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

BY
W. J. WONG[1]

In this paper we present a characterization of the projective symplectic groups $\mathrm{PSp}_4(q)$ in dimension 4 over finite fields of odd characteristic, in terms of the structure of the centralizer of an involution. The group $\mathrm{PSp}_4(q)$ is simple, of order $\frac{1}{2}q^4(q^2+1)(q^2-1)^2$, 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* $\mathrm{PSp}_4(q)$ *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* $\mathrm{PSp}_4(q)$.

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

A similar characterization of $\mathrm{PSp}_4(q)$ 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 $\mathrm{PSp}_4(q)$. 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 $y\colon x \to z$. If $y\colon x \to x^{-1}$, 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^2}, we shall always mean the norm from F_{q^2} 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 δ by the conditions

$$q \equiv \delta \pmod 4), \quad \delta = \pm 1. \tag{1}$$

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

$$q-\delta = 2^n e, \quad e \text{ odd}. \tag{2}$$

We fix a generator ε 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 $\mathrm{PSp}_4(q)$ 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 $\mathrm{PSp}_4(q)$ 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 $A, B \in \mathrm{SL}_2(q)$. Setting

$$L_1 = \left\{ \begin{bmatrix} A & 0 \\ 0 & I \end{bmatrix} \,\middle|\, A \in \mathrm{SL}_2(q) \right\}, \qquad L_2 = \left\{ \begin{bmatrix} I & 0 \\ 0 & B \end{bmatrix} \,\middle|\, B \in \mathrm{SL}_2(q) \right\},$$

$$u = \begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix},$$

we see that L_1 and L_2 are isomorphic with $\mathrm{SL}_2(q)$, elements of L_1 commute with elements of L_2, $L_1 \cap L_2 = \langle t \rangle$, $C = L_1L_2\langle u \rangle$, $u^2 = 1$, $L_1^u = L_2$. Since $\mathrm{SL}_2(q)$ has center of order 2 it follows easily that C has center $\langle t \rangle$.

Since C has order

$$|C| = |\mathrm{SL}_2(q)|^2 = q^2(q^2-1)^2,$$

the index of C in $\mathrm{PSp}_4(q)$ 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 $S = S_1S_2\langle u \rangle$, where S_1 is a Sylow 2-subgroup of L_1, $S_2 = S_1^u$. We construct the S_i as follows. Let

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

where in the second case α and β are elements of F_q 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 $\mathrm{SL}_2(q)$, generating a subgroup whose normalizer is $\langle d, b \rangle$, where

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

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

$$a = d^e, \tag{5}$$

then $\langle a, b \rangle$ is a Sylow 2-subgroup of $\mathrm{SL}_2(q)$, 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 $\mathrm{SL}_2(q)$ 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

$$\begin{gathered} S = \langle a_1, b_1, a_2, b_2, u \rangle, \\ a_i^{2^{n-1}} = b_i^2 = t, \qquad a_ib_i = b_ia_i^{-1}, \\ [a_1, a_2] = [a_1, b_2] = [b_1, a_2] = [b_1, b_2] = 1, \\ a_1^u = a_2, \qquad b_1^u = b_2. \end{gathered} \tag{6}$$

The order of S is 2^{2n+2}. Since a generalized quaternion group has center of order 2, it follows easily that S has center $\langle t \rangle$. Thus the involutions lying in the centers of Sylow 2-subgroups form a single conjugacy class and their centralizers are all isomorphic.

Every involution of L_1L_2 different from t is of the form xy, where x and y are elements of order 4 in L_1 and L_2 respectively. Since all elements of order 4 in $\mathrm{SL}_2(q)$ are conjugate, we see that all involutions of L_1L_2 different from t are conjugate in L_1L_2.

If x and y are elements of L_1 and L_2 respectively, then

$$(uxy)^2 = (y^u x)(x^u y),$$

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

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) *$C = L_1 L_2 \langle u \rangle$, where L_1 and L_2 are subgroups of C, such that*

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

u is an involution, and there are isomorphisms

$$x \to x_1, \qquad x \to x_2,$$

of $\mathrm{SL}_2(q)$ *on L_1 and L_2 respectively, such that*

$$x_1^u = x_2,$$

for all x in $\mathrm{SL}_2(q)$.

(iii) *If d, b and a are the elements of* $\mathrm{SL}_2(q)$ *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 $L_1 L_2 - \langle t \rangle$ are conjugate in C. All involutions of $C - L_1 L_2$ are conjugate in C to u or tu.*

If x is an element of $\mathrm{SL}_2(q)$, 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

$$Z(T) \leqq C(t) \cap T = S,$$

whence $Z(T) \leqq Z(S)$, so that $Z(T) = \langle t \rangle$, by Lemma 1.1 (iv). Hence $T \leqq C(t)$, so that $T = S$. This proves the lemma.

Two of the involutions of $L_1L_2-\langle t\rangle$ are

(7) $$v = (a_1a_2)^{2^{n-2}}, \qquad w = b_1b_2.$$

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

(8) $$C(t, v) = \langle u, d_1, d_2, w\rangle,$$

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

(9) $$d_1^u = d_2, \qquad d_i^w = d_i^{-1}, \qquad [u, w] = 1.$$

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, tv of $Z(T)$ is a power of exactly $2^{2n-1}-2^n+\frac{1}{3}(2^{2n-2}-1)$ elements of T, while t is a power of only $2^{2n-1}-2^{2n-2}+\frac{1}{3}(2^{2n-2}-1)$ 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

$$E = \langle t, u, v, w\rangle.$$

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

$$X = N(E)/E$$

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 $N(T)\leqq N(E)$. 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 $V\neq S$ since $S\nleqq C(v)$. 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 $2^6 3$ or $2^5 3$ [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_1f_2E permutes the involutions a_1E, b_1E, a_1b_1E of S/E cyclically. Hence $\langle a_1E, b_1E, f_1f_2E\rangle$ is isomorphic with A_4, and all involutions of X are conjugate. Since A_4 has no normal subgroup of order 3, f_1f_2E is not contained in $O(X)$, so that $|X : O(X)|$ is divisible by 3. Since 3^3 does not divide $|A_8|$, $|O(X)|$ is not divisible by 3^2. Hence $O(X)$ has a normal 3-complement W, by Burnside's theorem. If $C_X(a_1E) \cap O(X) \neq \{1\}$, then we must have

$$O(X) = (C_X(a_1E) \cap O(X))W.$$

Then a_1E centralizes the chief factor $O(X)/W$ of X. Hence the conjugate b_1E of a_1E should also centralize $O(X)/W$. But, b_1E inverts $C_X(a_1E) \cap O(X)$, so that we have a contradiction. Thus,

$$C_X(a_1E) \cap O(X) = \{1\}.$$

Now a theorem of Gorenstein and Walter [7, Theorem I] shows that $X/O(X)$ is isomorphic with $\mathrm{PSL}_2(11)$ or $\mathrm{PSL}_2(13)$. This contradicts the fact that $|A_8|$ is not divisible by 11 or 13. Hence v 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

$$G \neq C(t)O(G). \tag{10}$$

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 $C_{G/O(G)}(tO(G)) = C_G(t)O(G)/O(G)$, 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

$$tu \text{ is conjugate in } G \text{ to } t. \tag{11}$$

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*

$$z: t \to uv, \qquad u \to tv, \qquad v \to v. \tag{12}$$

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

$$E = C_S(tu) = \langle a_1a_2, w\rangle \times \langle t, u\rangle.$$

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, $|T| = 2^{2n+2} > |E|$. 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 uv 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 tuv of $Z(E)$ are conjugate in C. If the subset $\{v, tv\}$ were invariant under z, then $t = v(tv)$ would be invariant under z, contradicting the fact that $z \notin C(t)$. Hence v or tv is transformed by z into u or tuv, so that v, tv, u and tuv 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

$$t^z = uv, \qquad (uv)^z = t.$$

Hence $(tuv)^z = uvt = tuv$. 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

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

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,

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

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,

$$S' = \langle a_1^2, a_1a_2, w\rangle.$$

Since wa_1 is conjugate to w in C, S^* also contains wa_1, 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

$$q > 3. \tag{13}$$

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

$$A = \{x_1x_2 \mid x \in \mathrm{SL}_2(q)\}. \tag{14}$$

Then A is a subgroup of $C(t)$ isomorphic with $\mathrm{PSL}_2(q)$, an isomorphism being provided by the mapping taking x_1x_2 on the element of $\mathrm{PSL}_2(q)$ represented by the matrix x. For convenience, we shall identify A with $\mathrm{PSL}_2(q)$ by means of this isomorphism. We have

$$C(t, u) = \langle t, u\rangle \times A. \tag{15}$$

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

$$C(u, v) = \langle tu, d_1^z, d_2^z, w^z\rangle. \tag{16}$$

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*

$$w = (w(d_1d_2)^m tu)^z, \tag{17}$$

for some integer m.

Proof. We have

$$C(t, u, v) = \langle t, u\rangle \times C_A(v), \tag{18}$$

$$C_A(v) = \langle d_1d_2, w\rangle. \tag{19}$$

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

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

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

$$C(t, u, v) = \langle t, u\rangle \times \langle (d_1d_2)^z, w^z\rangle. \tag{20}$$

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

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

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

$$(g^z)^2 = uv, \qquad g^z\colon t \leftrightarrow tu.$$

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 $[g^z, Y] \leqq \langle t, u\rangle$. Since $d_1 d_2$ lies in both Y and $C_A(v)$, we have

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

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 eth powers, we have $(a_1 a_2)^z = u(a_1 a_2)^m$, so that, from (12),

$$(a_1 a_2)^{z^2} = tvu^m (a_1 a_2)^{m^2}.$$

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 $C_S(t, u) = \langle t, u\rangle \times \langle a_1 a_2, w\rangle$, 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 eth 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) $$w = w^z((d_1 d_2)^z)^m tv, \quad \text{or} \quad w = w^z((d_1 d_2)^z)^m tu,$$

for some integer m. Now, $w^z((d_1d_2)^z)^m tv$ is conjugate to $w(d_1d_2)^m u=(b_1d_1)^{-m}(tu) \times (b_1d_1)^m$, 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),

$$(24) \qquad (a_1^z)^w = (a_2^z)^{-1}, \qquad (a_2^z)^w = (a_1^z)^{-1}.$$

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,

$$T' = \langle a_1a_2, a_1^2\rangle^z.$$

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

$$W = \langle (a_1a_2)^z, (a_1^z)^2, w\rangle.$$

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

$$u,\ v,\ uv,\ w,\ uvw.$$

Since A contains only one class of involutions, v, w and vw are conjugate in $C(u)$. Hence uv and uvw are conjugate in $C(u)$. Thus the involutions of M lie in conjugacy classes of $C(u)$ represented by u, v, uv. 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 $tua_1^z w$ is an involution, conjugate in G to $tua_1w(d_1d_2)^m tu = a_2w(d_1d_2)^m$, by (17). Thus $tua_1^z w$ lies in K_2. If $tua_1^z w$ were conjugate in $C(u)$ to v, $ta_1^z w$ would be conjugate to uv. But $ta_1^z w$ is conjugate in G to $uva_1w(d_1d_2)^m tu = va_2w(d_1d_2)^m t$, which lies in K_2 by Lemmas 2.2 and 2.4, while uv lies in K_1. Hence $tua_1^z w$ is not conjugate in $C(u)$ to v. Obviously $tua_1^z w$ is not conjugate in $C(u)$ to u. Hence $tua_1^z w$ is conjugate in $C(u)$ to no element of M, so that, by Lemma 3.3, T^* does not contain $tua_1^z w$.

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

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

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^n 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

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

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

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

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, $A \leqq K$ and M^* contains $A \cap M = \langle a_1a_2, w \rangle$, which we denote J. Suppose that $M^* > J$. Then there exists an element of $M - J$ which is conjugate in K to an element of M', say

$$((a_1a_2)^j)^s = (a_1^z)^k x, \tag{25}$$

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

$$v^s = uvr \quad (r \in J), \qquad \text{or} \quad v^s \in J. \tag{26}$$

The second case can occur only when v is an even power of $(a_1a_2)^j$, since an odd power of $(a_1^z)^k$ does not lie in J. Thus $v = ((a_1a_2)^j)^{2i}$. Then, $((a_1^z)^k x)^i \in \langle uv \rangle J$. 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

$$v^s \in \langle a_1a_2 \rangle,$$

so that $v^s = v$. Hence $s \in C(u, v)$. Since $\langle a_1 a_2 \rangle$ 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 $E = \langle ((d_1 d_2^{-1})^z)^{2^{n-1}} \rangle$, a cyclic group of order e.*

Proof. Since $A \leqq K$, $|K : L| = 2^n$, and A has no subgroup of index 2, we must have $A \leqq L$. 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^n, and all involutions of L are conjugate in L. We have

$$C_L(v) \leqq C(u, v),$$

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 $\mathrm{PSL}_2(r)$, for some odd r.

Since $L/O(L)$ contains $O(L)A/O(L)$, which is isomorphic with $\mathrm{PSL}_2(q)$, it follows that either

$$L/O(L) \approx A_7, \quad q = 7 \text{ or } 9, \text{ or}$$
$$L/O(L) \approx \mathrm{PSL}_2(r), \quad \text{and } r \text{ is a power of } q \text{ or } q = 5,$$

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 $L/O(L) \approx A_7$, and $r \pm 1$ divides $2(q-\delta)^2$ if $L/O(L) \approx \mathrm{PSL}_2(r)$. The only possibility is that $L/O(L) \approx \mathrm{PSL}_2(r)$, $r = q$. Hence $L = O(L)A$.

Since every four-subgroup of $\mathrm{PSL}_2(q)$ is selfcentralizing, $C_L(v, w)O(L)/O(L)$ has order 4, so that

$$O(C_L(v, w)) \leqq O(L).$$

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

$$O(C_L(v, w)) = O(C(u, v, w)) = \langle ((d_1 d_2^{-1})^z)^{2^{n-1}} \rangle.$$

Thus, $|O(L)| \geqq e$.

From the structure of $\mathrm{PSL}_2(q)$,

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

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 $|C_L(v)| = 2^n e^2 = (q-\delta)e$. 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*

$$|K|\,|C_K(F)|^2 = |C_K(t_1)|\,|C_K(t_2)|\,|C_K(t_3)|,$$
$$K = C_K(t_1)C_K(t_2)C_K(t_3).$$

It follows immediately that $|O(L)|=e$, so that $O(L)=\langle((d_1d_2^{-1})^z)^{2^{n-1}}\rangle$, 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*

$$C(u) = \langle t, s\rangle(A\times E), \qquad \langle t, s\rangle \cap (A\times E) = \{1\}, \tag{27}$$

where $A=PSL_2(q)$, E is cyclic of order e, and $\langle t, s\rangle$ is dihedral of order 2^{n+1}:

$$t^2 = s^{2^n} = 1, \qquad s^t = s^{-1}.$$

Here u is the central involution of $\langle t, s\rangle$:

$$u = s^{2^{n-1}}$$

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

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

Proof. By Lemmas 3.2, 3.4 and 3.5, $C(u)=\langle tu, a_1^z, A\times E\rangle$. We put

$$s = a_1^z w(d_1d_2)^k, \tag{28}$$

where k is an integer, to be specified later. Since $w(d_1d_2)^k$ 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

$$s^2 = a_1^z(a_2^z)^{-1}.$$

It follows that $s^{2^{n-1}}=(tv)^z=u$. Thus we have

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

Since transformation by uv interchanges a_1 and a_2, transformation by $t=(uv)^z$ interchanges a_1^z and a_2^z. Thus,

$$s^2s^t = a_1^z(a_2^z)^{-1}a_2^z w(d_1d_2)^k = s,$$

so that $s^t=s^{-1}$ and $\langle t, s\rangle$ is dihedral of order 2^{n+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 $d_1^z(d_2^z)^{-1}$ into $d_2^z(d_1^z)^{-1} =(d_1^z(d_2^z)^{-1})^{-1}$, so that t inverts E. Since a_1^z centralizes $d_1^z(d_2^z)^{-1}$ and $w(d_1d_2)^k$ 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, $s^2=[t, s]$ also centralizes A. Thus the automorphism φ of A induced by s satisfies

$$\varphi^2 = 1. \tag{29}$$

Also, φ inverts $(d_1d_2)^z$, by (28) and Lemma 3.1, and transforms w into $w(d_1d_2)^{2k} \times (a_1a_2)^z$. Since v is the unique involution in $\langle (d_1d_2)^z\rangle$, φ fixes v. Since $(d_1d_2)^{2k}(a_1a_2)^z$ is an odd power of d_1d_2, w is not conjugate to $w(d_1d_2)^{2k}(a_1a_2)^z$ in $C_A(v)=\langle d_1d_2, w\rangle$. Hence φ is not an inner automorphism of A.

Identifying $A=\mathrm{PSL}_2(q)$ with its own inner automorphism group, we see that φ is an element of the automorphism group $\mathrm{P\Gamma L}_2(q)$ of A [5, pp. 90, 98], not contained in A.

Suppose that φ does not belong to $\mathrm{PGL}_2(q)$. Then, by (29), φ 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 $(d_1d_2)^z$ and w are elements of $A=\mathrm{PSL}_2(q)$ represented respectively by the matrices

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

where μ is a generator of the multiplicative group of F_q. If the matrix of the semilinear transformation inducing φ is R, then the fact that φ inverts $(d_1d_2)^z$ 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 φ^2 is the element of $PSL_2(q)$ 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 μ. Now φ transforms w into the element of $PSL_2(q)$ 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 φ transforms w into wx, where x is an even power of $(d_1d_2)^z$, and thus an even power of d_1d_2. But we have seen before that this is not so.

Thus φ belongs to $PGL_2(q)$ but not to $PSL_2(q)$, and inverts d_1d_2. If ψ is the element of $PGL_2(q)$ represented by the matrix

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

then ψ does not lie in $PSL_2(q)$, and inverts d_1d_2. Thus $\varphi\psi^{-1}$ is an element of $PSL_2(q)$ 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 α in F_q, we put

(30) $$\theta(\alpha) = \begin{bmatrix} 1 & 0 \\ \alpha & 1 \end{bmatrix}.$$

The $\theta(\alpha)$ form a Sylow p-subgroup of $SL_2(q)$. Using the isomorphisms of Lemma 1.1 (ii) and writing $\theta_i(\alpha)$ for $\theta(\alpha)_i$ $(i=1, 2)$, we obtain Sylow p-subgroups of L_1 and L_2:

(31) $$P_i = \{\theta_i(\alpha) \mid \alpha \in F_q\} \qquad (i = 1, 2).$$

The mapping $\alpha \to \theta_i(\alpha)$ 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

(32) $$R = P_1P_2 = P_1 \times P_2$$

is a Sylow p-subgroup of $C(t)$. By Lemma 3.7, the subgroup

(33) $$D_1 = \{\theta_1(\alpha)\theta_2(\alpha) \mid \alpha \in F_q\}$$

is a Sylow p-subgroup of $C(u)$, elementary Abelian of order q. We shall also need the subgroup

(34) $$D_2 = \{\theta_1(\alpha)\theta_2(-\alpha) \mid \alpha \in F_q\}.$$

Then R also has direct product decompositions

(35) $$R = P_1D_1 = D_1D_2.$$

We shall put

(36) $$h = \begin{bmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{bmatrix},$$

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

(37) $$H = \langle h_1, h_2 \rangle.$$

Then H is an Abelian subgroup of order $\frac{1}{2}(q-1)^2$, and we have

(38) $$h_1^{(q-1)/2} = h_2^{(q-1)/2} = t.$$

The normalizer of R in $C(t)$ is

(39) $$N(R) \cap C(t) = RH\langle u \rangle.$$

We shall also put

(40) $$y = (sw)^{2^n - 2e}, \quad \text{or} \quad y = s^{2^n - 2e}$$

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

$$\begin{bmatrix} i & 0 \\ 0 & 1 \end{bmatrix} \text{ or } \begin{bmatrix} 1 & 0 \\ 0 & \pm 1 \end{bmatrix},$$

according as $\delta=1$ or $\delta=-1$, where $i^2=-1$. Thus y has the following properties:

$$y \in N(D_1), \tag{41}$$

$$(h_1h_2)^y = h_1h_2; \quad \text{and} \quad w^y = vw \text{ if } \delta = 1, \quad w^y = w \text{ if } \delta = -1. \tag{42}$$

Also, we can compute that

$$y^2 = uv \quad \text{if } \delta = 1; \qquad y^2 = u \quad \text{if } \delta = -1; \tag{43}$$

$$t^y = tu, \qquad (tu)^y = t. \tag{44}$$

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

$$R \cap R^y = D_1. \tag{45}$$

We require the following result connecting R, R^y and subgroups of the group E of Lemma 3.7.

LEMMA 4.1. *If* $\{1\} < F \leqq E$, *then* $N(F) \cap R = N(F) \cap R^y = D_1$.

Proof. Clearly $N(F) \cap R \geqq D_1$. Suppose that $N(F) \cap R > D_1$. Then, from (35), $N(F) \cap P_1 > \{1\}$. Now $\langle h_1h_2 \rangle$ normalizes both F and P_1, so that it normalizes $N(F) \cap P_1$. But $\langle h_1h_2 \rangle$ acts irreducibly on P_1, since an element of $\langle h_1h_2 \rangle$ transforms $\theta_1(\alpha)$ into $\theta_1(\beta\alpha)$, where β 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

$$N(F) \geqq P_1D_1 = R.$$

Since F is cyclic, we have

$$|\text{Aut } F| \leqq |F|-1 \leqq e-1 < q,$$

since $e \leqq \frac{1}{2}(q+1)$. Thus $|N(F) \cap R : C(F) \cap R| < q$, so that $|C(F) \cap R| > q$. Since $C(F) \geqq D_1$, we have $C(F) \cap R > D_1$. Now the same argument as before shows that $C(F) \geqq P_1$. Since $A \leqq C(F)$, $C(F)$ 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 $N(F) \cap R^y = D_1$. 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 semidirect product*

$$M = EQ, \qquad Q \lhd M, \qquad E \cap Q = \{1\},$$

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

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

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

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

$$C(D_1) \cap C(t) = R\langle t, u \rangle, \tag{47}$$

$$C(D_1) \cap C(tu) = R^y\langle t, u \rangle. \tag{48}$$

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 $t\langle s^2 \rangle$ 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

$$C_M(u) = ED_1, \qquad C_M(t) = R, \qquad C_M(tu) = R^y. \tag{49}$$

By Lemma 3.6, we have $|M| = eq^3$, $M = ER^yR$.

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

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

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^yR, 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 $N(D_1)$, so that Q is normal in $N(D_1)$, i.e.

$$N(D_1) \leqq N(Q). \tag{50}$$

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,*

$$C(Q) = Q. \tag{51}$$

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 $C(u) \cap C(R) \leqq C(u) \cap C(D_1)$, and since $C(R) \cap E=\{1\}$ by Lemma 4.1, we find from (46) that $C_K(u)=D_1$. Thus, $C_K(tu) \geqq C_K(t, u)=D_1$.

Suppose that $C_K(tu) \cap R^v=D_1$. By (48), R^v 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 $C_K(tu) \cap R^v > D_1$. By (35) and (41), $R^v=P_1^v D_1$, so that

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

Now, elements of $\langle h_1h_2\rangle^v$ centralize $\langle t, u\rangle^v=\langle t, u\rangle$, and normalize $D_1^v=D_1$. In particular, $\langle h_1h_2\rangle^v$ must normalize the normal 2-complement R of $C(D_1) \cap C(t)$. Thus $\langle h_1h_2\rangle^v$ normalizes K. Since $\langle h_1h_2\rangle^v$ normalizes P_1^v, it normalizes $C_K(tu) \cap P_1^v$. Since $\langle h_1h_2\rangle^v$ acts irreducibly on P_1^v, we have $C_K(tu) \geqq P_1^v$, so that

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

Since $C(tu) \cap C(R) \leqq C(tu) \cap C(D_1)$, it follows from (48) that $C_K(tu)=R^v$. Now Lemma 3.6 shows that $K=R^vRD_1=R^vR=Q$.

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

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

$$N(R) \leqq N(Q). \tag{52}$$

We now put

$$P_3 = D_2^v, \qquad \theta_3(\alpha) = (\theta_1(\alpha)\theta_2(-\alpha))^v. \tag{53}$$

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

$$Q = P_1 \times P_2 \times P_3. \tag{54}$$

Since $C(Q)=Q$, $N(Q)/Q$ acts faithfully on Q. Since $H \leqq N(Q)$ 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*

$$h_1\colon \theta_1(\alpha) \to \theta_1(\varepsilon^2\alpha), \quad \theta_2(\alpha) \to \theta_2(\alpha), \quad \theta_3(\alpha) \to \theta_3(\varepsilon\alpha),$$

$$h_2\colon \theta_1(\alpha) \to \theta_1(\alpha), \quad \theta_2(\alpha) \to \theta_2(\varepsilon^2\alpha), \quad \theta_3(\alpha) \to \theta_3(\varepsilon\alpha).$$

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 $h_1h_2\colon \theta_1(\alpha)\theta_2(-\alpha) \to \theta_1(\varepsilon^2\alpha)\theta_2(-\varepsilon^2\alpha)$, (42) and (53) imply that

$$h_1h_2\colon \theta_3(\alpha) \to \theta_3(\varepsilon^2\alpha).$$

Thus the effect of $(h_1h_2)^m$ on Q is multiplication by the scalar ε^{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 ε^2, and tu transforms h_1 into h_2, we have

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

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 ε 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 $N(P_1)$.

LEMMA 4.5. *Let $V=O(C(P_1))$. Then*

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

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 $C(P_1)/V$ 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 $P_1 \leqq V$. 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 $C_V(t)=P_1$, t acts without fixed point on V/P_1, so that V/P_1 is Abelian. Since $P_1 \leqq Z(V)$, 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 $t=(tu)^y$ inverts $D_2^y=P_3$, so that we must have $P_3 \leqq V$. 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*

$$O(C(P_3)) \leqq QH.$$

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

$$C(D_2)\cap C(t) = R\langle t, uv\rangle.$$

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 $\langle t, uv\rangle$ is a Sylow 2-subgroup of $C(D_2)$. The involutions of $\langle t, uv\rangle$ are not all conjugate in $C(D_2)$, since $t\in K_1$, $tuv\in K_2$. Thus $C(D_2)$ has a normal 2-complement, and so does $C(P_3)=C(D_2)^y$.

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

$$O(C(D_2))\cap C(t) = R,\quad O(C(D_2))\cap C(u) \geqq D_1,\quad O(C(D_2))\cap C(tu) \geqq D_1.$$

Now each Sylow p-subgroup of $PSL_2(q)$ 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 $PSL_2(q)$. 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

$$O(C(D_2)) \cap C(u) \leqq D_1\langle h_1h_2\rangle.$$

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

$$O(C(D_2)) \cap C(tu) \leqq R^yH^y.$$

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

$$O(C(P_3)) = O(C(D_2))^y \leqq RR^yH = QH.$$

LEMMA 4.7. *$V=O(C(P_1))$ is a p-group.*

Proof. Applying Lemma 4.6, we find that

$$C_V(P_3) \leqq O(C(P_3)) \cap C(P_1) \leqq Q\langle h_2\rangle \leqq L_2P_1P_3.$$

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

$$c = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}. \tag{55}$$

The element c_2 of $C(t)$ centralizes P_1 and so normalizes V. Hence, $P_3^{c_2}\leqq V$. We put

$$P_4 = P_3^{c_2}, \qquad \theta_4(\alpha) = \theta_3(\alpha)^{c_2}. \tag{56}$$

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

$$h_1h_2 \in C(P_4). \tag{57}$$

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

$$P_1P_3 \cap P_4 = \{1\}, \qquad V \geqq P_1P_3P_4.$$

Since V/P_1 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*

$$N(U) \cap N(P_1) = UH \leqq N(Q).$$

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), $(tuv)^y=tv$. Since tuv centralizes D_2, tv centralizes $D_2^y=P_3$.

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

$$N(U)\cap N(P_1) = (N(P_2)\cap L_2\langle h_1\rangle)V = P_2\langle h_1, h_2\rangle V = UH.$$

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), $H\leqq N(Q)$. Thus $UH\leqq N(Q)$. 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 $\mathrm{PGL}_2(q)$, *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, $h_1h_2^{-1}Q$.

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

$$C_W(t)\geqq C_Q(t) = R,\quad C_W(u)\geqq C_Q(u) = D_1,\quad C_W(tu) = C_W(t)^y.$$

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

(58) $$W\leqq Q\langle h_1^2, (h_1^y)^2, h_1h_2, E\rangle.$$

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

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

The Sylow 2-subgroup $\langle t, s\rangle$ of this group is dihedral of order 2^{n+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

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

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],

$$N(Q)/W \approx \mathrm{PGL}_2(r),$$

for some odd prime power r.

Since the centralizer of an involution in $\mathrm{PGL}_2(r)$ 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,

$$W \cap E = \{1\}, \qquad C_{N(Q)/W}(uW) \approx \langle t, s\rangle E.$$

The order of $\langle t, s\rangle E$ is $2^{n+1}e = 2(q+1)$. But, the structure of $\mathrm{PGL}_2(r)$ 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

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

Since $h_1h_2 \in W$, it follows that

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

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

$$N(Q)/W \approx \mathrm{PGL}_2(q).$$

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

$$C_W(t) = R\langle h_1h_2\rangle, \quad C_W(u) = D_1\langle h_1h_2\rangle, \quad C_W(tu) = R^y\langle h_1h_2\rangle,$$

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:

$$N(Q)/Q = JZ, \qquad J \cap Z = 1,$$

where $Z = W/Q$, $J \approx \mathrm{PGL}_2(q)$. Now, Z is centralized by the involution tQ, which corresponds to an involution of $\mathrm{PGL}_2(q)$ not lying in $\mathrm{PSL}_2(q)$. Since such an involution and its conjugates generate $PGL_2(q)$, 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 $PGL_2(q)$, uQ must invert M. We know that uQ centralizes Z. Hence

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

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* $PGL_2(q)$ *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

(60) $$\eta(\alpha)\colon \theta_1(\beta) \to \theta_1(\beta), \quad \theta_2(\beta) \to \theta_1(\alpha^2\beta)\theta_2(\beta)\theta_3(\mu\alpha\beta), \quad \theta_3(\beta) \to \theta_1(2\mu\alpha\beta)\theta_3(\beta),$$

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 $(h_1h_2)^mQ$ of Z is multiplication by the scalar ε^{2m}. 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:

(61) $$tQ \to \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \quad uQ \to \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{bmatrix},$$
$$h_1h_2^{-1}Q \to \begin{bmatrix} \varepsilon^2 & 0 & 0 \\ 0 & \varepsilon^{-2} & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

In any 1-dimensional representation of $PGL_2(q)$, elements of $PSL_2(q)$ are represented by 1. Since uQ corresponds in $J = PGL_2(q)$ to an element of $PSL_2(q)$

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 $\mathrm{PGL}_2(q)$ over F_q shows that the representation of J on Q is irreducible, and that, if a matrix representation of J as $\mathrm{PGL}_2(q)$ 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

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

where

$$x_i' = \sum_j \varphi(a_{ij})x_j, \tag{62}$$

where φ 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 α 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 $\frac{1}{2}(q-1)-1$.

Since uQ lies in $\mathrm{PSL}_2(q)$, 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 $\mathrm{PGL}_2(q)-\mathrm{PSL}_2(q)$ 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 μ. 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 ν.

Since $h_1h_2^{-1}Q$ is an element of odd order commuting with tQ,

$$h_1h_2^{-1}Q \sim \begin{bmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{bmatrix},$$

for some scalar λ. Then $h_1h_2^{-1}Q$ transforms

$$x_1^2+x_2^2 \to \tfrac{1}{2}(\lambda^2+\lambda^{-2})(x_1^2+x_2^2)+\tfrac{1}{2}(\lambda^2-\lambda^{-2})(x_1^2-x_2^2),$$

$$x_1^2-x_2^2 \to \tfrac{1}{2}(\lambda^2-\lambda^{-2})(x_1^2+x_2^2)+\tfrac{1}{2}(\lambda^2+\lambda^{-2})(x_1^2-x_2^2).$$

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

$$\lambda^2+\lambda^{-2} = \varepsilon^2+\varepsilon^{-2} \qquad \mu(\lambda^2-\lambda^{-2}) = \nu(\varepsilon^2-\varepsilon^{-2}).$$

Since $\lambda^2+\lambda^{-2}-\varepsilon^2-\varepsilon^{-2}=(\lambda^2-\varepsilon^2)(1-\lambda^{-2}\varepsilon^{-2})$, $\lambda^2=\varepsilon^2$ or $\lambda^2=\varepsilon^{-2}$. Since a matrix and its negative represent the same element of $PGL_2(q)$, we may take $\lambda=\varepsilon$ or $\lambda=\varepsilon^{-1}$. Since uQ centralizes tQ and uQ, and inverts $h_1h_2^{-1}Q$, we may assume that $\lambda=\varepsilon$, so that

$$h_1h_2^{-1}Q \sim \begin{bmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{bmatrix}.$$

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

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

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 $\theta_3(1)$, 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

$$\eta(\alpha) \to \begin{bmatrix} 1 & 0 & 0 \\ \alpha^2 & 1 & \mu\alpha \\ 2\mu\alpha & 0 & 1 \end{bmatrix}.$$

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^2. 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, $N(U_1)\leqq N(Q)$. 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 $U_1\leqq C(P_1)$, U_1V is a p-subgroup of G, so that $U_1\geqq V$. Also, $P_2<Q\leqq U_1$. Hence $U=P_2V\leqq U_1$, so that $U=U_1$. Since P_1P_3 is normal in U, P_2 and P_4 are Abelian, and $[P_2,P_4]\leqq P_1P_3$ by (60), U/P_1P_3 is Abelian. As in the proof for the case $\delta=1$, $N(U)\cap N(P_1)=UH$. Finally, $U=U_1\leqq N(Q)$ and $H\leqq N(R)\leqq N(Q)$, so that $UH\leqq N(Q)$. 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*

$$[\theta_i(\alpha),\theta_1(\beta)]=[\theta_2(\alpha),\theta_3(\beta)]=1,\qquad (i=2,3,4),$$
$$\theta_4(\alpha)\colon \theta_2(\beta)\to\theta_1(-\delta\alpha^2\beta)\theta_2(\beta)\theta_3(\alpha\beta),\qquad \theta_3(\beta)\to\theta_1(-2\delta\alpha\beta)\theta_3(\beta),$$
$$h_1\colon \theta_4(\alpha)\to\theta_4(\varepsilon\alpha),\qquad h_2\colon \theta_4(\alpha)\to\theta_4(\varepsilon^{-1}\alpha),$$

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_1, inverts h_2, and transforms $\theta_3(\alpha)$ into $\theta_4(\alpha)$, we find from Lemma 4.4 that

$$h_1\colon \theta_4(\alpha)\to\theta_4(\varepsilon\alpha),\qquad h_2\colon \theta_4(\alpha)\to\theta_4(\varepsilon^{-1}\alpha).$$

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_q 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 $P_1\leqq Z(U)$ 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

$$\theta_4(\alpha)\to\begin{bmatrix}1&0&0\\ f(\alpha)&1&g(\alpha)\\ h(\alpha)&0&1\end{bmatrix},\tag{63}$$

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

Using (56), (63), and the fact that $c_2^2=t$ inverts P_3, we compute that

$$c_2\theta_2(1)\colon \theta_3(\alpha) \to \theta_1(f(-\alpha))\theta_3(g(-\alpha))\theta_4(\alpha), \qquad \theta_4(\alpha) \to \theta_3(-\alpha).$$

Then we compute, using (63), that

$$(c_2\theta_2(1))^3\colon \theta_4(\alpha) \to \theta_1(k(\alpha))\theta_3(r(\alpha))\theta_4(g(\alpha)),$$

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 $\theta_4(\alpha)h_1=h_1\theta_4(\varepsilon\alpha)$. Taking the matrices of the corresponding linear transformations on Q, by Lemma 4.4 and (63), we find that

$$f(\varepsilon\alpha) = \varepsilon^2 f(\alpha).$$

Since ε 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 β by α, we have $f(\alpha)=m\alpha^2$, 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 $h(\alpha)=2m\alpha$.

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

$$(tw\theta_1(1)\theta_2(-1))^3 = 1.$$

Transforming by yc_2, we obtain the equation

$$(tuv\theta_4(1))^3 = 1.$$

We calculate that

$$tuv\theta_4(1) \to \begin{bmatrix} -m & -1 & -1 \\ -1 & 0 & 0 \\ -2m & 0 & -1 \end{bmatrix}.$$

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 $N(U)\leqq N(P_1)$, 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 $V=P_1P_3P_4$ are given as follows.

LEMMA 5.1.

$$u\colon \theta_1(\alpha)\to\theta_2(\alpha),\qquad \theta_2(\alpha)\to\theta_1(\alpha),\qquad \theta_3(\alpha)\to\theta_3(-\alpha),$$
$$c_2\colon \theta_1(\alpha)\to\theta_1(\alpha),\qquad \theta_3(\alpha)\to\theta_4(\alpha),\qquad \theta_4(\alpha)\to\theta_3(-\alpha).$$

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

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

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

$$N = \langle H, u, c_2\rangle. \tag{64}$$

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*

$$h_1^{(q-1)/2} = h_2^{(q-1)/2} = c_2^2 = t,\qquad t^2 = u^2 = 1,$$
$$[h_1,h_2] = [h_1,c_2] = 1,\qquad h_1^u = h_2,\qquad h_2^{c_2} = h_2^{-1},\qquad (uc_2)^4 = 1.$$

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

$$r_1 = uH,\qquad r_2 = c_2H.$$

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 σ in W, let $\lambda(\sigma)$ be the number of factors r_i when σ 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 σK and $K\sigma$ for the cosets $\omega(\sigma)K$ and $K\omega(\sigma)$. If K is any subgroup normalized by H, we write K^{σ} for $K^{\omega(\sigma)}$. We set

$$B = UH. \tag{65}$$

Clearly $B \cap N = H$.

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

Proof. Since $G_iG_i = B \cup Br_iB \cup Br_iBr_iB$ and $r_i^2=1$, it is enough to prove that

$$B^{r_i} \subseteq B \cup Br_iB.$$

Since $u=\omega(r_1)$ normalizes $P_1P_2P_3H$ and $c_2=\omega(r_2)$ normalizes $P_1P_3P_4H$, it is enough to show that

$$P_4^{r_1} \subseteq B \cup Br_1B, \qquad P_2^{r_2} \subseteq B \cup Br_2B.$$

As is well known, e.g. [3, p. 34], $L_2 \approx SL_2(q)$ has the Bruhat decomposition

$$L_2 = B_2 \cup B_2c_2B_2,$$

where $B_2 = P_2\langle h_2\rangle \leqq B$. Hence $P_2^{r_2} = P_2^{c_2} \leqq L_2 \subseteq B \cup Br_2B$.

For x in $SL_2(q)$, set

$$\bar{x} = f^{-1}xf, \qquad \text{where } f = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Then

$$A_1 = \{x_1\bar{x}_2 \mid x \in SL_2(q)\}$$

is a subgroup of $C(t)$ isomorphic with $PSL_2(q)$, an isomorphism being provided by the correspondence associating $x_1\bar{x}_2$ with the element of $PSL_2(q)$ represented by the matrix x. The matrices

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

of $SL_2(q)$ give a Sylow p-subgroup D_2 of A_1, whose normalizer in A_1 is

$$B_1 = D_2\langle h_1h_2\rangle,$$

since $\bar{h}_2 = h_2$. Since $\bar{c}_2 = tc_2$, the Bruhat decomposition of $SL_2(q)$ leads to the decomposition

$$A_1 = B_1 \cup B_1tc_1c_2B_1.$$

In particular, $D_2^{tc_1c_2} \subseteq B_1 \cup B_1tc_1c_2B_1$.

Now, $D_2^{yc_2} = P_4$, $(h_1h_2)^{yc_2} = h_1h_2^{-1}$, and $(tc_1c_2)^{yc_2} = tuv$ or u according as $\delta = 1$ or $\delta = -1$. If $\delta = 1$, $tv \in H$ so that $tuv \equiv u \pmod{H}$. Then,

$$P_4^{r_1} \subseteq (B_1 \cup B_1tc_1c_2B_1)^{yc_2} \subseteq B \cup Br_1B,$$

since $B_1^{yc_2} = P_4\langle h_1h_2^{-1}\rangle \leqq B$. This proves the lemma.

LEMMA 5.4. *If $\sigma \in W$, $i=1$ or 2, and $\lambda(r_i\sigma) \geqq \lambda(\sigma)$, then $r_iB\sigma \subseteq Br_i\sigma B$.*

Proof. Since u normalizes $P_1P_2P_3H$ and c_2 normalizes $P_1P_3P_4H$, it is enough to show that

$$uP_4\omega(\sigma) \subseteq u\omega(\sigma)B \quad \text{if } \lambda(r_1\sigma) \geqq \lambda(\sigma),$$
$$c_2P_2\omega(\sigma) \subseteq c_2\omega(\sigma)B \quad \text{if } \lambda(r_2\sigma) \geqq \lambda(\sigma).$$

There are eight cases to examine, all easily verified by using Lemma 5.1. For example, when $i=1$, $\sigma=r_2r_1$,

$$uP_4c_2u = uc_2P_3u = uc_2uP_3.$$

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. $U \cap U^{r_1r_2r_1r_2}=\{1\}$.

Proof. Let $m=\omega(r_1r_2r_1r_2)=(uc_2)^2=c_1c_2$, 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 $C_U(t)=R$ 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

$$D \cap Q \leqq P_3.$$

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

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

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

Let $d \in D$. Then $d=mn$, where $m \in P_4$, $n \in Q$. Since h_1h_2 centralizes P_4 and normalizes both D and Q, we see that

$$[n, h_1h_2] = [d, h_1h_2] \in D \cap Q,$$

so that h_1h_2 commutes with n. Since h_1h_2 acts without fixed point on Q, $n=1$. Thus, $D \leqq P_4$. Since H acts irreducibly on P_4, either $D=\{1\}$ or $D=P_4$.

Since $m^2=1$, m normalizes D. If $D\neq\{1\}$, then m induces an automorphism of P_4, say

$$m\colon \theta_4(\alpha)\to\theta_4(f(\alpha)).$$

Now, $h_1m=mh_1^{-1}$, and we know the action of $\langle h_1\rangle$ on P_4, by Lemma 4.11. This implies that

$$f(\varepsilon\alpha) = \varepsilon^{-1}f(\alpha).$$

Since ε generates the multiplicative group of F_q,

$$f(\beta\alpha) = \beta^{-1}f(\alpha)$$

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 α, β, $\alpha+\beta$ are all nonzero,

$$(\alpha+\beta)^{-1} = \alpha^{-1}+\beta^{-1}.$$

Take $\beta=1$ and clear fractions. Then every nonzero element α 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 σ of W,*

$$U = U_\sigma U'_\sigma,\qquad \omega(\sigma)U_\sigma\omega(\sigma)^{-1} \leqq U^{r_1r_2r_1r_2},\qquad \omega(\sigma)U'_\sigma\omega(\sigma)^{-1} \leqq U,$$

where U_σ and U'_σ are subgroups of U given by the table

σ	1	r_1	r_2	r_1r_2	r_2r_1	$r_1r_2r_1$	$r_2r_1r_2$	$r_1r_2r_1r_2$
U_σ	$\{1\}$	P_4	P_2	P_2P_3	P_1P_4	$P_1P_3P_4$	$P_1P_2P_3$	U
U'_σ	U	$P_1P_2P_3$	$P_1P_3P_4$	P_1P_4	P_2P_3	P_2	P_4	$\{1\}$

Proof. This is straightforward computation, using Lemma 5.1. For example, $(P_2P_3)^{r_1r_2}=(P_1P_3)^{r_2}=P_1P_4$, so that

$$\omega(r_1r_2)P_1P_4\omega(r_1r_2)^{-1} = P_2P_3 \leqq U,$$

and

$$\begin{aligned}\omega(r_1r_2)P_2P_3\omega(r_1r_2)^{-1} &= \omega(r_1r_2r_1r_2)P_1P_4\omega(r_1r_2r_1r_2)^{-1}\\ &= P_1P_4^{r_1r_2r_1r_2} \leqq U^{r_1r_2r_1r_2}.\end{aligned}$$

LEMMA 5.8. *Every element of G_0 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_0 is equal to the order of* $\mathrm{PSp}_4(q)$.

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 $|B\sigma B|=|B|\,|U_\sigma|$, so that

$$|G_0| = |B| \sum_{\sigma\in W} |U_\sigma| = \tfrac{1}{2}q^4(q-1)^2(1+q+q+q^2+q^2+q^3+q^3+q^4)$$
$$= \tfrac{1}{2}q^4(q-1)^2(q+1)^2(q^2+1) = |\mathrm{PSp}_4(q)|.$$

This proves the lemma.

LEMMA 5.9. *G_0 is isomorphic with* $\mathrm{PSp}_4(q)$.

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 $\mathrm{PSp}_4(q)$ satisfies the hypothesis of the theorem and the condition (10), we see that $\mathrm{PSp}_4(q)$ has a subgroup isomorphic with G_0. By the equality of the orders, G_0 is isomorphic with $\mathrm{PSp}_4(q)$.

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,

$$G_2r_1G_2 = Br_1B \cup Br_2r_1B \cup Br_1r_2B \cup Br_2r_1r_2B,$$
$$G_2r_1r_2r_1G_2 = Br_1r_2r_1B \cup Br_1r_2r_1r_2B,$$

so that G_0 is decomposed into 3 double cosets

$$G_0 = G_2 \cup G_2r_1G_2 \cup G_2r_1r_2r_1G_2.$$

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

$$1, \qquad |G_2r_1G_2|/|G_2| = q(q+1), \qquad |G_2r_1r_2r_1G_2|/|G_2| = q^3.$$

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, $K\geqq P_1$. Hence $K\geqq P_1^u=P_2$, $K\geqq D_2$. Hence $K\geqq D_2^y=P_3$, and $K\geqq P_3^{c_2}=P_4$. Thus $K\geqq U$. By Lemma 4.11 and the Frattini argument, $G_0=KH\leqq G_2$, a contradiction. Thus P_1 is represented faithfully. From Lemma 5.8, every right coset of G_2 in $G_2r_1G_2$ has the form G_2r_1x or $G_2r_1r_2x$, where $x\in U$. Since P_1 is in the center of U and lies in U'_{r_1} and $U'_{r_1r_2}$, it follows that every element of P_1 fixes every right coset of G_2 in $G_2r_1G_2$. By [9, Theorem 2, p. 154], G_0 has $\mathrm{PSp}_4(q)$ as a chief factor, and so G_0 is isomorphic with $\mathrm{PSp}_4(q)$, by equality of orders.

LEMMA 5.10. $G_0=G$.

Proof. Since $PSp_4(q)$ 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

$$K_1' = K_1 \cap G_0, \qquad K_2' = K_2 \cap G_0.$$

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

1. R. Brauer, *Some applications of the theory of blocks of characters of finite groups.* II, J. Algebra **1** (1964), 307–334.

2. R. Brauer and C. Nesbitt, *On the modular characters of groups*, Ann. of Math. **42** (1941), 556–590.

3. C. Chevalley, *Sur certains groupes simples*, Tôhoku Math. J. (2) **7** (1955), 14–66.

4. L. E. Dickson, *Linear groups*, Dover, New York, 1958.

5. J. Dieudonné, *La géométrie des groupes classiques*, Springer, Berlin, 1955.

6. G. Glauberman, *Central elements in core-free groups*, J. Algebra **4** (1966), 403–420.

7. D. Gorenstein and J. H. Walter, *On finite groups with dihedral Sylow* 2-*subgroups*, Illinois J. Math. **6** (1962), 553–593.

8. M. Hall, *The theory of groups*, Macmillan, New York, 1959.

9. D. G. Higman, *Finite permutation groups of rank* 3, Math. Z. **86** (1964), 145–156.

10. Z. Janko, *A characterization of the finite simple group* $PSp_4(3)$, Canad. J. Math. **19** (1967), 872–894.

11. K.-W. Phan, *On a characterization of* $L_4(q)$, *q odd.* I, J. Algebra. (to appear).

12. M. Suzuki, *On characterizations of linear groups.* V (to appear).

13. ———, *On characterizations of linear groups.* VI (to appear).

14. ———, *Two characteristic properties of* (ZT)-*groups*, Osaka Math. J. **15** (1963), 143–150.

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

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

17. W. J. Wong, *A characterization of the alternating group of degree* 8, Proc. London Math. Soc. (3) **13** (1963), 359–383.

University of Notre Dame,
Notre Dame, Indiana