 1 & \\ & \delta \end{pmatrix} \rangle$. The normal subgroup $L_\beta \langle h_0 \rangle$ of $L_\beta H$ then contains all involutions of $L_\beta H$.

To prove (III) it will be sufficient to show that all involutions in $\langle SL(2, q_\beta), \begin{pmatrix} 1 & \\ & \delta \end{pmatrix} \rangle$ other than $\begin{pmatrix} -1 & \\ & -1 \end{pmatrix}$ are conjugate in $\langle SL(2, q_\beta), \begin{pmatrix} 1 & \\ & \delta \end{pmatrix}, Z \rangle$ to $\begin{pmatrix} 1 & \\ & -1 \end{pmatrix}$. If i is such an involution, then $i^g = \begin{pmatrix} 1 & \\ & -1 \end{pmatrix}$ for some $g \in GL(2, q_\beta)$. Now we can express $g = cd$, where $c \in SL(2, q_\beta)$ and d is a diagonal matrix, so that $i^c = \begin{pmatrix} 1 & \\ & -1 \end{pmatrix}^{d^{-1}} = \begin{pmatrix} 1 & \\ & -1 \end{pmatrix}$. Finally, U admits $L_\beta H$ and j inverts U . It is a easy consequence of the proof of (1E) that L_β is even transitive on $U - \{1\}$ so that (V) holds. This completes the proof of (7H).

By (7H) and [3], I, there exists a Desarguesian plane π whose points and lines are in 1-1 correspondence with subsets of \hat{G} of the form $g^{-1}jUg$ and $g^{-1}jU^*g$, $g \in \hat{G}$. Moreover, there exists a homomorphism f of \hat{G} into $\text{coll}(\pi)$, the group of collineations of π , such that $f(\hat{G})$ contains the projective group $PSL(3, q_\beta)$. Thus we have a normal series

$$(7.3) \quad \hat{G} \triangleright \hat{G}_0 \triangleright K \triangleright 1,$$

where K is the kernel of f , $|K|$ is odd, \hat{G}/\hat{G}_0 is cyclic, and $\hat{G}_0/K \simeq PGL(3, q_\beta)$ or $PSL(3, q_\beta)$. In particular, $|\hat{G}_0/K| = \frac{1}{d} q_\beta^3 (q_\beta^3 - 1) (q_\beta^2 - 1)$, where $d = 1$ or 3 , the latter case occurring only if $q_\beta \equiv 1 \pmod{3}$. But by (7F),

$|\hat{G}| = q_\beta^3(q_\beta^3 - 1)(q_\beta + 1)(q_\alpha - 1)$. Thus $d(q_\alpha - 1)/(q_\beta - 1)$ is an integer. If $q_\alpha < q_\beta$ and $q_\alpha = p^{n_\alpha}$, $q_\beta = p^{n_\beta}$, we may write $n_\beta = n_\alpha + t$, where $t \geq 1$. But then

$$p^{n_\beta} - 1 = p^{n_\alpha} p^t - 1 > p^t(p^{n_\alpha} - 1) \geq 3(p^{n_\alpha} - 1),$$

and $d(q_\alpha - 1)/(q_\beta - 1)$ cannot be integral. Thus $q_\alpha \geq q_\beta$, so that by (4E), $q_\alpha = q_\beta$ or $q_\alpha = q_\beta^3$. This together with (5C) and (5D) gives

(7I) If G is a finite group with property (*) and (2A) (iii) holds, then q_1 and q_2 are equal, or one is the cube of the other.

This completes the proof of the theorem stated in the introduction.

We conclude with an identification of the group \hat{G} . Now the preceding proof shows that $q_\alpha = q_\beta$ or $q_\alpha = q_\beta^3$. Let $q_\beta = q$, and define $K_0 = (H)^{q-1}$. Clearly $K_0 = 1$ if $q_\alpha = q_\beta$, and $K_0 = (H_\alpha)^{q-1}$ is cyclic of order $q^2 + q + 1$ if $q_\alpha = q_\beta^3$. In either case, K_0 is a cyclic characteristic subgroup of H , so that $\langle \omega_1, \omega_2, \eta \rangle$ induces an abelian group of automorphisms on K_0 . In particular, η must centralize K_0 . K_0 then centralizes $\langle L_\beta, H, \eta \rangle = \hat{G}$, and so $K_0 \leq Z(\hat{G})$. Thus $K_0 \leq K$, where K is the normal subgroup of (7.3). Moreover, $|\hat{G}/K_0| = q^3(q^3 - 1)(q^2 - 1)$ by (7F).

If $q \equiv 1 \pmod{3}$, then $PGL(3, q)$, $PSL(3, q)$, and $SL(3, q)$ are isomorphic groups of order $q^3(q^3 - 1)(q^2 - 1)$. Since $|\hat{G}_0: K| \geq q^3(q^3 - 1)(q^2 - 1)$ in this case, it follows that $\hat{G} = \hat{G}_0$, $K = K_0$, and $\hat{G}/K_0 \simeq SL(3, q)$.

Assume then that $q \not\equiv 1 \pmod{3}$. If $\hat{G}_0/K \simeq PGL(3, q)$ the above argument will show that $\hat{G} = \hat{G}_0$, $K = K_0$, so that $\hat{G}/K_0 \simeq PGL(3, q)$. We assume then that $\hat{G}_0/K \simeq PSL(3, q)$, so that either $|\hat{G}: \hat{G}_0| = 3$, $|K: K_0| = 1$, or $|\hat{G}: \hat{G}_0| = 1$, $|K: K_0| = 3$. In the latter case, $\hat{G}/K_0 \simeq SL(3, q)$ or $PSL(3, q) \times Z_3$ by a result of Steinberg, [17]. The remaining case $|\hat{G}: \hat{G}_0| = 3$, $K = K_0$, leads to a contradiction if $\hat{G}/K \not\cong PGL(3, q)$. Indeed, since $q \equiv 1 \pmod{3}$, we have

$$q^2 + q + 1 \equiv 0 \pmod{3}, \quad q^2 + q + 1 \not\equiv 0 \pmod{9},$$

so that $|\hat{N}|$ contains the full power of 3 dividing $|\hat{G}|$, and thus $\hat{N} \cap \hat{G}_0 < \hat{N}$. On the other hand, L_β has no normal subgroups of index 3, so that L_β , and in particular, H_β , are contained in \hat{G}_0 . The definition of incidence in π given in [3], I, shows that the point jU is not on the line jU^* . The $q + 1$ involutions j_2, j_{1t} with t in X_β belong to $q + 1$ points of π , namely the $q + 1$ subsets of the form $\eta^{-2}jU\eta^2, s^{-1}\eta^{-1}jU\eta s$ with $s^2 = t$, s in X_β res-

pectively, and these points all lie on the line jU^* by [3], I, (2D). Moreover, these $q + 1$ points are distinct. Indeed, if $\eta^{-2}jU\eta^2 = s^{-1}\eta^{-1}jU\eta s$, then $\eta^{-2}U\eta^2 = jt \cdot s^{-1}\eta^{-1}U\eta s$, where $t = s^2$. This is impossible since jt has even order. If $s_1^{-1}\eta^{-1}jU\eta s_1 = s^{-1}\eta^{-1}jU\eta s$, then $s_1 s^{-1} \in C(j) \cap N(U^\eta) \leq N(C(j) \cap U^\eta) = N(X_{-\beta})$. Since $s_1 s^{-1} \in X_\beta$, this implies that $s_1 = s$. But the collineations on π induced by H_α leave the point jU fixed and the line jU^* pointwise fixed, so that $H_\alpha \leq \hat{G}_0$. Thus $H_1 H_2 \leq \hat{G}_0$. Since $|H: H_1 H_2| = 2$ and \hat{N}/H is generated by involutions, it now follows that $\hat{N} \leq \hat{G}_0$, which is a contradiction. We have thus proven

(7J) Let $q = \min\{q_1, q_2\}$, and let $K_0 = (H)^{q-1}$. Then K_0 is central in \hat{G} , and $\hat{G}/K_0 \simeq SL(3, q)$, $PGL(3, q)$, or $PSL(3, q) \times Z_3$.

§8. We now indicate how the arguments of [3], II, may be modified in order to prove (3E). Accordingly we shall adopt notation conforming in an obvious way with that of [3], II, so that a number of symbols already used will have different meanings in this section. Thus we shall assume that G is a finite group satisfying the following conditions.

(I) G has an involution j such that $C(j) = U \times L \langle j_1 \rangle$, where $L \simeq SL(2, q)$, U is a cyclic group of order dividing $\frac{1}{2}(q + \varepsilon)$ with $\varepsilon = \pm 1$, $q \equiv \varepsilon \pmod{4}$, and j_1 is an involution inducing an automorphism of class T_1 on L .

(II) $j \sim j_1$ in G .

We wish to show that $|G|$ is divisible by q^3 if $q > 3$, $G \simeq M_{11}$ or $SL(3, 3)$ if $q = 3$, and $q \leq 7$ if $U = 1$.

From (1.8), we see that an S_2 -subgroup S of $C(j)$ is of quasi-dihedral type, with center $\langle j \rangle$. As in (2B), we see that S is an S_2 -subgroup of G . Now (I), (II) imply that G has no normal subgroup of index 2.

If $\varepsilon = -1$, then $C(j)$ is isomorphic with the quotient group of $GL(2, q)$ by the subgroup of order $\frac{1}{2}(q-1)/|U|$ in its center. Then the desired results follow immediately from Theorem (1A) of [3], II.

We henceforth assume that $\varepsilon = 1$. Setting $D = \langle j, j_1 \rangle$ and using (1.9), we see that $C(D) = D \times U \times W$, where W is cyclic of order $\frac{1}{2}(q+1)$. Also, from (1.8), L contains an element f of order 4 which is inverted by j_1 , and $C(f)$ has order $2(q-1)|U|$. The element $t = f j_1$ is an involution such that $t: j_1 \rightarrow j_2 = j j_1$.

As in [3], II, we can apply the results of [2], III, §8. The principal 2-block of G consists of four irreducible characters $\chi_0 = 1, \chi_1, \chi_2, \chi_3$ of odd degrees $x_i = \chi_i(1)$, and 2^{n-2} irreducible characters $\chi_4, \chi^{(\mu)}$ with $1 \leq \mu \leq 2^{n-2} - 1$, of even degrees, where 2^n is the order of the S_2 -subgroup S of G . The relations (3. 1), (3. 2) of [3], II hold, and there exists a function φ on $C(j)$ such that $\pm\varphi$ is an irreducible character of $C(j)$ whose kernel contains j , and such that

$$(8. 1) \quad \begin{cases} \chi_1(jg) = -\delta_1 + \delta_1\varphi(g), & \chi_2(jg) = \delta_2 - \delta_2\varphi(g), \\ \chi_3(jg) = -\delta_3, & \chi_4(jg) = -2\delta_2 + \delta_2\varphi(g), & \chi^{(\mu)}(jg) = \pm\varphi(g), \end{cases}$$

for 2-regular g in $C(j)$. Moreover, we have

$$\varphi(1) \equiv 2 + 2^{n-2} \pmod{2^{n-1}}.$$

Since $C(j)/\langle j \rangle$ is isomorphic with the direct product of $PGL(2, q)$ with a cyclic group, its irreducible characters have degrees 1, $q, q - 1, q + 1$. It follows that φ is an irreducible character of $C(j)$ and that

$$(8. 2) \quad \varphi(1) = q + 1.$$

Further, the relation (3. 6) of [3], II holds, while the relations (3. 7) are replaced by

$$(8. 3) \quad \delta_1 x_1 \equiv 2 - q, \quad \delta_2 x_2 \equiv -q, \quad \delta_3 x_3 \equiv -1 + 2^{n-1} \pmod{2^n}.$$

In particular, the degrees 1, x_1, x_2, x_3 are all distinct. The order formula (4F) of [3], II is replaced by

$$(8. 4) \quad |G| = 2|U|q^2(q + 1)(q - 1)^3\mu,$$

$$(8. 5) \quad \mu = \left(1 + \frac{1}{q}\right)x_1(x_1 + \delta_1)/(x_1 - \delta_1q)^2 = \left(1 - \frac{1}{q}\right)x_2(x_2 + \delta_2)/(x_2 + \delta_2q)^2.$$

The lemmas (4D), (4E), (4H) of [3], II may now be shown to hold in the present situation, without any significant change in their proofs. We then have

(8A) It suffices to consider the case that $Z(G) = 1$. If this is satisfied, then $C(z) = C(j)$ whenever $1 \neq z \in Z(C(j))$.

Proof. Since $Z(G) \leq Z(C(j)) = U\langle j \rangle$ and $j \notin Z(G)$, it follows that $Z(G) \leq U$. If $Z(G) \neq 1$, then we can use induction on the group order to show that $|G/Z(G)|$ and hence $|G|$ are divisible by q^3 .

The second statement is proved as in [3], II, (4G), except for the possibility that

$$q = 5, |U| = 3, |G: C(U)| = 3.$$

In this case $C(U)$ must be normal in G , for otherwise G would have a quotient group isomorphic with the symmetric group of degree 3 and so would have a normal subgroup of index 2. Since $C(j)/U$ has no normal subgroup of index 3, $C(j) \leq C(U)$. Then $Z(C(U)) \leq Z(C(j))$, so that $Z(C(U)) = U$. Hence U is normal in G , and $G/C(U)$ is isomorphic with a subgroup of the automorphism group of U , a contradiction. Precisely as in [3], II, §9, we may prove

(8B) If $U \neq 1$ and $Z(G) = 1$, then $|G|$ is divisible by q^3 .

From now on we assume that $U = 1$. The arguments of [3], II, §10 apply, with rather obvious changes because the relations (8.1) to (8.5) hold rather than the corresponding relations of [3], II. Thus the contradiction at the end of the proof of [3], II, (10E), which now applies for prime divisors p of $l = \frac{1}{2}(q+1)$, stems from the relation

$$\gamma(x_1 - \delta_1)(q+1) = (x_1 + \delta_1)(q-1),$$

where $\gamma = 3$ or $5/3$, which leads to the relation $3\delta_1 = t(q+2)$ or $15\delta_1 = t(q+4)$, where t is an integer, an impossibility for $q \equiv 1 \pmod{4}$. The final contradiction on p. 150 of [3], II becomes the contradiction $x_1 = q^2(q-2)/(2q-1)$. We thus obtain

(8C) If $U = 1$, then $l = \frac{1}{2}(q+1)$ is 1, 3, 5 or 15.

The possible values for q are then 5, 9 or 29. In each case we can compute the possible values for x_1, x_2, x_3 . We have the eleven cases

- (1) $q = 5; x_1 = 125, x_2 = 21, x_3 = 105; |G| = 2^4 \cdot 3^2 \cdot 5^3 \cdot 7.$
- (2) $q = 5; x_1 = 19, x_2 = 75, x_3 = 57; |G| = 2^4 \cdot 3^2 \cdot 5^2 \cdot 19.$
- (3) $q = 5; x_1 = 35, x_2 = 85, x_3 = 119; |G| = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 17.$
- (4) $q = 9; x_1 = 729, x_2 = 73, x_3 = 657; |G| = 2^5 \cdot 3^6 \cdot 5 \cdot 73.$
- (5) $q = 9; x_1 = 135, x_2 = 201, x_3 = 335; |G| = 2^5 \cdot 3^3 \cdot 5^3 \cdot 67.$
- (6) $q = 9; x_1 = 71, x_2 = 567, x_3 = 497; |G| = 2^5 \cdot 3^4 \cdot 5 \cdot 7 \cdot 71.$
- (7) $q = 29; x_1 = 29 \cdot 41, x_2 = 17 \cdot 29, x_3 = 17 \cdot 41; |G| = 2^4 \cdot 3^2 \cdot 5 \cdot 7^4 \cdot 17 \cdot 29 \cdot 41.$

- (8) $q = 29$; $x_1 = 29^3$, $x_2 = 3 \cdot 271$, $x_3 = 3 \cdot 29 \cdot 271$; $|G| = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 29^3 \cdot 271$.
 (9) $q = 29$; $x_1 = 23 \cdot 29$, $x_2 = 3 \cdot 29 \cdot 37$, $x_3 = 3 \cdot 23 \cdot 37$; $|G| = 2^4 \cdot 3^2 \cdot 5^2 \cdot 7^3 \cdot 23 \cdot 29 \cdot 37$.
 (10) $q = 29$; $x_1 = 3 \cdot 13 \cdot 29$, $x_2 = 29 \cdot 113$, $x_3 = 3 \cdot 13 \cdot 113$; $|G| = 2^4 \cdot 3^3 \cdot 5 \cdot 7^3 \cdot 13 \cdot 29 \cdot 113$.
 (11) $q = 29$; $x_1 = 811$, $x_2 = 3^3 \cdot 29^2$, $x_3 = 3^3 \cdot 811$; $|G| = 2^4 \cdot 3^4 \cdot 5 \cdot 7 \cdot 29^2 \cdot 811$.

All these cases except (1) can be ruled out by a combination of Sylow's Theorem and the theory of blocks of defect 1. This completes the proof of (3E).

REFERENCES

- [1] R. Brauer, Zur Darstellungstheorie der Gruppen endlicher Ordnung I, *Math. Z.* **63** (1956), 406–444.
 [2] R. Brauer, Some applications of the theory of blocks of characters of finite groups II, III, *J. Alg.* **1** (1964), 307–334, **3** (1966), 225–255.
 [3] R. Brauer, On finite Desarguesian planes I, II, *Math. Z.* **90** (1965), 117–123, **91** (1966), 124–151.
 [4] R. Brauer, Investigations on groups of even order, *Proc. Nat. Acad. Sci.* **55** (1966), 254–259.
 [5] R. Brauer, On blocks and sections in finite groups II, *Amer. J. Math.*, **90** (1968), 895–925.
 [6] R. Brauer and C. Nesbitt, On the modular characters of groups, *Annals of Math.* **42** (1941), 556–590.
 [7] R. Brauer and M. Suzuki, On finite groups of even order whose 2–Sylow group is a quaternion group, *Proc. Nat. Acad. Sci.* **45** (1959), 1757–1759.
 [8] R.W. Carter, Simple groups and simple Lie algebras, *J. London Math. Soc.* **40** (1965), 193–240.
 [9] E.C. Dade, Blocks with cyclic defect groups, *Annals of Math.* **84** (1966), 20–48.
 [10] L.E. Dickson, Determination of all the subgroups of the known simple group of order 25920, *Trans. Amer. Math. Soc.* **5** (1904), 126–166.
 [11] J. Dieudonné, *La géométrie des groupes classiques*, Springer, 1955.
 [12] P. Fong, A characterization of the finite simple groups $PSp(4, q)$, $G_2(q)$, $D_4^{\epsilon}(q)$, II, to appear, *Nagoya Math. J.*
 [13] G. Glauberman, Central elements in core-free groups, *J. Alg.* **4** (1966), 403–420.
 [14] P. Hall and G. Higman, The p -length of a p -soluble group and reduction theorems for Burnside's problem, *Proc. London Math. Soc.* (3), **7** (1956), 1–42.
 [15] G.A. Miller, The groups of isomorphisms of the simple groups whose degrees are less than fifteen, *Arch. Math. u. Phys.* **12** (1907), 249–251.
 [16] I. Schur, Untersuchungen über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen, *J. für reine u. angew. Math.* **132** (1907), 85–137.
 [17] R. Steinberg, Générateurs, relations, et revêtements de groupes algébriques, *Colloque sur la Théorie des groupes algébriques*, Brussels, 1962.
 [18] W.J. Wong, A characterization of the finite projective symplectic groups $PSp_4(q)$, *Trans. Amer. Math. Soc.*, **139** (1969), 1–35.

University of Illinois, Chicago, Illinois

University of Notre Dame, Notre Dame, Indiana