A CHARACTERIZATION OF THE FINITE PROJECTIVE SYMPLECTIC GROUPS $\text{PSp}_4(q)$

BY

W. J. WONG(1)

In this paper we present a characterization of the projective symplectic groups $\text{PSp}_4(q)$ in dimension 4 over finite fields of odd characteristic, in terms of the structure of the centralizer of an involution. The group $\text{PSp}_4(q)$ is simple, of order $\frac{1}{4}q^4(q^2+1)(q^2-1)^2$, with a Sylow 2-subgroup whose center has order 2, so that involutions which lie in the centers of Sylow 2-subgroups form a single conjugacy class (see §1). We shall prove the following result.

THEOREM. Let $C$ be the centralizer in $\text{PSp}_4(q)$ of an involution lying in the center of some Sylow 2-subgroup, where $q$ is odd. Let $G$ be a finite group containing an involution $t$ whose centralizer $C(t)$ in $G$ is isomorphic with $C$. Then either

(i) $G = C(t)O(G)$, or
(ii) $G$ is isomorphic with $\text{PSp}_4(q)$.

Here $O(G)$ denotes the largest normal subgroup of odd order in $G$. In particular, $\text{PSp}_4(q)$ is the only simple group satisfying the hypothesis of the theorem.

A similar characterization of $\text{PSp}_4(q)$ in the case of even $q$ has been given by Suzuki [13]. A special case of our theorem has been obtained by Janko, who dealt with the case $q = 3$ [10].

We use a method which appears to be rapidly becoming standard (e.g., [11], [12], [13]). This is the construction of a $(BN)$-pair for $G$ [16]. In our case, after discarding the case (i) of the theorem, we show that $G$ has a subgroup $G_0$ with a $(BN)$-pair having as Weyl group the dihedral group of order 8. This in itself is not sufficient to identify $G_0$, but we can prove that the multiplication table of $G_0$ is uniquely determined, from which it follows that $G_0$ is isomorphic with $\text{PSp}_4(q)$. By using a lemma of Suzuki we prove that $G_0 = G$. Our techniques are similar to those of Janko and Phan [10], [11]. We do not use directly the theory of group characters, but we do use a result of Gorenstein and Walter which requires the character theory [7].

The paper is organized as follows. In §1 we determine the structure of the group $C$. Next we show in §2 that if case (i) of the conclusion of the theorem does not hold then $G$ has exactly two classes of involutions. In §3 we determine the structure of the centralizer of an involution in the second class. By studying the centralizers

Received by the editors September 4, 1967.

(1) Research partially supported by National Science Foundation grant GP-6652 at the University of Notre Dame.
and normalizers of various $p$-subgroups ($p$ the prime divisor of $q$), we find the structure of the normalizer of a Sylow $p$-subgroup in §4. In §5 we put together the $(BN)$-pair and finish the proof as outlined above.

Our notation is largely standard. We use $O(X)$ to denote the largest normal subgroup of odd order in the finite group $X$. $N_X(Y)$ and $C_X(Y)$ are the normalizer and centralizer of $Y$ in $X$; we omit the subscript when $X= G$. We write $[x, y] = x^{-1}x^y = x^{-1}y^{-1}xy$. If $x^y = z$, we also write $y: x \rightarrow z$. If $y: x \rightarrow x^{-1}$, we say that $y$ inverts $x$. The field of $q$ elements is denoted $F_q$. When we speak of the norm of an element of $F_q^*$, we shall always mean the norm from $F_q^*$ to $F_q$. Finally, we shall take linear transformations on a vector space as acting on the right.

1. **The group $C$.** Let $q$ be a power of an odd prime number $p$. We define the integer $\delta$ by the conditions

\[
q \equiv \delta \pmod{4}, \quad \delta = \pm 1.
\]

Let $2^n$ be the greatest power of 2 dividing $q - \delta$, so that

\[
q - \delta = 2^ne, \quad e \text{ odd}.
\]

We fix a generator $e$ of the multiplicative group of $F_q$. Setting

\[
J = \begin{bmatrix}
0 & 1 & 0 & 0 \\
-1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & -1 & 0
\end{bmatrix},
\]

we may take $\text{PSp}_4(q)$ as the group of all matrices $A$ of degree 4 with coefficients in $F_q$ such that $A'JA = J$, where $A'$ denotes the transpose of $A$ and we identify two such matrices if they are negatives of each other. Let $C$ be the centralizer in $\text{PSp}_4(q)$ of the involution $t = \begin{bmatrix} I & 0 \\ 0 & -I \end{bmatrix}$, where $I$ is the identity matrix of degree 2. It is easily verified that $C$ consists of all elements of the form

\[
\begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} 0 & A \\ B & 0 \end{bmatrix},
\]

where $A, B \in \text{SL}_2(q)$. Setting

\[
L_1 = \left\{ \begin{bmatrix} A & 0 \\ 0 & I \end{bmatrix} \bigg| A \in \text{SL}_2(q) \right\}, \quad L_2 = \left\{ \begin{bmatrix} I & 0 \\ 0 & B \end{bmatrix} \bigg| B \in \text{SL}_2(q) \right\},
\]

\[
u = \begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix},
\]
we see that $L_1$ and $L_2$ are isomorphic with $SL_2(q)$, elements of $L_1$ commute with elements of $L_2$, $L_1 \cap L_2 = \langle t \rangle$, $C = L_1 L_2 \langle u \rangle$, $u^2 = 1$, $L_1^2 = L_2$. Since $SL_2(q)$ has center of order 2 it follows easily that $C$ has center $\langle t \rangle$.

Since $C$ has order

$$|C| = |SL_2(q)|^2 = q^2(q^2-1)^2,$$

the index of $C$ in $PSp_4(q)$ is $\frac{1}{2} q^2(q^2+1)$, an odd number. Thus a Sylow 2-subgroup $S$ of $C$ is also a Sylow 2-subgroup of $G$, and $t$ lies in the center of $S$. We can take $S = S_1 S_2 \langle u \rangle$, where $S_1$ is a Sylow 2-subgroup of $L_1$, $S_2 = S_1^T$. We construct the $S_i$ as follows. Let

$$(3) \quad d = \begin{bmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{bmatrix} (\delta = 1), \text{ or } d = \begin{bmatrix} \alpha & \beta \\ \varepsilon \beta & \alpha \end{bmatrix} (\delta = -1),$$

where in the second case $\alpha$ and $\beta$ are elements of $F_2$ such that $\alpha + \beta \sqrt{\varepsilon}$ is a generator of the group of elements of norm 1 in $F_{q^2}$. Then $d$ is an element of order $q - \delta$ in $SL_2(q)$, generating a subgroup whose normalizer is $\langle d, b \rangle$, where

$$(4) \quad b = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} (\delta = 1), \text{ or } b = \begin{bmatrix} \lambda & \mu \\ -\varepsilon \mu & -\lambda \end{bmatrix} (\delta = -1),$$

where in the second case $\lambda$ and $\mu$ are elements of $F_q$ such that $\lambda^2 - \varepsilon \mu^2 = -1$. Then $b$ inverts $d$ and $b^2 = -I$. If we put

$$(5) \quad a = d^e,$$

then $\langle a, b \rangle$ is a Sylow 2-subgroup of $SL_2(q)$, a generalized quaternion group of order $2^{n+1}$. If $a$ and $b$ are transformed into $a_1$ and $b_1$ by an isomorphism of $SL_2(q)$ with $L_1$, and $u$ transforms $a_1$ and $b_1$ into $a_2$ and $b_2$, then we may take $S_i = \langle a_i, b_i \rangle$, so that we have

$$S = \langle a_1, b_1, a_2, b_2, u \rangle,$$

$$a_1^2 = b_1^2 = t, \quad a_1 b_1 = b_1 a_1^{-1},$$

$$[a_1, a_2] = [a_1, b_2] = [b_1, a_2] = [b_1, b_2] = 1,$$

$$a_1^u = a_2, \quad b_1^u = b_2.$$
If \( x \) and \( y \) are elements of \( L_1 \) and \( L_2 \) respectively, then

\[(uxy)^2 = (y^ux)(x^uy),\]

and \( y^ux \in L_1, x^uy \in L_2 \). Hence, if \( uxy \) is an involution then \( y^ux \in L_1 \cap L_2 = \langle t \rangle \), so that \( uxy = y^ux = x^{-1}ux \) or \( x^{-1}txtu \).

We summarize all the properties of \( C \) which we have found in the following lemma.

**Lemma 1.1.** (i) \(|C| = q^2(q^2 - 1)^2\).
(ii) \( C = L_1L_2t \), where \( L_1 \) and \( L_2 \) are subgroups of \( C \), such that

\[L_1 \cap L_2 = \langle t \rangle, \quad [L_1, L_2] = \{1\},\]

\( u \) is an involution, and there are isomorphisms

\[x \rightarrow x_1, \quad x \rightarrow x_2,\]

of \( SL_2(q) \) on \( L_1 \) and \( L_2 \) respectively, such that

\[x_1^u = x_2,\]

for all \( x \) in \( SL_2(q) \).

(iii) If \( d, b \) and \( a \) are the elements of \( SL_2(q) \) given by (3), (4) and (5), then

\[S = \langle a_1, b_1, a_2, b_2, u \rangle\]

is a Sylow 2-subgroup of \( C \), of order \( 2^{2n+2} \), with the generators of \( S \) satisfying the relations (6).

(iv) \( Z(C) = Z(S) = \langle t \rangle \).

(v) All involutions of \( L_1L_2 = \langle t \rangle \) are conjugate in \( C \). All involutions of \( C - L_1L_2 \) are conjugate in \( C \) to \( u \) or \( tu \).

If \( x \) is an element of \( SL_2(q) \), we shall always let \( x_1 \) and \( x_2 \) be the elements of \( L_1 \) and \( L_2 \) obtained from \( x \) by applying the isomorphisms of (ii) above.

2. **Classes of involutions in \( G \).** From now on we assume that \( G \) is a finite group satisfying the hypothesis of the theorem. In the isomorphism of \( C(t) \) with \( C \), the image of \( t \) must be the unique nontrivial element of \( Z(C) \). Thus we may take \( C(t) = C \), where \( C \) has the properties of Lemma 1.1.

**Lemma 2.1.** \( S \) is a Sylow 2-subgroup of \( G \).

**Proof.** Let \( T \) be a Sylow 2-subgroup of \( G \) containing \( S \). Then \( Z(T) \) centralizes \( t \), so that

\[Z(T) \leq C(t) \cap T = S,\]

whence \( Z(T) \leq Z(S) \), so that \( Z(T) = \langle t \rangle \), by Lemma 1.1 (iv). Hence \( T \leq C(t) \), so that \( T = S \). This proves the lemma.
Two of the involutions of $L_1L_2 - \langle t \rangle$ are

\begin{equation}
 v = (a_1a_2)^{2^n-2}, \quad w = b_1b_2.
\end{equation}

**Lemma 2.2.** The involutions of $L_1L_2 - \langle t \rangle$ are not conjugate in $G$ to $t$.

**Proof.** By Lemma 1.1 (v), it is enough to show that $v$ is not conjugate in $G$ to $t$. The centralizer of $v$ in $C(t)$ is

\begin{equation}
 C(t, v) = \langle u, d_1, d_2, w \rangle,
\end{equation}

a group of order $2(q - 8)^2$. We have

\begin{equation}
 d_1^1 = d_2, \quad d_1^w = d_1^{-1}, \quad [u, w] = 1.
\end{equation}

A Sylow 2-subgroup of $C(t, v)$ is $T = \langle u, a_1, a_2, w \rangle$, a group of order $2^{2n+1}$. We compute that $Z(T) = \langle t, v \rangle$.

Suppose first that $n > 2$. We can calculate that each of the involutions $v$, $w$ of $Z(T)$ is a power of exactly $2^{2n-1} - 2^{n-1}(2^{2n-2} - 1)$ elements of $F$, while $t$ is a power of only $2^{2n-1} - 2^{n-1} + \frac{1}{2}(2^{2n-2} - 1)$ elements of $T$. It follows that $\langle t \rangle$ is a characteristic subgroup of $T$. If $v$ were conjugate in $G$ to $t$, then $C(v)$ would contain a Sylow 2-subgroup $V$ of $G$ containing $T$. Since $|V : T| = 2$, $T$ would be normal in $V$, so that $\langle t \rangle$ would be normal in $V$. Then $Z(V)$ would contain $v$ and $t$, contradicting the fact that $Z(S)$ has order 2 and $V$ is isomorphic with $S$.

Now suppose that $n = 2$, so that $|T| = 32$. We repeat an argument of Janko [10]. $T$ has an elementary Abelian maximal subgroup

\begin{equation}
 E = \langle t, u, v, w \rangle.
\end{equation}

Since $C(E) \leq C(t)$, we can compute $C(E)$. We find that $C(E) = E$. Hence

\begin{equation}
 X = N(E)/E
\end{equation}

is isomorphic with a subgroup of the automorphism group of $E$, which is isomorphic with $GL_4(2)$, i.e. with the alternating group $A_8$.

Since $|Z(T)| = 4$, $E$ is the only Abelian maximal subgroup of $T$, for otherwise the intersection of two such subgroups would be a subgroup of order 8 in $Z(T)$. Hence $N(T) \leq N(E)$. Suppose that $v$ is conjugate to $t$ in $G$. Then, as before, a Sylow 2-subgroup $V$ of $C(v)$ containing $T$ is a Sylow 2-subgroup of $G$, and $V \not= S$ since $S \not\leq C(v)$. Since $V$ and $S$ normalize $T$, they are contained in $N(E)$. The four-groups $V/E$ and $S/E$ are Sylow 2-subgroups of $X$ containing $T/E = \langle a_1E \rangle$. Thus the centralizer in $X$ of the involution $a_1E$ has more than one Sylow 2-subgroup. Since involutions of $A_8$ have centralizers of order $2^3$ or $2^3$ [17, p. 360], we see that $C_X(a_1E)$ is dihedral of order 12.

Since $n = 2$, SL$_2(q)$ contains an element $f$ of order 3 normalizing the Sylow 2-subgroup $\langle a, b \rangle$ of SL$_2(q)$, and permuting the subgroups $\langle a \rangle$, $\langle b \rangle$ and $\langle ab \rangle$ cyclically (since PSL$_2(q)$ has subgroups isomorphic with $A_4$ [4, p. 268]). Then $f_1f_2$ normalizes $\langle a_1a_2, b_1b_2 \rangle = \langle v, w \rangle$. Also, $f_1f_2$ centralizes $\langle t, u \rangle$. Hence $f_1f_2 \in N(E)$,
and \( f_1 f_2 E \) permutes the involutions \( a_1 E, b_1 E, a_1 b_1 E \) of \( S/E \) cyclically. Hence \( \langle a_1 E, b_1 E, f_1 f_2 E \rangle \) is isomorphic with \( A_4 \), and all involutions of \( X \) are conjugate.

Since \( A_4 \) has no normal subgroup of order 3, \( f_1 f_2 E \) is not contained in \( O(X) \), so that \(|X : O(X)| \) is divisible by 3. Since \( 3^3 \) does not divide \(|A_4|, |O(X)| \) is not divisible by \( 3^2 \). Hence \( O(X) \) has a normal 3-complement \( W \), by Burnside's theorem. If \( C_X(a_1 E) \cap O(X) \neq \{1\} \), then we must have

\[
O(X) = (C_X(a_1 E) \cap O(X))W.
\]

Then \( a_1 E \) centralizes the chief factor \( O(X)/W \) of \( X \). Hence the conjugate \( b_1 E \) of \( a_1 E \) should also centralize \( O(X)/W \). But, \( b_1 E \) inverts \( C_X(a_1 E) \cap O(X) \), so that we have a contradiction. Thus,

\[
C_X(a_1 E) \cap O(X) = \{1\}.
\]

Now a theorem of Gorenstein and Walter [7, Theorem I] shows that \( X/O(X) \) is isomorphic with \( PSL_2 (11) \) or \( PSL_2 (13) \). This contradicts the fact that \(|A_8| \) is not divisible by 11 or 13. Hence \( \nu \) is not conjugate in \( G \) to \( t \). This completes the proof of the lemma.

We now assume that case (i) of the conclusion of our theorem does not hold, i.e. that

(10) \( G \neq C(t)O(G) \).

**Lemma 2.3.** Either \( u \) or \( tu \) is conjugate in \( G \) to \( t \).

**Proof.** If this were not so, then \( t \) would be conjugate in \( G \) to no other involution of \( S \), by Lemma 1.1 (v). By a theorem of Glauberman [6, Theorem 1], \( tO(G) \) lies in the center of \( G/O(G) \), i.e.

\[
C_{G/O(G)}(tO(G)) = G/O(G).
\]

Since \( C_{G/O(G)}(tO(G)) = C_{G}(tO(G))/O(G) \), we find that \( G = C(t)O(G) \), contradicting the assumption (10). This proves the lemma.

From the description of \( C \) given in Lemma 1.1 (ii) we see that \( C \) has an automorphism interchanging the involutions \( u \) and \( tu \). Thus we may assume that

(11) \( tu \) is conjugate in \( G \) to \( t \).

**Lemma 2.4.** \( G \) has exactly two conjugacy classes of involutions, \( K_1 \) and \( K_2 \), such that \( K_1 \cap C \) consists of the classes in \( C \) represented by \( t \) and \( tu \), and \( K_2 \cap C \) consists of the classes in \( C \) represented by \( v \) and \( u \). There exists an element \( z \) of \( G \) such that \( z^2 \) lies in \( S \) and

(12) \[
z: t \to uv, \quad u \to tv, \quad v \to v.
\]

**Proof.** Let \( K_1 \) be the conjugacy class of \( t \) in \( G \) and \( K_2 \) the conjugacy class of \( v \) in \( G \). By Lemma 2.2, \( K_1 \neq K_2 \). We set

\[
E = C_S(tu) = \langle a_1 a_2, w \rangle \times \langle t, u \rangle.
\]
The subgroup \( \langle a_1a_2, w \rangle \) is dihedral of order \( 2^n \), so that \(|E| = 2^{n+2}\). Let \( T \) be a Sylow 2-subgroup of \( C(tu) \) containing \( E \). Since \( tu \) is conjugate in \( G \) to \( t \), \(|T| = 2^{n+2} > |E| \). Hence there exists an element \( z \) of \( T - E \) such that \( z^2 \in E \) and \( z \) normalizes \( E \).

Suppose first that \( n > 2 \). Then \( Z(E) = \langle t, u, v \rangle \) is normalized by \( z \). Since \( tu \) is conjugate in \( C \) to \( tu \), the involutions \( t, tu \), and \( uv \) lie in \( K_1 \), by (11). Since \( v \) and \( tv \) are conjugate in \( C \) by Lemma 1.1 (v), \( v \) and \( tv \) lie in \( K_2 \). The other two involutions \( u \) and \( tuw \) of \( Z(E) \) are conjugate in \( C \). If the subset \{v, tv\} were invariant under \( z \), then \( t = z(tu) \) would be invariant under \( z \), contradicting the fact that \( z \notin C(t) \). Hence \( v \) or \( tv \) is transformed by \( z \) into \( u \) or \( tuw \), so that \( v, tv, u \) and \( tuw \) all lie in \( K_2 \). Since every involution of \( G \) is conjugate to an element of \( S \) and thus to one of the involutions \( t, v, u, tu \), we have the first statement of the lemma. Also since \((tu)^z = tu \) and \( t^z \neq t \), we must have

\[ t^z = uv, \quad (uv)^z = t. \]

Hence \((tuw)^z = uv = tuw \). Since \((tu)^z = tu \), we have \( v^z = v \). Then \( u^z = (uvv)^z = tv \), and we have proved (12).

Now suppose that \( n = 2 \). Then \( E = \langle t, u, v, w \rangle \). The intersections of \( E \) with the conjugacy classes of involutions of \( C \) are

\[ J_1 = \{t\}, \quad J_3 = \{v, w, vw, tv, tw, tvw\}, \]
\[ J_2 = \{tu, uw, uv, uvw\}, \quad J_4 = \{u, tw, tuw, tuvw\}. \]

We know that \( J_1 \) and \( J_2 \) lie in \( K_1 \) and \( J_3 \) lies in \( K_2 \). If \( J_3 \) were invariant under \( z \), then the product of the elements of \( J_3 \), which is \( t \), would also be invariant under \( z \), a contradiction. Hence one of the involutions in \( J_3 \) is conjugate to one of the involutions of \( J_4 \), and we have the first statement of the lemma. In particular,

\[ K_1 \cap E = \{t, tu, uw, uv, uvw\}. \]

In the proof of Lemma 2.2, we saw that a Sylow 2-subgroup of \( N(E)/E \) is contained in a subgroup isomorphic with \( A_4 \). Thus the involution \( zE \) of \( N(E)/E \) is contained in such a subgroup \( F \) of \( N(E)/E \). Then \( F \) acts on the set \( K_1 \cap E \), the action being faithful since \( zE \) moves \( t \). Now \( A_4 \) has only one faithful permutation representation of degree 5, the obvious one. In this representation, a letter fixed by one involution is fixed by all, and the involutions permute the remaining letters transitively. Since \( zE \) fixes \( tu \), \( F \) contains an involution which fixes \( tu \) and transforms \( t \) into \( uv \). We now replace \( z \) by an element of \( N(E) \) representing this involution, and the proof is finished as before.

We remark that in \( PSp_4(q) \) one class of involutions consists of elements coming from involutions of \( Sp_4(q) \), and the other class comes from the semi-involutions [5, p. 5].

If \( S^* \) is the focal group of \( S \) in \( G \), i.e. the intersection of \( S \) with the derived group \( G' \) of \( G \), then \( S^* \) contains the derived group of \( S \),

\[ S' = \langle a_1^2, a_2a_2, w \rangle. \]
Since $w_1a$ is conjugate to $w$ in $C$, $S^*$ also contains $w_1a$, and hence $a_1$. Since $b_1$ is conjugate to a power of $a_1$, $S^*$ contains $b_1$. Finally, $tu$ is conjugate in $G$ to the element $t$ of $S'$. Thus we obtain $S^* = S$, so that $G$ has no subgroup of index 2.

If $q = 3$, our theorem now follows from the result of Janko [10]. Since a few of the arguments which we shall use do not work in the case $q = 3$ but have to be replaced by special arguments (given by Janko), we shall henceforth assume that

$$q > 3.$$

3. **Centralizers of involutions in $K_2$.** We shall determine the structure of $C(u)$. Let

$$A = \{x_1x_2 \mid x \in SL_2(q)\}.$$  

Then $A$ is a subgroup of $C(t)$ isomorphic with $PSL_2(q)$, an isomorphism being provided by the mapping taking $x_1x_2$ on the element of $PSL_2(q)$ represented by the matrix $x$. For convenience, we shall identify $A$ with $PSL_2(q)$ by means of this isomorphism. We have

$$C(t, u) = \langle t, u \rangle \times A.$$  

Also, by (8), we have $C(t, v) = \langle tu, d_1, d_2, w \rangle$. Transforming by the element $z$ of Lemma 2.4, we find that

$$C(u, v) = \langle tu, d_1^z, d_2^z, w^z \rangle.$$  

In order to use the information in (15) and (16) to determine $C(u)$, we require more knowledge of the action of $z$.

**Lemma 3.1.** $\langle d_1d_2 \rangle^z = \langle d_1d_2 \rangle$, $\langle a_1a_2 \rangle^z = \langle a_1a_2 \rangle$, and

$$w = (w(d_1d_2)^mtu)^z,$$  

for some integer $m$.

**Proof.** We have

$$C(t, u, v) = \langle tv, uw \rangle \times \langle d_1d_2, w \rangle.$$  

Here $C_A(v)$ is a dihedral group of order $q - 3$. Since $v$ is a central involution of $C_A(v)$, we may also write

$$C(t, u, v) = \langle tv, uw \rangle \times \langle d_1d_2, w \rangle.$$  

Since $z$ normalizes $\langle t, u, v \rangle$, we may transform by $z$, and, using (12), obtain

$$C(t, u, v) = \langle t, u \rangle \times \langle (d_1d_2)^z, w^z \rangle.$$
Calculation of the subgroup $Y$ of $C(t, u, v)$ generated by those elements which have as a power an involution in $\langle t, u, v \rangle$ (using (18), (19) and (20)) shows that

$$Y = \langle t, u \rangle \times \langle d_1 d_2 \rangle = \langle t, u \rangle \times \langle (d_1 d_2)^z \rangle.$$

Now put

$$g = a_2^{2s-2}.$$

Then $g^2 = t$, and transformation by $g$ interchanges $tu$ and $uv$. By (12), we see that

$$(g^z)^2 = uv, \quad g^z : t \leftrightarrow tu.$$ 

In particular, $g^z$ normalizes $\langle t, u \rangle$ and so normalizes $C(t, u)$. From (15), $A$ is the derived group of $C(t, u)$, so that $g^z$ normalizes $A$. Also, $g$ commutes with $v$ and $v^z = v$, so that $g^z$ commutes with $v$. Hence $g^z$ normalizes $C_A(v)$.

Now, $[g^z, (d_1 d_2)^z] = [g, d_1 d_2]^z = 1$, so that $[g^z, Y] \leq \langle t, u \rangle$. Since $d_1 d_2$ lies in both $Y$ and $C_A(v)$, we have

$$[g^z, d_1 d_2] \leq \langle t, u \rangle \cap C_A(v) = \{1\},$$

so that $g^z$ commutes with $d_1 d_2$.

We also have $[g, w] = t$, so that, by (12), $[g^z, w^z] = uv$. Hence, if $x$ is any element of $C(t, u, v) - Y = w^z Y$, then

$$[g^z, x] \in v\langle t, u \rangle.$$ 

Since $w$ is such an element, $w \in C_A(v)$, and $v\langle t, u \rangle \cap C_A(v) = \{v\}$, we have

(21)

$$[g^z, w] = v.$$ 

We now know the action of $g^z$ on $t, u, v, w, d_1 d_2$, and their transforms by $z$. From (18), (19) and (20), we obtain

(22)

$$\langle u \rangle \times \langle d_1 d_2 \rangle = C(t, u, v, g^z) = \langle u \rangle \times \langle (d_1 d_2)^z \rangle.$$

Suppose that $(d_1 d_2)^z = u(d_1 d_2)^m$ for some integer $m$. Then, taking $e$th powers, we have $(a_1 a_2)^z = u(a_1 a_2)^m$, so that, from (12),

$$(a_1 a_2)^{ze} = twu^m(a_1 a_2)^m.$$ 

Thus $z^2$ does not normalize $\langle a_1 a_2 \rangle$. This is a contradiction, since, by Lemma 2.4, $z^2$ lies in $C_3(t, u) = \langle t, u \rangle \times \langle a_1 a_2, w \rangle$, which has $\langle a_1 a_2 \rangle$ as a normal subgroup.

It now follows from (22) that

$$\langle (d_1 d_2)^z \rangle = \langle d_1 d_2 \rangle.$$ 

Taking $e$th powers shows that $\langle (a_1 a_2)^z \rangle = \langle a_1 a_2 \rangle$.

Since $w$ has the property (21), computation in the group $C(t, u, v)$ shows that

(23)

$$w = w^e((d_1 d_2)^z)^m tw, \quad \text{or} \quad w = w^e((d_1 d_2)^z)^m tu.$$
for some integer \( m \). Now, \( w^m((d_1d_2)^m)v = w(d_1d_2)^m = (b_1d_1)^m \times (b_1d_1)^m \), which lies in \( K_1 \), and \( w \) lies in \( K_2 \). Hence the second alternative in (23) must hold. Since \((tu)^z = tu\), we have the formula (17). This proves the lemma.

By (16), \( C(u, v) \) contains the subgroup \( \langle tu, a_1^z, a_2^z \rangle \), of order \( 2^{2n} \). Now, \( w \) centralizes \( tu \), and by (17),

\[
(a_1^z)^w = (a_3^z)^{-1}, \quad (a_2^z)^w = (a_3^z)^{-1}.
\]

Hence the element \( w \) of \( C(u, v) \) normalizes \( \langle tu, a_1^z, a_2^z \rangle \), so that \( C(u, v) \) contains the subgroup

\[
T = \langle tu, a_1^z, a_2^z, w \rangle
\]

of order \( 2^{2n+1} \). Since \( u \) does not lie in the center of a Sylow 2-subgroup of \( G \), \( T \) must be a Sylow 2-subgroup of \( C(u) \).

**Lemma 3.2.** \( C(u) \) has a normal subgroup \( K \) of index 2 with Sylow 2-subgroup

\[
M = \langle a_1^z, a_2^z, w \rangle.
\]

**Proof.** Let \( T^* \) be the focal group of \( T \) in \( C(u) \), i.e. the intersection of \( T \) with the derived group of \( C(u) \). Then \( T^* \) contains the derived group of \( T \),

\[
T' = \langle a_1a_2, a_2^z \rangle.
\]

Also, since \( A \) is a subgroup of \( C(u) \) having no subgroup of index 2, \( T^* \) contains \( A \cap T = \langle a_1a_2, w \rangle \). Thus \( T^* \) contains the subgroup

\[
W = \langle (a_1a_2)^z, (a_1^z)^z, w \rangle.
\]

This is a normal subgroup of \( T \), and \( T/W \) is a four-group.

We shall use the following result of Thompson [15, Lemma 5.38], proved by a simple transfer argument.

**Lemma 3.3.** Let \( M \) be a maximal subgroup of a Sylow 2-subgroup of a finite group \( X \). Then every involution of the derived group of \( X \) is conjugate in \( X \) to an element of \( M \).

Here we take \( M = \langle a_1^z, a_2^z, w \rangle \). Using the relations (24), we see that \( M \) has five classes of involutions, represented by

\[
u, v, w, w, uvw.
\]

Since \( A \) contains only one class of involutions, \( v, w \) and \( uw \) are conjugate in \( C(u) \). Hence \( uw \) and \( uvw \) are conjugate in \( C(u) \). Thus the involutions of \( M \) lie in conjugacy classes of \( C(u) \) represented by \( u, v, uw \). We have \( u, v \in K_2, uv \in K_1 \).

If \( tu \) were conjugate in \( C(u) \) to \( uv \), then \( t = (tu)u \) would be conjugate to \( (uv)u = v \), contradicting Lemma 2.2. Hence \( tu \) is conjugate in \( C(u) \) to no element of \( M \), so that, by Lemma 3.3, \( T^* \) does not contain \( tu \).
The element $tua_1^2w$ is an involution, conjugate in $G$ to $tua_1w(d_1d_2)^mtu = a_2w(d_1d_2)^m$, by (17). Thus $tua_1^2w$ lies in $K_2$. If $tua_1^2w$ were conjugate in $C(u)$ to $v$, $tua_1^2w$ would be conjugate to $w$. But $tua_1^2w$ is conjugate in $G$ to $uwa_1w(d_1d_2)^mtu = va_2w(d_1d_2)^mt$, which lies in $K_2$ by Lemmas 2.2 and 2.4, while $w$ lies in $K_1$. Hence $tua_1^2w$ is not conjugate in $C(u)$ to $v$. Obviously $tua_1^2w$ is not conjugate in $C(u)$ to $u$. Hence $tua_1^2w$ is conjugate in $C(u)$ to no element of $M$, so that, by Lemma 3.3, $T^*$ does not contain $tua_1^2w$.

It now follows that we have two possibilities for $T^*$:

$$T^* = W, \text{ or } T^* = \langle a_1^2, W \rangle = M.$$ 

In either case, we have a subgroup of index 2 in $C(u)$ having $M$ as Sylow 2-subgroup. This proves Lemma 3.2.

**Lemma 3.4.** $K$ has a normal subgroup $L$ of index 2 with Sylow 2-subgroup

$$J = \langle a_1a_2, w \rangle.$$

**Proof.** We find the focal subgroup $M^*$ of $M$ in $K$. From (24) and Lemma 3.1, the derived subgroup of $M$ is

$$M' = \langle (a_1a_2)^r \rangle = \langle a_1a_2 \rangle.$$

Thus the subgroup $\langle v \rangle$ of order 2 in $M'$ is characteristic in $M$, and we have

$$N_K(M) \leq C_K(v) \leq C(u, v).$$

From (16), $C(u, v)$ has a normal 2-complement. Hence so has $N_K(M)$, so that $N_K(M) \cap M = M'$. By Grün's first theorem [8, Theorem 14.4.4], $M^*$ is the subgroup of $M$ generated by those elements of $M$ which are conjugate in $K$ to elements of $M'$. Since $A$ has no subgroup of index 2, $A \leq K$ and $M^*$ contains $A \cap M = \langle a_1a_2, w \rangle$, which we denote $J$. Since $T^* > J$. Then there exists an element of $M - J$ which is conjugate in $K$ to an element of $M'$, say

$$\langle a_1a_2 \rangle^r = (a_1^2)^r x,$$

where $s \in K$, $x \in J$, $(a_1^2)^r x \neq 1$. By taking a suitable power, we find that $v^r$ lies in $\langle a_1^2 \rangle J$, so that $v^r$ lies in $\langle uv \rangle J$, since $\langle uv \rangle J/J$ is the unique subgroup of order 2 in $\langle a_1^2 \rangle J/J$. Hence either

$$v^r = uvr \quad (r \in J), \text{ or } v^r \in J.$$

The second case can occur only when $v$ is an even power of $(a_1a_2)^l$, since an odd power of $(a_1^2)^k$ does not lie in $J$. Thus $v = ((a_1a_2)^l)^{2k}$. Then, $(a_1^2)^k x \in \langle uv \rangle J$. Now, $\langle a_1a_2 \rangle$ is a normal subgroup of $\langle uv \rangle J$, with elementary Abelian quotient group (of order 4). Hence, squaring, we find that

$$v^4 \in \langle a_1a_2 \rangle.$$
so that \( v^s = v \). Hence \( s \in C(u, v) \). Since \( \langle a_1a_2 \rangle \) is a normal subgroup of \( C(u, v) \), we have a contradiction to (25).

If the first case holds in (26), then \( (uv)^s = vr \). But \( vr \) is an involution in \( A \), and so is conjugate to \( w \), which lies in \( K_2 \). This is a contradiction, since \( uv \) lies in \( K_1 \). Hence \( M^* = J \). This proves the lemma.

**Lemma 3.5.** \( L = A \times E \), where \( E = \langle ((d_1d_2^{-1})^s)^{2^{a-1}} \rangle \), a cyclic group of order \( e \).

**Proof.** Since \( A \leq K \), \( |K : L| = 2^a \), and \( A \) has no subgroup of index 2, we must have \( A \leq L \). Since \( A \) contains a Sylow 2-subgroup of \( L \), \( L \) has no subgroup of index 2. The Sylow 2-subgroup \( J \) of \( L \) is dihedral of order \( 2^a \), and all involutions of \( L \) are conjugate in \( L \). We have

\[ C_L(v) \leq C(u, v), \]

which has an Abelian 2-complement, by (16). By a theorem of Gorenstein and Walter [7, Theorem I], \( L/O(L) \) is isomorphic with the alternating group \( A_7 \), or with \( PSL_2 (r) \), for some odd \( r \).

Since \( L/O(L) \) contains \( O(L)A/O(L) \), which is isomorphic with \( PSL_2 (q) \), it follows that either

\[ L/O(L) \simeq A_7, \quad q = 7 \text{ or } 9, \]
\[ L/O(L) \simeq PSL_2 (r), \quad \text{and } r \text{ is a power of } q \text{ or } q = 5, \]

by [4, p. 286] and the assumption that \( q > 3 \). We also have

\[ C_{L/O(L)}(vO(L)) = C_L(v)O(L)/O(L), \]

so that \( |C_{L/O(L)}(vO(L))| \) divides \( |C_L(v)| \), which divides \( |C(u, v)| \). This means that 24 divides \( 2(q - \delta)^2 \) if \( L/O(L) \simeq A_7 \), and \( r \pm 1 \) divides \( 2(q - \delta)^2 \) if \( L/O(L) \simeq PSL_2 (r) \). The only possibility is that \( L/O(L) \simeq PSL_2 (r) \), \( r = q \). Hence \( L = O(L)A \).

Since every four-subgroup of \( PSL_2 (q) \) is selfcentralizing, \( C_L(v, w)O(L)/O(L) \) has order 4, so that

\[ O(C_L(v, w)) \leq O(L). \]

From (16), (17) and (24), we have

\[ O(C_L(v, w)) = O(C(u, v, w)) = \langle ((d_1d_2^{-1})^s)^{2^{a-1}} \rangle. \]

Thus, \( |O(L)| \geq e \).

From the structure of \( PSL_2 (q) \),

\[ |C_{L/O(L)}(vO(L))| = q - \delta. \]

Now \( C_L(v) \) has \( J \) as Sylow 2-subgroup and contains the normal 2-complement of \( C(u, v) \), which has order \( e^2 \). Hence \( |C_L(v)| = 2^ae^2 = (q - \delta)e \). It follows that

\[ |C_{O(L)}(v)| = e. \]
Since $w$ and $vw$ are conjugate in $L$ to $v$, we also have
\[ |C_{O_{L}(w)}| = |C_{O_{L}(vw)}| = e. \]

We shall apply the following result of Brauer, and Gorenstein and Walter [1, p. 328]; [7, p. 555].

**Lemma 3.6.** Let $F$ be a four-group acting on a group $K$ of odd order. Let $t_1, t_2, t_3$ be the three involutions of $F$. Then
\[ |K| |C_F(K)|^2 = |C_F(t_1)| |C_F(t_2)| |C_F(t_3)|, \]
\[ K = C_F(t_1)C_F(t_2)C_F(t_3). \]

It follows immediately that $|O(L)| = e$, so that $O(L) = \langle ((d_1 d_2^{-1})^2)^{2n-1} \rangle$, which we denote $E$.

Now $C_L(E)$ is a normal subgroup of $L$ containing $E$ and the involution $v$. Since $L/E$ is simple, we must have $C_L(E) = L$, so that $L = A \times E$. This proves Lemma 3.5.

**Lemma 3.7.** The centralizer $C(u)$ of $u$ in $G$ is a semidirect product
\[ C(u) = \langle t, s \rangle (A \times E), \quad \langle t, s \rangle \cap (A \times E) = \{1\}, \]
where $A = PSL_2(q)$, $E$ is cyclic of order $e$, and $\langle t, s \rangle$ is dihedral of order $2n + 1$:
\[ t^2 = s^{2n} = 1, \quad s^4 = s^{-1}. \]

Here $u$ is the central involution of $\langle t, s \rangle$:
\[ u = s^{2n-1}. \]

The involution $t$ centralizes $A$ and inverts $E$, and the element $s$ centralizes $E$ and induces the same automorphism on $A$ as the element of $PGL_2(q)$ represented by the matrix
\[ \begin{bmatrix} 0 & \varepsilon \\ -1 & 0 \end{bmatrix} (\delta = 1), \quad \text{or} \quad \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} (\delta = -1). \]

**Proof.** By Lemmas 3.2, 3.4 and 3.5, $C(u) = \langle tu, a_x^2, A \times E \rangle$. We put
\[ s = a_x^k w(d_1 d_2)^k, \]
where $k$ is an integer, to be specified later. Since $w(d_1 d_2)^k$ lies in $A$, we have $C(u) = \langle tu, s, A \times E \rangle$. Using (9), (24) and Lemma 3.1, we can compute that
\[ s^2 = a_x^k (a_x^2)^{-1}. \]

It follows that $s^{2n-1} = (tv)^2 = u$. Thus we have
\[ C(u) = \langle t, s, A \times E \rangle. \]
Since transformation by \( uv \) interchanges \( a_1 \) and \( a_2 \), transformation by \( t = (uv)t \) interchanges \( a_1^2 \) and \( a_2^2 \). Thus,

\[
 s^2 s^t = a_1^2 (a_2^2)^{-1} a_2^2 w(d_1 d_2)^k = s,
\]

so that \( s^t = s^{-1} \) and \( \langle t, s \rangle \) is dihedral of order \( 2n + 1 \).

The subgroup \( L = A \times E \) is characteristic in \( K \), being the smallest normal subgroup of \( K \) having index a power of 2. Since \( K \) is normal in \( C(u) \), \( L \) is also normal in \( C(u) \). Since every normal subgroup of \( \langle t, s \rangle \) contains the central involution \( u \), but \( u \) does not lie in \( L \), we see that \( C(u) \) is a semidirect product (27).

We know that \( t \) centralizes \( A \), and that it transforms \( d_1^2 (d_2^2)^{-1} \) into \( d_2^2 (d_1^2)^{-1} = (d_2^2 (d_1^2)^{-1})^{-1} \), so that \( t \) inverts \( E \). Since \( a_1^2 \) centralizes \( d_2^2 (d_1^2)^{-1} \) and \( w(d_1 d_2)^k \) lies in \( A \), which centralizes \( E \), we see that \( s \) centralizes \( E \). It remains to find the action of \( s \) on \( A \), which is normal in \( C(u) \), being the derived group of \( L \).

Since \( t \) centralizes \( A \), \( s^3 = [t, s] \) also centralizes \( A \). Thus the automorphism \( \varphi \) of \( A \) induced by \( s \) satisfies

\[
 \varphi^2 = 1.
\]

Also, \( \varphi \) inverts \( (d_1 d_2)^s \), by (28) and Lemma 3.1, and transforms \( w \) into \( w(d_1 d_2)^{2k} \times (a_1 a_2)^s \). Since \( v \) is the unique involution in \( \langle (d_1 d_2)^s \rangle \), \( \varphi \) fixes \( v \). Since \( (d_1 d_2)^{2k} (a_1 a_2)^s \) is an odd power of \( d_1 d_2 \), \( w \) is not conjugate to \( w(d_1 d_2)^{2k} (a_1 a_2)^s \) in \( C_4(v) = \langle d_1 d_2, w \rangle \). Hence \( \varphi \) is not an inner automorphism of \( A \).

Identifying \( A = PSL_2(q) \) with its own inner automorphism group, we see that \( \varphi \) is an element of the automorphism group \( PGL_2(q) \) of \( A \) [5, pp. 90, 98], not contained in \( A \).

Suppose that \( \varphi \) does not belong to \( PGL_2(q) \). Then, by (29), \( \varphi \) is induced on \( A \) by a semilinear transformation relative to a field automorphism of order 2. This is possible only if \( q \) is a square, \( q = r^2 \). Then we have \( \delta = 1 \), so that \( (d_1 d_2)^s \) and \( w \) are elements of \( A = PSL_2(q) \) represented respectively by the matrices

\[
\begin{bmatrix}
\mu & 0 \\
0 & \mu^{-1}
\end{bmatrix}, \quad \begin{bmatrix}
0 & -1 \\
1 & 0
\end{bmatrix},
\]

where \( \mu \) is a generator of the multiplicative group of \( F_q \). If the matrix of the semilinear transformation inducing \( \varphi \) is \( R \), then the fact that \( \varphi \) inverts \( (d_1 d_2)^s \) means that

\[
R^{-1} \begin{bmatrix}
\mu^r & 0 \\
0 & \mu^{-r}
\end{bmatrix} R = \pm \begin{bmatrix}
\mu^{-1} & 0 \\
0 & \mu
\end{bmatrix}.
\]

Comparing eigenvalues, we see that \( \mu^r = \pm \mu \) or \( \pm \mu^{-1} \), whence

\[
\mu^{2(r-1)} = 1, \quad \text{or} \quad \mu^{2(r+1)} = 1.
\]
Thus $q - 1$ divides $2(r - 1)$ or $2(r + 1)$. If $r > 3$, then $q - 1 = (r - 1)(r + 1) > 2(r + 1)$. Hence $r = 3$, $q = 9$, $\mu^3 = -\mu^{-1}$, and

$$R^{-1} \begin{bmatrix} \mu^3 & 0 \\ 0 & \mu^{-3} \end{bmatrix} R = - \begin{bmatrix} \mu^{-1} & 0 \\ 0 & \mu \end{bmatrix} = \begin{bmatrix} \mu^3 & 0 \\ 0 & \mu^{-3} \end{bmatrix}.$$

It follows that $R$ has the form

$$R = \begin{bmatrix} c & 0 \\ 0 & 1 \end{bmatrix}.$$

Now $\varphi^2$ is the element of $\text{PSL}_2(q)$ represented by the matrix

$$\begin{bmatrix} c^3 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} c & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} c^4 & 0 \\ 0 & 1 \end{bmatrix},$$

so that $c^4 = 1$, i.e. $c$ is an even power of $\mu$. Now $\varphi$ transforms $w$ into the element of $\text{PSL}_2(q)$ represented by the matrix

$$R^{-1} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} R = \begin{bmatrix} 0 & -c^{-1} \\ c & 0 \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} c & 0 \\ 0 & c^{-1} \end{bmatrix}.$$

Since

$$\begin{bmatrix} c & 0 \\ 0 & c^{-1} \end{bmatrix}$$

is an even power of

$$\begin{bmatrix} \mu & 0 \\ 0 & \mu^{-1} \end{bmatrix},$$

this means that $\varphi$ transforms $w$ into $wx$, where $x$ is an even power of $(d_1d_2)^2$, and thus an even power of $d_1d_2$. But we have seen before that this is not so.

Thus $\varphi$ belongs to $\text{PGL}_2(q)$ but not to $\text{PSL}_2(q)$, and inverts $d_1d_2$. If $\psi$ is the element of $\text{PGL}_2(q)$ represented by the matrix

$$\begin{bmatrix} 0 & \delta \\ -1 & 0 \end{bmatrix} (\delta = 1),$$

or

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} (\delta = -1),$$

then $\psi$ does not lie in $\text{PSL}_2(q)$, and inverts $d_1d_2$. Thus $\varphi \psi^{-1}$ is an element of $\text{PSL}_2(q)$ lying in the centralizer of $d_1d_2$, which is $\langle d_1d_2 \rangle$ if $q > 5$. Then appropriate choice of the number $k$ in (28) gives $\varphi = \psi$. If $q = 5$ then $d_1d_2 = v$, whose centralizer in $A$ is $\langle v, w \rangle$. Then we compute that $w \psi$ and $vw \psi$ have order 4. Hence again $\varphi \psi^{-1}$ lies in $\langle v \rangle$ and we can obtain $\varphi = \psi$ by appropriate choice of $k$. This completes the proof of Lemma 3.7.

4. The $p$-structure of $G$. We shall determine the structure of the normalizer in $G$ of a Sylow $p$-subgroup, where $p$ is the characteristic of the field $F_q$. 
For $\alpha$ in $F_q$, we put
\[
\theta(\alpha) = \begin{bmatrix} 1 & 0 \\ \alpha & 1 \end{bmatrix}.
\]

The $\theta(\alpha)$ form a Sylow $p$-subgroup of $\text{SL}_2(q)$. Using the isomorphisms of Lemma 1.1 (ii) and writing $\theta_i(\alpha)$ for $\theta(\alpha)$, $(i=1, 2)$, we obtain Sylow $p$-subgroups of $L_1$ and $L_2$:
\[
P_i = \{\theta_i(\alpha) \mid \alpha \in F_q\} \quad (i=1, 2).
\]

The mapping $\alpha \rightarrow \theta_i(\alpha)$ is an isomorphism of the additive group of $F_q$ with $P_i$, so that $P_i$ is elementary Abelian of order $q$. The subgroup
\[
R = P_1P_2 = P_1 \times P_2
\]
is a Sylow $p$-subgroup of $C(t)$. By Lemma 3.7, the subgroup
\[
D_1 = \{\theta_1(\alpha)\theta_2(\alpha) \mid \alpha \in F_q\}
\]
is a Sylow $p$-subgroup of $C(u)$, elementary Abelian of order $q$. We shall also need the subgroup
\[
D_2 = \{\theta_1(\alpha)\theta_2(-\alpha) \mid \alpha \in F_q\}.
\]

Then $R$ also has direct product decompositions
\[
R = P_1D_1 = D_1D_2.
\]

We shall put
\[
h = \begin{bmatrix} e & 0 \\ 0 & e^{-1} \end{bmatrix},
\]

which is the same as $d$ when $\delta = 1$ but not when $\delta = -1$, and, using the isomorphisms of Lemma 1.1 (ii), form the subgroup
\[
H = \langle h_1, h_2 \rangle.
\]

Then $H$ is an Abelian subgroup of order $\frac{1}{2}(q-1)^2$, and we have
\[
h_1^{(q-1)/2} = h_2^{(q-1)/2} = t.
\]

The normalizer of $R$ in $C(t)$ is
\[
N(R) \cap C(t) = RH\langle u \rangle.
\]

We shall also put
\[
y = (sw)^{2n-2e}, \quad \text{or} \quad y = s^{2n-2e}
\]
according as \( \delta = 1 \) or \( \delta = -1 \), where \( s \) is the element of \( C(u) \) referred to in Lemma 3.7. Then the automorphism of \( A \) induced by \( y \) is the same as that induced by the matrix
\[
\begin{bmatrix}
i & 0 \\
0 & 1
\end{bmatrix} \quad \text{or} \quad \begin{bmatrix}
1 & 0 \\
0 & \pm 1
\end{bmatrix},
\]
according as \( \delta = 1 \) or \( \delta = -1 \), where \( i^2 = -1 \). Thus \( y \) has the following properties:

(41) \( y \in N(D_4) \),
(42) \( (h_1 h_2)^\nu = h_1 h_2 \); and \( w^\nu = wv \) if \( \delta = 1 \), \( w^\nu = w \) if \( \delta = -1 \).

Also, we can compute that

(43) \( y^2 = uv \) if \( \delta = 1 \); \( y^2 = u \) if \( \delta = -1 \);
(44) \( t^\nu = tu \), \( (tu)^\nu = t \).

Thus \( R^\nu \) is a Sylow \( p \)-subgroup of \( C(tu) \), and

(45) \( R \cap R^\nu = D_1 \).

We require the following result connecting \( R \), \( R^\nu \) and subgroups of the group \( E \) of Lemma 3.7.

**Lemma 4.1.** If \( \{1\} < F \leq E \), then \( N(F) \cap R = N(F) \cap R^\nu = D_1 \).

**Proof.** Clearly \( N(F) \cap R \geq D_1 \). Suppose that \( N(F) \cap R > D_1 \). Then, from (35), \( N(F) \cap P_1 > \{1\} \). Now \( \langle h_1 h_2 \rangle \) normalizes both \( F \) and \( P_1 \), so that it normalizes \( N(F) \cap P_1 \). But \( \langle h_1 h_2 \rangle \) acts irreducibly on \( P_1 \), since an element of \( \langle h_1 h_2 \rangle \) transforms \( \theta_i(\alpha) \) into \( \theta_i(\beta \alpha) \), where \( \beta \) can be any nonzero square in \( F_q \), and every element of \( F_q \) is a sum of squares. Thus \( N(F) \cap P_1 = P_1 \), so that

\[
N(F) \geq P_1 D_1 = R.
\]

Since \( F \) is cyclic, we have

\[
|\text{Aut } F| \leq |F| - 1 \leq e - 1 < q,
\]
since \( e \leq \frac{1}{2}(q + 1) \). Thus \( |N(F) \cap R : C(F) \cap R| < q \), so that \( |C(F) \cap R| > q \). Since \( C(F) \geq D_1 \), we have \( C(F) \cap R > D_1 \). Now the same argument as before shows that \( C(F) \geq P_1 \). Since \( A \leq C(F) \), \( C(F) \) contains all transforms of \( P_1 \) by elements of \( A \). Since these generate \( L_1 \), \( C(F) \) contains the element \( t \) of \( L_1 \). But \( t \) inverts \( F \), so that we have a contradiction. Hence \( N(F) \cap R = D_1 \). Transforming by \( y \), we have \( N(F) \cap R^\nu = D_1 \). This proves the lemma.

We now consider the centralizer of \( D_1 \) in \( G \).
Lemma 4.2. The group $C(D_1)$ has a normal 2-complement $M$, which is a semi-direct product

$$M = EQ, \quad Q \triangleleft M, \quad E \cap Q = \{1\},$$

where $Q = R^uR$, $|Q| = q^3$.

Proof. Since $C_d(D_1) = D_1$, we find from Lemma 3.7 that

$$C(D_1) \cap C(u) = D_1 \times \langle t, s^2 \rangle E.\quad (46)$$

The Sylow 2-subgroup $\langle t, s^2 \rangle$ of this group is dihedral of order $2^q$. Also, from the structure of $C(t)$, and (41) and (44), we have

$$C(D_1) \cap C(t) = R(t, u),\quad (47)$$
$$C(D_1) \cap C(tu) = R^u(t, u).\quad (48)$$

The argument of Lemma 2.1 shows that $\langle t, s^2 \rangle$ is a Sylow 2-subgroup of $C(D_1)$.

All involutions of $\langle t^2 \rangle$ are conjugate in $\langle t, s \rangle$ to $t$, and so are not conjugate to the involution $u$ of $\langle s^2 \rangle$. It follows (for example, by Lemma 3.3 and Burnside’s theorem) that $C(D_1)$ has a normal 2-complement $M$.

The four-subgroup $\langle t, u \rangle$ of $C(D_1)$ acts on $M$. By (46), (47) and (48), we have

$$C_M(u) = ED_1, \quad C_M(t) = R, \quad C_M(tu) = R^u.\quad (49)$$

By Lemma 3.6, we have $|M| = q^3$, $M = ER^uR$.

If $F$ is any nontrivial subgroup of $E$, then $\langle t, u \rangle$ acts on $N_M(F)$. Using (49) and Lemma 4.1, we find that

$$N_M(F) \cap C(u) = ED_1, \quad N_M(F) \cap C(t) = N_M(F) \cap C(tu) = D_1.$$

By Lemma 3.6, $N_M(F) = ED_1$, so that $F$ lies in the center of $N_M(F)$. It follows from Burnside’s theorem [8, Theorem 14.3.1] that $M$ has a normal $r$-complement for every prime divisor $r$ of $e$. Thus $M$ has a normal subgroup $Q$ of order $q^3$, which must be $R^uR$, and $M = EQ$. This proves the lemma.

We remark that $Q$ is characteristic in $M$, which is characteristic in $C(D_1)$, which is normal in $N(D_2)$, so that $Q$ is normal in $N(D_2)$, i.e.

$$N(D_1) \leq N(Q).\quad (50)$$

We shall prove that $Q$ is Abelian by considering the centralizer of $R$.

Lemma 4.3. The group $Q$ is elementary Abelian of order $q^3$, and is the normal 2-complement of the group $C(R)$. Also,

$$C(Q) = Q.\quad (51)$$

Proof. From the structure of $C(t)$, $C(R) \cap C(t) = R \langle t \rangle$. By the argument of Lemma 2.1, $\langle t \rangle$ is a Sylow 2-subgroup of $C(R)$, so that, by Burnside’s theorem, $C(R)$ has a normal 2-complement $K$. The four-group $\langle t, u \rangle$ normalizes $R$ and so
acts on $K$. We have $C_K(t) = R$. Since $C(u) \cap C(R) \subseteq C(u) \cap C(D_1)$, and since $C(R) \cap E = \{1\}$ by Lemma 4.1, we find from (46) that $C_K(u) = D_1$. Thus, $C_K(tu) \supseteq C_K(t, u) = D_1$.

Suppose that $C_K(tu) \cap R^u = D_1$. By (48), $R^u$ is the only Sylow $p$-subgroup of $C(tu)$ containing $D_1$, so that $D_1$ is a Sylow $p$-subgroup of $C_K(tu)$. Then Lemma 3.6 shows that $R$ is a Sylow $p$-subgroup of $K$. Now the Frattini argument and (39) show that

$$N(R) = C(R)(N(R) \cap C(t)) = C(R)H\langle u \rangle,$$

so that a Sylow $p$-subgroup of $C(R)$ is also a Sylow $p$-subgroup of $N(R)$. Thus $R$ is a Sylow $p$-subgroup of $N(R)$, so that $R$ is a Sylow $p$-subgroup of $G$, contradicting Lemma 4.2.

Hence $C_K(tu) \cap R^u > D_1$. By (35) and (41), $R^u = P_1^x D_1$, so that

$$C_K(tu) \cap P_1^x > \{1\}.$$

Now, elements of $\langle h_1, h_2 \rangle^u$ centralize $\langle t, u \rangle^v = \langle t, u \rangle$, and normalize $D_1^v = D_1$. In particular, $\langle h_1, h_2 \rangle^u$ must normalize the normal 2-complement $R$ of $C(D_1) \cap C(t)$. Thus $\langle h_1, h_2 \rangle^u$ normalizes $K$. Since $\langle h_1, h_2 \rangle^u$ normalizes $P_1^x$, it normalizes $C_K(tu) \cap P_1^x$.

Since $\langle h_1, h_2 \rangle^u$ acts irreducibly on $P_1^x$, we have $C_K(tu) \supseteq P_1^x$, so that

$$C_K(tu) \supseteq P_1^x D_1 = R^v.$$

Since $C(tu) \cap C(R) \subseteq C(tu) \cap C(D_1)$, it follows from (48) that $C_K(tu) = R^v$. Now Lemma 3.6 shows that $K = R^v R D_1 = R^v R = Q$.

Since $R$ and $R^v$ are elementary Abelian and $R^v \subseteq C(R)$, $Q$ is elementary Abelian. Since $C(Q) \subseteq C(R) = \langle t \rangle Q$, $C(Q) = Q$. This proves the lemma.

We remark that $Q$ is characteristic in $C(R)$ which is normal in $N(R)$, so that we have

(52) \hspace{1cm} N(R) \subseteq N(Q).

We now put

(53) \hspace{1cm} P_3 = D_3^y, \hspace{1cm} \theta_3(\alpha) = (\theta_1(\alpha) \theta_2(-\alpha))^y.

Then, by (35) and (41), $R^v = D_1 \times P_3$, so that

(54) \hspace{1cm} Q = P_1 \times P_2 \times P_3.

Since $C(Q) = Q$, $N(Q)/Q$ acts faithfully on $Q$. Since $H \subseteq N(Q)$ by (39) and (52), $H$ acts faithfully on $Q$. We now determine this action.

**Lemma 4.4.** The action of $H$ on $Q$ is given by

\[ h_1 : \theta_1(\alpha) \rightarrow \theta_1(e^2\alpha), \hspace{1cm} \theta_2(\alpha) \rightarrow \theta_2(\alpha), \hspace{1cm} \theta_3(\alpha) \rightarrow \theta_3(e\alpha), \]

\[ h_2 : \theta_1(\alpha) \rightarrow \theta_1(\alpha), \hspace{1cm} \theta_2(\alpha) \rightarrow \theta_2(e^2\alpha), \hspace{1cm} \theta_3(\alpha) \rightarrow \theta_3(e\alpha). \]
Proof. The actions of $h_1$ and $h_2$ on $\theta_1(\alpha)$ and $\theta_2(\alpha)$ are known, since these elements are contained in $C(t)$. Since $tu$ inverts $D_2$, (44) and (53) show that $t$ inverts $P_3$, so that $[t, Q] = P_3$. Since $H$ normalizes $Q$ and centralizes $t$, $H$ normalizes $P_3$.

We now write $Q$ additively instead of multiplicatively, and make it into a 3-dimensional vector space over $F_q$ by defining scalar multiplication as follows:

$$\lambda(\theta_1(\alpha) + \theta_2(\beta) + \theta_3(\gamma)) = \theta_1(\lambda \alpha) + \theta_2(\lambda \beta) + \theta_3(\lambda \gamma).$$

Since $h_1h_2: \theta_1(\alpha)\theta_2(-\alpha) \to \theta_1(\varepsilon^2 \alpha)\theta_2(-\varepsilon^2 \alpha)$, (42) and (53) imply that $h_1h_2: \theta_3(\alpha) \to \theta_3(\varepsilon^2 \alpha)$.

Thus the effect of $(h_1h_2)^m$ on $Q$ is multiplication by the scalar $\varepsilon^{2m}$. Since $h_1$, $h_2$ and $tu$ commute with $h_1h_2$, their action on $Q$ is additive and commutes with multiplication by square scalars. Since every element of $F_q$ is a sum of squares, $h_1$, $h_2$ and $tu$ induce linear transformations on $Q$. Representing these transformations by their matrices with respect to the basis $\theta_1(1)$, $\theta_2(1)$, $\theta_3(1)$ of $Q$, we have

$$h_1 \to \begin{bmatrix} \varepsilon^2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \mu \end{bmatrix}, \quad h_2 \to \begin{bmatrix} 1 & 0 & 0 \\ 0 & \varepsilon^2 & 0 \\ 0 & 0 & \nu \end{bmatrix}, \quad tu \to \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Since $h_1h_2$ induces multiplication by the scalar $\varepsilon^2$, and $tu$ transforms $h_1$ into $h_2$, we have

$$\mu \nu = \varepsilon^2, \quad \mu = \nu.$$

When $\delta = -1$, we cannot have $\mu = -\varepsilon$, since then $t = h_1^{(q-1)/2}$ would act trivially on $Q$, which is not so. When $\delta = 1$, nothing up to this point is changed if we replace $\varepsilon$ by $-\varepsilon$, which is another generator of the multiplicative group of $F_q$, and $s$ by $sv$. Thus in either case we may take $\mu = \nu = \varepsilon$, which yields the lemma.

We now consider the structure of $N(P_3)$.

Lemma 4.5. Let $V = O(C(P_3))$. Then

$$C(P_1) = L_2V, \quad N(P_3) = L_2V \langle h_1 \rangle.$$

The group $V/P_1$ is Abelian, and $V$ is nilpotent. Also,

$$Q \cap V = P_1P_3.$$

Proof. The centralizer of $P_1$ in $C(t)$ is

$$C(P_1) \cap C(t) = L_2P_1.$$

The Sylow 2-subgroup $\langle a_2, b_2 \rangle$ of this group is a generalized quaternion group. By the argument of Lemma 2.1, $\langle a_2, b_2 \rangle$ is a Sylow 2-subgroup of $C(P_1)$. By a
Theorem of Brauer and Suzuki [1, Theorem 2, p. 321], if \( V = O(C(P_1)) \), then \( C(P_1) \) has center \( \langle t \rangle V/V \). Thus \( \langle t \rangle V \) is normal in \( C(P_1) \). By the Frattini argument,

\[
C(P_1) = (C(P_1) \cap C(t))V = L_2V,
\]

since obviously \( P_1 \leq V \). Since \( C(P_1) \) is normal in \( N(P_1) \), we have, by the Frattini argument and the fact that \( \langle t \rangle \) is characteristic in \( \langle a_2, b_2 \rangle \),

\[
N(P_1) = C(P_1)(N(P_1) \cap C(t)) = L_2V\langle h_1 \rangle.
\]

Since \( C_P(t) = P_1 \), \( t \) acts without fixed point on \( V/P_1 \), so that \( V/P_1 \) is Abelian.

Since \( P_1 \leq Z(V) \), \( V \) is nilpotent (of class at most 2).

Suppose that \( x \) is an element of odd order in \( C(P_1) \) which is inverted by \( t \). Since \( t \) centralizes all elements of \( C(P_1) \) modulo \( V \), \( x \) must be an element of \( V \). Now \( t = (tu)^v \) inverts \( D_2 = P_3 \), so that we must have \( P_3 \leq V \). It follows that \( Q \cap V = P_1P_3 \).

This proves the lemma.

By considering \( C(P_3) \), we shall show that in fact \( V \) is a \( p \)-group.

**Lemma 4.6.** \( C(P_3) \) has a normal 2-complement, and

\[
O(C(P_3)) \leq QH.
\]

**Proof.** Suppose first that \( \delta = 1 \). Then the centralizer of \( D_2 \) in \( C(t) \) is

\[
C(D_2) \cap C(t) = R\langle t, u \rangle.
\]

If \( x \) is any involution, then, from the structures of \( C(t) \) and \( C(u) \), the centralizer in \( C(x) \) of any subgroup of order \( q \) has as Sylow 2-subgroup either a four-group or a generalized quaternion group. Now the argument of Lemma 2.1 shows that \( \langle t, u \rangle \) is a Sylow 2-subgroup of \( C(D_2) \). The involutions of \( \langle t, u \rangle \) are not all conjugate in \( C(D_2) \), since \( t \in K_1 \), \( tw \in K_2 \). Thus \( C(D_2) \) has a normal 2-complement, and so does \( C(P_3) = C(D_2)^\delta \).

Suppose now that \( \delta = -1 \). Then the centralizer of \( D_2 \) in \( C(t) \) is

\[
C(D_2) \cap C(t) = R\langle t \rangle,
\]

and \( \langle t \rangle \) is a Sylow 2-subgroup of \( C(D_2) \), so that \( C(D_2) \) and hence \( C(P_3) \) has a normal 2-complement.

In either case, the four-group \( \langle t, u \rangle \) normalizes \( D_2 \) and so acts on \( O(C(D_2)) \).

We have

\[
O(C(D_2)) \cap C(t) = R, \quad O(C(D_2)) \cap C(u) \geq D_1, \quad O(C(D_2)) \cap C(tu) \geq D_1.
\]

Now each Sylow \( p \)-subgroup of \( \text{PSL}_q(q) \) is contained in a unique largest odd order subgroup, the normal 2-complement of its normalizer, since every pair of distinct Sylow \( p \)-subgroups generates \( \text{PSL}_q(q) \). It follows that \( C(u) \) has a unique largest odd order subgroup containing \( D_1 \), and that this is contained in \( D_1\langle h_1h_2 \rangle E \). If \( C(D_2) \) contains an element \( xf \) of \( D_1\langle h_1h_2 \rangle E \), where \( x \in D_1\langle h_1h_2 \rangle, f \in E \), then \( C(D_2) \)
also contains \([t, xf]=f^2\). Then \(D_2\) normalizes \(\langle f^2 \rangle\), so that, by Lemma 4.1, \(f^2=1\), i.e. \(f=1\). Hence

\[ O(C(D_2)) \cap C(u) \leq D_1\langle h_1h_2 \rangle. \]

Also, \(C(tu)=C(t)^y\) has a unique largest odd order subgroup containing \(D_1^x=D_1\), and this is contained in \(R^yH^y\). Thus,

\[ O(C(D_2)) \cap C(tu) \leq R^yH^y. \]

By Lemma 3.6, we have \(O(C(D_2)) \leq R^yR^yH^y\), since \(\langle h_1h_2 \rangle=\langle h_1h_2 \rangle^y\). From (43), \(y^2\) normalizes \(R\) and \(H\), so that we have

\[ O(C(P_3)) = O(C(D_2))^y \leq R^yH = QH. \]

**Lemma 4.7.** \(V=O(C(P_1))\) is a \(p\)-group.

**Proof.** Applying Lemma 4.6, we find that

\[ C_V(P_3) \leq O(C(P_3)) \cap C(P_1) \leq Q\langle h_2 \rangle \leq L_2P_1P_3. \]

Hence \(C_V(P_3)=P_1P_3\). By nilpotency of \(V\), \(C_V(P_3)\) contains all \(p'\)-elements of \(V\). Hence \(V\) is a \(p\)-group. This proves the lemma.

We now set

\[ c = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}. \]

The element \(c_2\) of \(C(t)\) centralizes \(P_1\) and so normalizes \(V\). Hence, \(P_0^2 \leq V\). We put

\[ P_4 = P_0^2, \quad \theta_4(\alpha) = \theta_3(\alpha)^{c_2}. \]

By Lemma 4.4, \(h_1h_2^{-1}\) centralizes \(P_3\). Since \(c_2\) transforms \(h_1h_2^{-1}\) into \(h_1h_2\),

\[ h_1h_2 \in C(P_4). \]

Also by Lemma 4.4, and the assumption (13), \(h_1h_2\) acts without fixed point on \(P_1P_3\). Hence,

\[ P_1P_3 \cap P_4 = \{1\}, \quad V \geq P_1P_3P_4. \]

Since \(V/P_2\) is Abelian, \(P_4\) normalizes \(P_1P_3\), so that \(P_1P_3P_4\) is in fact a group. This shows that a Sylow \(p\)-subgroup of \(G\) has order at least \(q^4\). We shall prove

**Lemma 4.8.** \(V=P_1P_3P_4\). If \(U=P_2V=P_1P_2P_3P_4\), then

\[ N(U) \cap N(P_1) = UH \leq N(Q). \]

**Also,** \(P_1P_3\) is normal in \(U\), and \(U/P_1P_3\) is Abelian.

**Proof.** Consider first the case when \(\delta=1\). Then \(\langle t, v \rangle\) normalizes \(P_1\), and so acts on \(V\). We know that \(C_V(t)=P_1\). Since \(v=(h_1h_2)^{(q-1)/4}\) in this case, \(y\) commutes with \(v\), by (42). By (44), \((tv)^y=tv\). Since \(tuv\) centralizes \(D_2\), \(tv\) centralizes \(D_2^x=P_3\).
Then $P_3$ is a Sylow p-subgroup of $C(tv)$, since $tv$ lies in $K_2$. By Lemma 4.7, it follows that

$$C_v(tv) = P_3.$$ 

Since $c_2$ normalizes $V$ and transforms $tv$ into $v$, we have $C_v(v) = P_4$. By Lemma 3.6, $V = P_1P_3P_4$.

If $U = P_2V$, it now follows from Lemma 4.5 that

$$N(U) \cap N(P_4) = (N(P_2) \cap L_2\langle h_1 \rangle)V = P_2\langle h_1, h_2 \rangle V = UH.$$ 

Since $V/P_1$ is Abelian, $P_1P_3$ is normal in $V$. Also, $P_2$ centralizes $P_1P_3$. Hence $P_1P_3$ is normal in $U$. Since $tv$ inverts $P_2 \approx U/V$ and $C_v(tv) = P_3$, $tv$ acts without fixed point on $U/P_1P_3$, so that $U/P_1P_3$ is Abelian.

In particular, $Q = P_1P_2P_3$ is normal in $U$. By (39) and (52), $H \leq N(Q)$. Thus $UH \leq N(Q)$. This completes the proof of Lemma 4.8 in the case $\delta = 1$.

If $\delta = -1$, the above argument is not available since $v$ does not normalize $P_1$. However we can obtain the same result, and more information as well, by studying $N(Q)$.

**Lemma 4.9.** Let $\delta = -1$. Then,

$$N(Q)/Q = J \times Z,$$

where $J$ is isomorphic with $PGL_2(q)$, and $Z = \langle h_1h_2 \rangle Q/Q$, a cyclic group of order $\frac{1}{2}(q-1)$. $J$ contains the elements $tQ, uQ, yQ, h_1 h_2^{-1} Q$.

**Proof.** Let $W = O(N(Q))$. By (47) and (50), $\langle t, u \rangle \leq N(Q)$, so that $\langle t, u \rangle$ acts on $W$. Also, $y \in N(Q)$, by (41) and (50). Of course $W \geq Q$. We have

$$C_w(t) \geq C(t) = R, \quad C_w(u) \geq C(u) = D_1, \quad C_w(tu) = C_w(t)^y.$$ 

Now $R\langle h_1^2, h_1h_2 \rangle$ is the unique largest subgroup of odd order in $C(t)$ containing $R$, and $D_1\langle h_1h_2 \rangle E$ is the unique largest subgroup of odd order in $C(u)$ containing $D_1$.

Since $(h_1h_2)^y = h_1h_2$, it follows from Lemma 3.6 that

$$W \leq Q\langle h_1^2, h_1^2h_2, E \rangle.$$ 

By (50) and the fact that $D_1 = Q \cap C(u)$, we have

$$N(Q) \cap C(u) = N(D_1) \cap C(u) = \langle t, s \rangle D_1\langle h_1h_2 \rangle E.$$ 

The Sylow 2-subgroup $\langle t, s \rangle$ of this group is dihedral of order $2^s + 1$, with $u$ as its unique central involution. By the argument of Lemma 2.1, $\langle t, s \rangle$ is a Sylow 2-subgroup of $N(Q)$.

We know that a Sylow $p$-subgroup of $G$ has order at least $q^4$, so that $Q$ is not a Sylow $p$-subgroup of $G$, and hence not of $N(Q)$. However, $Q$ is a Sylow $p$-subgroup of $W$, by (58). Hence $|N(Q) : W|$ is divisible by $p$, so that $N(Q)$ does not have a normal 2-complement.
Not all the involutions of \( \langle t, s \rangle \) are conjugate in \( N(Q) \), since \( t \) and \( u \) are not conjugate in \( G \). This implies that \( N(Q) \) has a subgroup of index 2 and that \( u \) is conjugate in \( N(Q) \) to \( ts \). Now, using (59), we have

\[
C_{N(Q)/O}(uQ) = C_{N(Q)}(u)Q/Q = \langle t, s, h_1h_2, E \rangle Q/Q,
\]

which is isomorphic with \( \langle t, s, h_1h_2, E \rangle \), which has a normal Abelian 2-complement \( \langle h_1h_2, E \rangle \). By a theorem of Gorenstein and Walter [7, Theorem I],

\[
N(Q)/W \cong \text{PGL}_2(r),
\]

for some odd prime power \( r \).

Since the centralizer of an involution in \( \text{PGL}_2(r) \) is dihedral, and \( h_1h_2 \) lies in the center of \( \langle t, s, h_1h_2, E \rangle \), we must have \( h_1h_2 \in W \).

Suppose that \( W \cap E = F \{1\} \). Then, since \( W \) is solvable and \( F \) is a Hall subgroup of \( W \), there is a chief factor \( X \) of \( N(Q) \) in \( W \), covered by a subgroup of \( F \). Then \( X \) is centralized by \( u \) and hence by its conjugate \( ts \). But, \( ts \) inverts \( E \) and so inverts \( X \), so that we have a contradiction. Thus,

\[
W \cap E = \{1\}, \quad C_{N(Q)/W}(uW) \cong \langle t, s \rangle E.
\]

The order of \( \langle t, s \rangle E \) is \( 2^{n+1}e = 2(q+1) \). But, the structure of \( \text{PGL}_2(r) \) shows that its order must be \( 2(r+1) \) or \( 2(r-1) \). Thus, \( r = q \) or \( r = q + 2 \).

By (52), the fact that \( R = Q \cap C(t) \), and (39), we have

\[
N(Q) \cap C(t) = RH(u) = R\langle t, u \rangle \langle h_1^2, h_1h_2 \rangle.
\]

Since \( h_1h_2 \in W \), it follows that

\[
C_{N(Q)/W}(tW) \cong \langle t, u \rangle \langle h_1^2 \rangle/(\langle h_1^2 \rangle \cap W),
\]

whose order is a divisor of \( 2(q-1) \). By the structure of \( \text{PGL}_2(r) \), this order must be \( 2(r-1) \) or \( 2(r+1) \), so that \( r \leq q \). Hence we must have \( r = q \), so that

\[
N(Q)/W \cong \text{PGL}_2(q).
\]

Also, \( \langle h_1^2 \rangle \cap W = \{1\} \), and we have

\[
C_w(t) = R\langle h_1h_2 \rangle, \quad C_w(u) = D_1\langle h_1h_2 \rangle, \quad C_w(tu) = R^v\langle h_1h_2 \rangle,
\]

so that, by Lemma 3.6, \( W = Q\langle h_1h_2 \rangle \).

The Hall subgroup \( \langle h_1^2, h_1h_2 \rangle \) of \( N(Q) \) splits over \( \langle h_1h_2 \rangle \). It follows by a theorem of Gaschütz [8, Theorem 15.8.6] that \( N(Q)/Q \) splits over \( W/Q \): 

\[
N(Q)/Q = JZ, \quad J \cap Z = 1,
\]

where \( Z = W/Q, J \cong \text{PGL}_2(q) \). Now, \( Z \) is centralized by the involution \( tQ \), which corresponds to an involution of \( \text{PGL}_2(q) \) not lying in \( \text{PSL}_2(q) \). Since such an
involution and its conjugates generate $\text{PGL}_2(q)$, we see that $Z$ lies in the center of $N(Q)/Q$, so that

$$N(Q)/Q = J \times Z.$$  

Since $Z$ has odd order, $J$ must contain all elements of order 2 or 4 in $N(Q)/Q$. Thus $J$ contains $tQ, uQ, yQ$. We have

$$C_J(tQ) = \langle tQ, uQ, M \rangle,$$

where $MZ = \langle h_1^2, h_1h_2 \rangle Q/Q$. From the structure of $\text{PGL}_2(q)$, $uQ$ must invert $M$. We know that $uQ$ centralizes $Z$. Hence

$$M = [uQ, M] = [u, \langle h_1^2, h_1h_2 \rangle] Q/Q = \langle h_1h_2^{-1} \rangle Q/Q,$$  

so that $h_1h_2^{-1}$ lies in $J$. This completes the proof of Lemma 4.9.

**Lemma 4.10.** Let $\delta = -1$. One can choose a matrix representation of $J$ as $\text{PGL}_2(q)$ in such a way that, if $\eta(\alpha)$ is the element of $J$ represented by the matrix

$$\begin{bmatrix} 1 & 0 \\ \alpha & 1 \end{bmatrix},$$

then the action of the Sylow $p$-subgroup $P = \{ \eta(\alpha) \mid \alpha \in F_q \}$ of $J$ on $Q$ is given by

$$\eta(\alpha): \theta_1(\beta) \rightarrow \theta_1(\beta), \quad \theta_2(\beta) \rightarrow \theta_2(\alpha^2\beta)\theta_2(\beta)\theta_3(\mu\beta), \quad \theta_3(\beta) \rightarrow \theta_3(2\mu\alpha\beta)\theta_3(\beta),$$

where $\mu = \pm 1$. If $U_1$ is the subgroup of $N(Q)$ containing $Q$ such that $U_1/Q = P$, then $U_1$ is a Sylow $p$-subgroup of $G$ (of order $q^4$), $Q$ is the unique Abelian subgroup of order $q^3$ in $U_1$, $Z(U_1) = P_1$, and $P_1P_3$ is normal in $U_1$.

**Proof.** We write $Q$ additively and make it into a 3-dimensional vector space over $F_q$, as in the proof of Lemma 4.4. The action on $Q$ of the element $(h_1h_2)^nQ$ of $Z$ is multiplication by the scalar $e^{2n}$. Since $J$ centralizes $Z$, the action of $J$ on $Q$ is additive and commutes with multiplication by square scalars. Since all scalars are sums of squares, $J$ acts linearly on $Q$. We represent linear transformations on $Q$ by matrices with respect to the basis $\theta_1(1), \theta_2(1), \theta_3(1)$. From Lemma 4.4, we know the action on $Q$ of the elements $tQ, uQ, h_1h_2^{-1}Q$ of $J$:

$$tQ \rightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \quad uQ \rightarrow \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{bmatrix},$$

$$h_1h_2^{-1}Q \rightarrow \begin{bmatrix} e^2 & 0 & 0 \\ 0 & e^{-2} & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$  

In any 1-dimensional representation of $\text{PGL}_2(q)$, elements of $\text{PSL}_2(q)$ are represented by 1. Since $uQ$ corresponds in $J = \text{PGL}_2(q)$ to an element of $\text{PSL}_2(q)$
but one of the eigenvalues of the linear transformation on $Q$ corresponding to $uQ$ is $-1$, the representation of $J$ on $Q$ is not reducible into three 1-dimensional constituents.

The description by Brauer and Nesbitt [2, p. 588] of the irreducible representations of $\text{PGL}_2(q)$ over $F_q$ shows that the representation of $J$ on $Q$ is irreducible, and that, if a matrix representation of $J$ as $\text{PGL}_2(q)$ is taken, then $Q$ can be identified with the space of homogeneous polynomials of degree 2 in two variables $x_1$, $x_2$, the action on $Q$ of the element of $J$ represented by the matrix $A = [a_{ij}]$ being to transform

$$f(x_1, x_2) \rightarrow (\det A)^m f(x_1', x_2'),$$

where

$$x_i' = \sum_j \varphi(a_{ij})x_j,$$

where $\varphi$ is an automorphism of the field $F_q$ and $m$ is an integer such that diagonal matrices act trivially on $Q$, i.e. $\alpha^{2m}\varphi(\alpha)^2 = 1$ for all nonzero $\alpha$ in $F_q$.

If we replace the matrix $[a_{ij}]$ representing an element of $J$ by the matrix $[\varphi(a_{ij})]$, we have another matrix representation of $J$. Thus we can assume in (62) that $\varphi = 1$. Then we must have $m = -1$ or $q - 1 - 1$.

Since $uQ$ lies in $\text{PSL}_2(q)$, which has only one class of involutions, we can suppose that the matrix representation of $J$ is such that

$$uQ \sim \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

(where $\sim$ means "is represented by"). Since all involutions of the centralizer of $uQ$ which lie in $\text{PGL}_2(q) - \text{PSL}_2(q)$ are conjugate in the centralizer of $uQ$, we can assume that

$$tQ \sim \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

If $m = -1$, the subspace $[t, Q]$ of elements of $Q$ transformed by $tQ$ into their negatives would be the subspace spanned by $x_1^2$ and $x_2^2$. But, (61) shows that $[t, Q]$ is the 1-dimensional subspace $P_3$. Hence $m = \frac{1}{2}(q - 1) - 1$, and $P_3$ is the subspace spanned by $x_1x_2$. By choice of scale, we may take $\theta_3(1) = 2x_1x_2$. The subspace of vectors of $Q$ fixed by $uQ$ is the subspace spanned by $x_1^2 + x_2^2$. By (61), it is the subspace spanned by $\theta_1(1) + \theta_2(1)$. Hence,

$$\theta_1(1) + \theta_2(1) = \mu(x_1^2 + x_2^2),$$

for some scalar $\mu$. The subspace of vectors of $Q$ transformed into their negatives by $tuQ$ is spanned by $x_1^2 - x_2^2$ and also by $\theta_1(1) - \theta_2(1)$. Hence,

$$\theta_1(1) - \theta_2(1) = \nu(x_1^2 - x_2^2),$$

for some scalar $\nu$. 

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
Since \( h_1 h_2^{-1} Q \) is an element of odd order commuting with \( tQ \),

\[
h_1 h_2^{-1} Q \sim \begin{bmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{bmatrix},
\]

for some scalar \( \lambda \). Then \( h_1 h_2^{-1} Q \) transforms

\[
\begin{align*}
 x_1^2 + x_2^2 &\rightarrow \frac{1}{4}(\lambda^2 + \lambda^{-2})(x_1^2 + x_2^2) + \frac{1}{4}(\lambda^2 - \lambda^{-2})(x_1^2 - x_2^2), \\
 x_1^2 - x_2^2 &\rightarrow \frac{1}{4}(\lambda^2 - \lambda^{-2})(x_1^2 + x_2^2) + \frac{1}{4}(\lambda^2 + \lambda^{-2})(x_1^2 - x_2^2).
\end{align*}
\]

Substitution for \( x_1^2 + x_2^2 \) and \( x_1^2 - x_2^2 \) in terms of \( \theta_1(1) \) and \( \theta_2(1) \) and comparison with (61) shows that

\[
\lambda^2 + \lambda^{-2} = \varepsilon^2 + \varepsilon^{-2}, \quad \mu(\lambda^2 - \lambda^{-2}) = \nu(\varepsilon^2 - \varepsilon^{-2}).
\]

Since \( \lambda^2 + \lambda^{-2} - \varepsilon^2 - \varepsilon^{-2} = (\lambda^2 - \varepsilon^2)(1 - \varepsilon^{-2}) \), \( \lambda^2 = \varepsilon^2 \) or \( \lambda^2 = \varepsilon^{-2} \). Since a matrix and its negative represent the same element of \( \text{PGL}_2(q) \), we may take \( \lambda = \varepsilon \) or \( \lambda = \varepsilon^{-1} \). Since \( uQ \) centralizes \( tQ \) and \( uQ \), and inverts \( h_1 h_2^{-1} Q \), we may assume that \( \lambda = \varepsilon \), so that

\[
h_1 h_2^{-1} Q \sim \begin{bmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{bmatrix}.
\]

Now, \( \mu(\varepsilon^2 - \varepsilon^{-2}) = \nu(\varepsilon^2 - \varepsilon^{-2}) \), and \( \varepsilon^2 \neq \varepsilon^{-2} \), by the assumption that \( q > 3 \). Hence \( \mu = \nu \), so that

\[
\theta_1(1) = \mu x_1^2, \quad \theta_2(1) = \mu x_2^2.
\]

Since \( y^2 = u \), by (43), we have

\[
yQ \sim \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}.
\]

This transforms \( x_1^2 - x_2^2 \) into \( \pm 2x_1x_2 \). Since \( yQ \) transforms \( \theta_1(1) - \theta_2(1) \) into \( \theta_0(1) \), by (53), we have \( \mu = \pm 1 \).

If \( \eta(\alpha) \) is the element of \( J \) such that

\[
\eta(\alpha) \sim \begin{bmatrix} 1 & 0 \\ \alpha & 1 \end{bmatrix},
\]

then we can now compute that the action of \( \eta(\alpha) \) of \( Q \) is given by

\[
\eta(\alpha) \rightarrow \begin{bmatrix} 1 & 0 & 0 \\ \alpha^2 & 1 & \mu \alpha \\ 2\mu \alpha & 0 & 1 \end{bmatrix}.
\]

This is equivalent to the relations (60).

Let \( P \) be the group consisting of all the \( \eta(\alpha) \) and \( U_1 \) the subgroup of \( N(Q) \) containing \( Q \) such that \( U_1/Q = P \). If \( \alpha \neq 0 \), then the subgroup of vectors of \( Q \) left fixed
by $\eta(\alpha)$ is $P_1$. It follows that every Abelian subgroup of $U_1$ not contained in $Q$ must meet $Q$ in at most $P_1$, and so has order at most $q^3$. Hence $Q$ is the only Abelian subgroup of order $q^3$ in $U_1$, and also $Z(U_1) = P_1$. Also, the relations (60) imply that $P_1P_3$ is normal in $U_1$.

Since $Q$ is characteristic in $U_1$, $N(U_1) \leq N(Q)$. Since $U_1$ is a Sylow $p$-subgroup of $N(Q)$, we see that $U_1$ is a Sylow $p$-subgroup of $G$. Obviously $|U_1| = q^4$. This completes the proof of Lemma 4.10.

We can now prove Lemma 4.8 in the case $\delta = -1$. Since a Sylow $p$-subgroup of $G$ has order $q^4$, we must have $V = P_1P_3P_4$ since otherwise $P_2V$ would be a $p$-subgroup of $G$ (Lemma 4.7) of order greater than $q^4$. Since $U_1 \leq C(P_1)$, $U_1V$ is a $p$-subgroup of $G$, so that $U_1 \geq V$. Also, $P_2 \leq Q \leq U_1$. Hence $U = P_2V \leq U_1$, so that $U = U_1$. Since $P_1P_3$ is normal in $U$, $P_2$ and $P_4$ are Abelian, and $[P_2, P_4] \leq P_1P_3$ by (60), $U/P_2P_3$ is Abelian. As in the proof for the case $\delta = 1$, $N(U) \cap N(P_1) = UH$. Finally, $U = U_1 \leq N(Q)$ and $H \leq N(R) \leq N(Q)$, so that $UH \leq N(Q)$. This completes the proof of Lemma 4.8.

We now achieve the object of this section, by determining the structure of $UH$.

**Lemma 4.11.** The structure of $UH = P_1P_2P_3P_4H$ is determined by the relations

$$\begin{align*}
\theta_1(\alpha) &= \theta_2(\alpha), \\
\theta_2(\alpha) &= \theta_3(\alpha), \\
\theta_3(\alpha) &= \theta_4(\alpha) - 1,
\end{align*}$$

and the relations of Lemma 4.4, together with the known structure of $P_1, P_2, P_3, P_4$ and $H$. The group $U$ is a Sylow $p$-subgroup of $G$, and $N(U) = UH$.

**Proof.** Since $c_2$ centralizes $h_2$, inverts $h_2$, and transforms $\theta_3(\alpha)$ into $\theta_4(\alpha)$, we find from Lemma 4.4 that

$$h_1: \theta_4(\alpha) \rightarrow \theta_4(\alpha), \quad h_2: \theta_4(\alpha) \rightarrow \theta_4(\alpha^{-1}).$$

Now, $UH = QP_4H$, and $Q$ is a normal subgroup of $UH$. We have determined the action of $H$ on $Q$ in Lemma 4.4. We need to find the action of $P_4$ on $Q$.

By (57), $h_1h_2$ centralizes $P_4$. Making $Q$ into a 3-dimensional vector space over $F_4$ as in Lemma 4.4, we see that $P_4$ induces linear transformations on $Q$. Again we represent linear transformations by their matrices with respect to the basis $\theta_1(1), \theta_2(1), \theta_3(1)$.

Since $P_4 \leq Z(U)$ and $U/P_1P_3$ is Abelian, elements of $P_4$ fix elements of $P_1$ and fix all elements of $Q$ modulo $P_1P_3$. It follows that

$$\theta_4(\alpha) \rightarrow \begin{bmatrix} 1 & 0 & 0 \\ f(\alpha) & 1 & g(\alpha) \\ h(\alpha) & 0 & 1 \end{bmatrix},$$

where $f, g, h$ are functions from $F_4$ into itself, and the 1 in the last row follows from the fact that $\theta_4(\alpha)^p = 1$. 

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
Using (56), (63), and the fact that \( c_2^2 = t \) inverts \( P_3 \), we compute that

\[
c_2 \theta_2(1) : \theta_3(\alpha) \to \theta_1(\theta_3(-\alpha)) \theta_3(g(-\alpha)) \theta_3(\alpha), \quad \theta_4(\alpha) \to \theta_3(-\alpha).
\]

Then we compute, using (63), that

\[
(c_2 \theta_2(1))^3 : \theta_4(\alpha) \to \theta_1(k(\alpha)) \theta_3(r(\alpha)) \theta_3(g(\alpha)),
\]

where \( k(\alpha) = f(\alpha) + f(-g(\alpha)) + h(-g(\alpha)) \alpha \), \( r(\alpha) = g(-g(\alpha)) + \alpha \). But, computation using (30) and (55) shows that

\[
(c_2 \theta_2(1))^3 = 1.
\]

It follows that \( k(\alpha) = r(\alpha) = 0 \), and, in particular, that \( g(\alpha) = \alpha \).

In the case \( \delta = -1 \), comparison with Lemma 4.10 now shows that \( \theta_4(\alpha) \) belongs to the coset \( \eta(\mu \alpha) \) of \( U/Q \). Then Lemma 4.10 determines the action of \( \theta_4(\alpha) \) on \( Q \), and we obtain the relations stated in the lemma.

Now let \( \delta = 1 \). We have already shown that \( \theta_4(\alpha) h_1 = h_1 \theta_4(\alpha) \). Taking the matrices of the corresponding linear transformations on \( Q \), by Lemma 4.4 and (63), we find that

\[
f(\epsilon \alpha) = \epsilon^2 f(\alpha).
\]

Since \( \epsilon \) is a generator of the multiplicative group of \( F_q \), this implies that

\[
f(\beta \alpha) = \beta^2 f(\alpha),
\]

for \( \beta \neq 0 \). Setting \( \alpha = 1 \) and then replacing \( \beta \) by \( \alpha \), we have \( f(\alpha) = ma^2 \), for \( \alpha \neq 0 \), where \( m = f(1) \). This formula holds also for \( \alpha = 0 \), since \( \theta_4(0) = 1 \).

The relation \( \theta_4(1) \theta_4(\alpha) = \theta_4(1 + \alpha) \) implies that

\[
f(1 + \alpha) = f(1) + f(\alpha) + h(\alpha),
\]

so that we have \( h(\alpha) = 2ma \).

To determine \( m \), we compute in \( C(t) \) that

\[
(t w \theta_3(1) \theta_2(-1))^3 = 1.
\]

Transforming by \( y c_2 \), we obtain the equation

\[
(t w \theta_3(1))^3 = 1.
\]

We calculate that

\[
t w \theta_3(1) \to \begin{bmatrix} -m & -1 & -1 \\ -1 & 0 & 0 \\ -2m & 0 & -1 \end{bmatrix}.
\]

Cubing, we find that \( m = -1 \), so that

\[
\theta_4(\alpha) \to \begin{bmatrix} 1 & 0 & 0 \\ -\alpha^2 & 1 & \alpha \\ -2\alpha & 0 & 1 \end{bmatrix},
\]
and we have determined the action of $P_4$ on $Q$. This gives the relations of the lemma.

It follows from our relations that $Z(U) = P_1$. Hence $N(U) \leq N(P_1)$, so that Lemma 4.8 implies that $N(U) = UH$. Since $U$ is a Sylow $p$-subgroup of $UH$, it follows that $U$ is a Sylow $p$-subgroup of $G$. This completes the proof of Lemma 4.11.

5. The $(BN)$-pair. The action of $u$ on $Q = P_1P_2P_3$ and the action of $c_2$ on $V = P_1P_2P_4$ are given as follows.

**Lemma 5.1.**

\[
u: \theta_1(a) \to \theta_2(a), \quad \theta_2(a) \to \theta_1(a), \quad \theta_3(a) \to \theta_3(-a),
\]

\[
c_2: \theta_1(a) \to \theta_1(a), \quad \theta_3(a) \to \theta_4(a), \quad \theta_4(a) \to \theta_3(-a).
\]

**Proof.** The action of $u$ on $P_1P_2$ is given by the structure of $C(t)$. Since $u$ inverts $D_2$, $u = u^v$ also inverts $D_2 = P_3$.

By the structure of $C(t)$, $c_2$ centralizes $P_1$; and $c_2$ transforms $\theta_3(a)$ into $\theta_4(a)$ by the definition (56). Finally, $c_2^2 = t$ inverts $P_3$, so that $c_2$ transforms $\theta_4(a)$ into $\theta_3(-a)$. This proves the lemma.

The normalizer of $H$ in $C(t)$ is the group

\[(64) \quad N = \langle H, u, c_2 \rangle.
\]

This is in fact the normalizer of $H$ in $G$, since $\langle t \rangle$ is characteristic in $H$, being the group of $\frac{1}{2}(q-1)$th powers of elements of $H$.

**Lemma 5.2.** The structure of $N = \langle H, u, c_2 \rangle$ is determined by the relations

\[h_1^{q-1/2} = h_2^{q-1/2} = c_2^2 = t, \quad t^2 = u^2 = 1,
\]

\[[h_1, h_2] = [h_1, c_2] = 1, \quad h_1^u = h_2, \quad h_2^{c_2} = h_2^{-1}, \quad (uc_2)^4 = 1.
\]

The group $W = N/H$ is dihedral of order 8.

**Proof.** This is all computation within $C(t)$. The group $W = N/H$ is dihedral of order 8 because of the relations $u^2 = 1$, $c_2^2 \in H$, $(uc_2)^4 = 1$.

Now set

\[r_1 = uH, \quad r_2 = c_2H.
\]

Then $r_1$ and $r_2$ are involutions generating $N/H = W$. The elements of $W$, written in shortest possible form in terms of $r_1$ and $r_2$, are

\[1, \quad r_1, \quad r_2, \quad r_1r_2, \quad r_2r_1, \quad r_1r_2r_1, \quad r_2r_1r_2, \quad r_1r_2r_1r_2.
\]

For $\sigma$ in $W$, let $\lambda(\sigma)$ be the number of factors $r_i$ when $\sigma$ is expressed in the shortest form as above. Set $\omega(r_1) = u$, $\omega(r_2) = c_2$, and, for $\sigma = r_{i_1}\cdots r_{i_k}$, set $\omega(\sigma) = \omega(r_{i_1}) \cdots \omega(r_{i_k})$. Then $\sigma = \omega(\sigma)H$. If $K$ is any subgroup containing $H$, we write $\sigma K$ and $K\sigma$ for the
cosets $\omega(\sigma)K$ and $K\omega(\sigma)$. If $K$ is any subgroup normalized by $H$, we write $K^\sigma$ for $K^{\omega(\sigma)}$. We set
\[(65)\quad B = UH.\]
Clearly $B \cap N = H$.

**Lemma 5.3.** Let $G_i = S \cup B_i B$, $i = 1, 2$. Then $G_1$ and $G_2$ are subgroups of $G$.

**Proof.** Since $G_i G_i = S \cup B_i B \cup B_i B_i B$ and $r^2 = 1$, it is enough to prove that $B^i \subseteq B \cup B_i B$.

Since $u = \omega(r_1)$ normalizes $P_1 P_2 P_3 H$ and $c_2 = \omega(r_2)$ normalizes $P_1 P_3 P_4 H$, it is enough to show that
\[P_4^i \subseteq B \cup B_1 B, \quad P_2^i \subseteq B \cup B_2 B.\]

As is well known, e.g. [3, p. 34], $L_2 \cong \text{SL}_2(q)$ has the Bruhat decomposition
\[L_2 = B_2 \cup B_2 c_2 B_2,\]
where $B_2 = P_2(h_2) S B$. Hence $P_2^i = P_2^i \subseteq L_2 \subseteq B \cup B_2 B$.

For $x$ in $\text{SL}_2(q)$, set
\[\bar{x} = f^{-1} x f, \quad \text{where} \quad f = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.\]

Then
\[A_1 = \left\{ x_1 \bar{x}_2 \mid x \in \text{SL}_2(q) \right\}\]
is a subgroup of $C(\gamma)$ isomorphic with $\text{PSL}_2(q)$, an isomorphism being provided by the correspondence associating $x_1 \bar{x}_2$ with the element of $\text{PSL}_2(q)$ represented by the matrix $x$. The matrices
\[\begin{bmatrix} 1 & 0 \\ \alpha & 1 \end{bmatrix}\]
of $\text{SL}_2(q)$ give a Sylow $p$-subgroup $D_2$ of $A_1$, whose normalizer in $A_1$ is
\[B_1 = D_2 \langle h_1 h_2 \rangle,\]
since $h_2 = h_2$. Since $\bar{c}_2 = tc_2$, the Bruhat decomposition of $\text{SL}_2(q)$ leads to the decomposition
\[A_1 = B_1 \cup B_1 t c_1 c_2 B_1.\]

In particular, $D_2^x \subseteq B_1 \cup B_1 t c_1 c_2 B_1$.

Now, $D_2^x = P_4$, $(h_1 h_2)^x = h_1 h_2^{-1}$, and $(tc_1 c_2)^x = tuw$ or $u$ according as $\delta = 1$ or $\delta = -1$. If $\delta = 1$, $tu \in H$ so that $tuw \equiv u \pmod{H}$. Then,
\[P_4^i \subseteq (B_1 \cup B_1 t c_1 c_2 B_1)^x \subseteq B \cup B_1 B,\]
since $B_1^x = P_4 \langle h_1 h_2^{-1} \rangle \subseteq B$. This proves the lemma.
**Lemma 5.4.** If $\sigma \in W$, $i = 1$ or 2, and $\lambda(r_i \sigma) \geq \lambda(\sigma)$, then $r_i B \sigma \subseteq Br_i \sigma B$.

**Proof.** Since $u$ normalizes $P_1 P_2 P_3 H$ and $c_2$ normalizes $P_1 P_3 P_4 H$, it is enough to show that

$$uP_4\omega(\sigma) \subseteq u\omega(\sigma)B \quad \text{if} \quad \lambda(r_3 \sigma) \geq \lambda(\sigma),$$

$$c_2 P_2 \omega(\sigma) \subseteq c_2 \omega(\sigma)B \quad \text{if} \quad \lambda(r_2 \sigma) \geq \lambda(\sigma).$$

There are eight cases to examine, all easily verified by using Lemma 5.1. For example, when $i = 1$, $\sigma = r_2 r_1$,

$$uP_4 c_2 u = uc_2 P_3 u = uc_2 u P_3.$$

Seven more such verifications complete the proof of the lemma.

**Lemma 5.5.** The set $G_0 = BNB$ is a subgroup of $G$, and $G_0$ is the disjoint union of the eight double cosets $B \sigma B$, $\sigma \in W$.

**Proof.** This follows from Lemmas 5.3 and 5.4 by a theorem of Tits [16].

**Lemma 5.6.** $U \cap U^* t^2 = \{1\}$.

**Proof.** Let $m = \omega(r_1 r_2 r_1 r_2) = (uc_2)^2 = c_1 c_2$, and set

$$D = U \cap U^m.$$

Since $m$ normalizes $H$, and $H$ normalizes $U$,

$$D^H \subseteq U^H \cap U^{mH} = U^H \cap U^{Hm} = U \cap U^m = D,$$

so that $H$ normalizes $D$. Since $C_\nu(t) = R$ and $R \cap R^m = \{1\}$,

$$C_D(t) = \{1\}.$$

Hence $t$ inverts $D$. The subgroup of $Q$ inverted by $t$ is $P_3$, so that

$$D \cap Q \leq P_3.$$

Also, $C_\nu(tu) = R^\nu$ and $R^\nu \cap R^{\nu m} = R^\nu \cap R^{m \nu} = (R \cap R^m)^\nu = \{1\}$, since $ym = my$ if $\delta = -1$, and $ym = vmy$ if $\delta = 1$. Thus,

$$C_D(tu) = \{1\}.$$

Since $P_3 \leq C(tu)$, we have $D \cap Q = \{1\}$.

Let $d \in D$. Then $d = mn$, where $m \in P_4$, $n \in Q$. Since $h_1 h_2$ centralizes $P_4$ and normalizes both $D$ and $Q$, we see that

$$[n, h_1 h_2] = [d, h_1 h_2] \in D \cap Q,$$

so that $h_1 h_2$ commutes with $n$. Since $h_1 h_2$ acts without fixed point on $Q$, $n = 1$. Thus, $D \leq P_4$. Since $H$ acts irreducibly on $P_4$, either $D = \{1\}$ or $D = P_4$. 

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
Since $m^2 = 1$, $m$ normalizes $D$. If $D \neq \{1\}$, then $m$ induces an automorphism of $P_4$, say
\[ m: \theta_4(\alpha) \mapsto \theta_4(f(\alpha)). \]
Now, $h_1 m = mh_1^{-1}$, and we know the action of $\langle h_1 \rangle$ on $P_4$, by Lemma 4.11. This implies that
\[ f(e \alpha) = e^{-1}f(\alpha). \]
Since $e$ generates the multiplicative group of $F_q$, we have
\[ f(\beta \alpha) = \beta^{-1}f(\alpha) \]
for $\beta \neq 0$, so that $f(\beta) = \gamma \beta^{-1}$, where $\gamma = f(1)$. Since $m$ induces an automorphism of $P_4$, we have $\gamma \neq 0$, and
\[ f(\alpha + \beta) = f(\alpha) + f(\beta). \]
Hence, whenever $\alpha, \beta, \alpha + \beta$ are all nonzero,
\[ (\alpha + \beta)^{-1} = \alpha^{-1} + \beta^{-1}. \]
Take $\beta = 1$ and clear fractions. Then every nonzero element $\alpha$ of $F_q$ different from $-1$ must satisfy the equation
\[ \alpha^2 + \alpha + 1 = 0. \]
This is impossible since $q > 4$. Hence $D = \{1\}$ and we have proved the lemma.

**Lemma 5.7.** For each element $\sigma$ of $W$,
\[ U = U_\sigma U'_\sigma, \quad \omega(\sigma)U_\sigma\omega(\sigma)^{-1} \subseteq U^{r_1 t_2 r_1 t_2}, \quad \omega(\sigma)U'_\sigma\omega(\sigma)^{-1} \subseteq U, \]
where $U_\sigma$ and $U'_\sigma$ are subgroups of $U$ given by the table

<table>
<thead>
<tr>
<th>$\sigma$</th>
<th>1</th>
<th>$r_1$</th>
<th>$r_2$</th>
<th>$r_1 r_2$</th>
<th>$r_2 r_1$</th>
<th>$r_1 r_2 r_1 r_2$</th>
<th>$r_2 r_1 r_2 r_1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$U_\sigma$</td>
<td>${1}$</td>
<td>$P_4$</td>
<td>$P_2$</td>
<td>$P_2 P_3$</td>
<td>$P_1 P_4$</td>
<td>$P_1 P_4 P_3$</td>
<td>$P_1 P_2 P_3$</td>
</tr>
<tr>
<td>$U'_\sigma$</td>
<td>$U$</td>
<td>$P_1 P_2 P_3$</td>
<td>$P_1 P_3 P_4$</td>
<td>$P_1 P_4$</td>
<td>$P_2 P_3$</td>
<td>$P_2$</td>
<td>$P_4$</td>
</tr>
</tbody>
</table>

**Proof.** This is straightforward computation, using Lemma 5.1. For example, $(P_2 P_3)^{r_1 t_2} = (P_1 P_3)^{t_2} = P_1 P_4$, so that
\[ \omega(r_1 r_2)P_1 P_4 \omega(r_1 r_2)^{-1} = P_2 P_3 \subseteq U, \]
and
\[ \omega(r_1 r_2)P_2 P_3 \omega(r_1 r_2)^{-1} = P_1 P_4 \omega(r_1 r_2 r_1 r_2)^{-1} = P_1 P_2 P_3 \subseteq U^{r_1 t_2 r_1 t_2}. \]

**Lemma 5.8.** Every element of $G_\sigma$ has a unique expression in the form $b \omega(\sigma)x$, where $b \in B$, $\sigma \in W$, $x \in U_\sigma$. The order of $G_\sigma$ is equal to the order of $\text{PSp}_4(q)$.
Proof. By using Lemmas 5.6, 5.7, we prove the existence and uniqueness of the "normal form" in the usual way [3, p. 42]. It follows that \(|B \sigma B| = |B| \cdot |U_2|\), so that

\[
|G_0| = |B| \sum_{\sigma \in \mathcal{W}} |U_2| = \frac{1}{2}q^4(q-1)^2(1+q+q^2+q^2+q^3+q^4)
\]

\[
= \frac{1}{2}q^4(q-1)^2(q+1)^2(q^2+1) = |\text{PSp}_4(q)|.
\]

This proves the lemma.

Lemma 5.9. \(G_0\) is isomorphic with \(\text{PSp}_4(q)\).

Proof. Given two elements of \(G_0\) in normal form, the normal form of their product is uniquely determined, by Lemmas 4.11, 5.1, 5.2, 5.3, 5.4, 5.7 and 5.8 (cf [12, §8]). Thus the multiplication table of \(G_0\) is uniquely determined. Since \(\text{PSp}_4(q)\) satisfies the hypothesis of the theorem and the condition (10), we see that \(\text{PSp}_4(q)\) has a subgroup isomorphic with \(G_0\). By the equality of the orders, \(G_0\) is isomorphic with \(\text{PSp}_4(q)\).

An alternative method of proving this lemma which does not require the structure of \(UH\) and the action of \(u\) and \(c_2\) on \(Q\) and \(V\) to be known with the exactness of Lemmas 4.11 and 5.1 can be given, by using a theorem of Higman. By Lemmas 5.3, 5.4,

\[
G_2 = \sigma G_2 \cap G_2 \sigma \cap G_2 \sigma \sigma, \quad G_2 = \sigma G_2 \cap G_2 \sigma \cap G_2 \sigma \sigma,
\]

so that \(G_0\) is decomposed into 3 double cosets

\[
G_0 = G_2 \cup G_2 \sigma G_2 \cup G_2 \sigma \sigma \sigma G_2.
\]

This means that the transitive permutation representation of \(G_0\) on the right cosets of \(G_2\) has rank 3 in the sense of Higman [9], i.e. \(G_2\) has three orbits. These orbits have lengths

\[
1, \quad |G_2 \sigma G_2| \big/ |G_2| = q(q+1), \quad |G_2 \sigma \sigma G_2| \big/ |G_2| = q^3.
\]

If the kernel of the permutation representation of \(G_0\) is \(K\), suppose that \(K \cap P_1 > \{1\}\). Since \(H\) acts irreducibly on \(P_1\), \(K \geq P_1\). Hence \(K \geq P_1 = P_2, K \geq D_2\). Hence \(K \geq D_2\) = \(P_3\), and \(K \geq P_3 = P_4\). Thus \(K \geq U\). By Lemma 4.11 and the Frattini argument, \(G_0 = KH \leq G_2\), a contradiction. Thus \(P_1\) is represented faithfully. From Lemma 5.8, every right coset of \(G_2\) in \(G_2 \sigma G_2\) has the form \(G_2 \sigma_1 x\) or \(G_2 \sigma_2 x\), where \(x \in U\). Since \(P_1\) is in the center of \(U\) and lies in \(U_1\) and \(U_1^{\sigma_1}\), it follows that every element of \(P_1\) fixes every right coset of \(G_2\) in \(G_2 \sigma G_2\). By [9, Theorem 2, p. 154], \(G_0\) has \(\text{PSp}_4(q)\) as a chief factor, and so \(G_0\) is isomorphic with \(\text{PSp}_4(q)\), by equality of orders.

Lemma 5.10. \(G_0 = G\).
Proof. Since $\text{PSp}_4(q)$ satisfies the hypothesis of the theorem, and the condition (10), $G_0$ possesses all the properties found for $G$. In particular, $G_0$ has two classes of involutions, and the centralizer in $G_0$ of an involution has order $q^2(q^2 - 1)^2$ or $q(q^2 - 1)(q - \delta)$, depending on whether or not it lies in the center of a Sylow 2-subgroup of $G_0$. Since $G_0$ contains $t$ and $u$, involutions of $K_1$ and $K_2$, the classes of involutions in $G_0$ must be

$$K'_1 = K_1 \cap G_0, \quad K'_2 = K_2 \cap G_0.$$ 

Since Sylow 2-subgroups of $G_0$ are Sylow 2-subgroups of $G$, $K'_2$ must consist of the involutions of $G_0$ which do not lie in the center of a Sylow 2-subgroup, so that $K'_1$ must consist of those which do. If $x$ is any involution of $G_0$, we see now that $C_{G_0}(x) = C(x)$. Since $G$ has two classes of involutions, $G_0$ must contain all the involutions of $G$ [14, Lemma 1, p. 144]. In particular, $K'_1 = K_1$, so that

$$|G_0| = |K'_1| |C_{G_0}(t)| = |K_1| |C_G(t)| = |G|.$$

Thus, $G_0 = G$.

This completes the proof of the theorem.

REFERENCES

15. J. G. Thompson, Nonsolvable finite groups all of whose local subgroups are solvable, Bull. Amer. Math. Soc. 74 (1968), 383-437.

UNIVERSITY OF NOTRE DAME,
NOTRE DAME, INDIANA