JOURNAL OF ALGEBRA 15, 252–279 (1970)

A Characterization of Four-Dimensional Unimodular Groups

KOK-WEE PHAN

University of Notre Dame, Notre Dame, Indiana 46556

Communicated by Richard Brauer

Received July 19, 1969

In this paper we shall show that the four-dimensional unimodular group over the finite field of odd characteristic q is characterized by the structure of the centralizer of an element of order 2. Let H_q denote the centralizer in $L_4(q)$ of an involution contained in the center of an S_2-subgroup of $L_4(q)$. Our characterization is given by the following:

THEOREM. *Let G be a finite group of even order with the following properties:*

(a) *G has no subgroup of index 2;*

(b) *G contains an involution t such that the centralizer $C_G(t) = H$ of t in G is isomorphic to H_q.*

Then G is isomorphic to $L_4(q)$.

The method of our proof is the familiar one. Briefly we aim to construct a subgroup of G which is a (B, N)-pair in the sense of Tits and finally to show that this subgroup is G itself. It turns out that the information needed for the construction can be obtained by the study of the fusion of involutions. Since these involutions fuse differently when $q \equiv -1 \pmod 4$ and when $q \equiv 1 \pmod 4$, it appears best to treat the two cases separately for the sake of clarity but at the expense of some repetition.

As is often the case with this type of work, a detailed knowledge of the structure of H_q is essential. We shall freely use results on the structure of H_q without proof, which are essentially simple deductions from Dickson's list of all subgroups of $L_2(q)$. Our arguments are group theoretic but rely on character theory implicitly via the work of Gorenstein–Walter [4].

The notation is standard. See for example, Gorenstein's book [3]. The symbols $N(X)$ and $C(X)$ shall denote the normalizer and centralizer, respectively, in the group G of the theorem of some subset X of G.

1. STRUCTURE OF THE GROUP H_q

Let $\tilde{V}$ be a four-dimensional vector space over the finite field F_q where q is odd. We shall identify a linear transformation of $\tilde{V}$ with the corresponding matrix in terms of a fixed basis of $\tilde{V}$. For every $x \in SL(2, q)$, let x_1', x_2' denote the matrices

$$\begin{pmatrix} x & & \\ & 1 & \\ & & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & & \\ & 1 & \\ & & x \end{pmatrix},$$

respectively. Let $L_i' = \langle x_i' \mid x \in SL(2, q) \rangle$ $(i = 1, 2)$. The matrix

$$t_0' = \begin{pmatrix} -1 & & & \\ & -1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix}$$

is an involution in $SL(4, q)$. Let H_q' denote the group of matrices (α_{ij}) in $SL(4, q)$ which commute projectively with t_0', i.e.,

$$(\alpha_{ij})^{-1}\, t_0'(\alpha_{ij})\, t_0' \in Z(SL(4, q)),$$

the center of $SL(4, q)$. It is easy to see that H_q' is a splitting extension of $L_1' \times L_2'$ by a dihedral group $\langle u', w' \rangle$ of order $2(q - 1)$ where

$$u' = \begin{pmatrix} & & 1 & 0 \\ & & 0 & 1 \\ 1 & 0 & & \\ 0 & 1 & & \end{pmatrix}, \qquad w' = \begin{pmatrix} 1 & & & \\ & \lambda & & \\ & & 1 & \\ & & & \lambda^{-1} \end{pmatrix}$$

λ a primitive element of F_q.

Form the factor group $H_q = H_q'/Z(SL(4, q))$ which clearly is the centralizer in $L_4(q)$ of the involution $t_0 = t_0'Z(SL(4, q))$. In the natural homomorphism of H_q' onto H_q, let the images of L_i', x' be L_i, x, respectively, where $x' \in H_q'$.

Let $q = p^f$, $q - 1 = 2^\alpha d$, $q + 1 = 2^\beta e$ where d and e are odd. When $q \equiv -1 \pmod 4$, $\alpha = 1$, $\beta \geqslant 2$, $|Z(SL(4, q))| = 2$ and $|H_q| = (q - 1)^3 q^2 (q + 1)^2$. When $q \equiv 1 \pmod 4$, $\alpha \geqslant 2$, $\beta = 1$, $|Z(SL(4, q))| = 4$ and $|H_q| = \frac{1}{2}(q - 1)^3 q^2 (q + 1)^2$. Comparing the order of H_q with that of $L_4(q)$, t_0 is indeed an involution contained in the center of an S_2-subgroup of $L_4(q)$.

We shall need the images α_1, c_1, and θ_1 in H_q of the following matrices in H_q':

$$\alpha_1' = \begin{pmatrix} \lambda & & & \\ & \lambda^{-1} & & \\ & & 1 & \\ & & & 1 \end{pmatrix}; \qquad c_1' = \begin{pmatrix} 0 & 1 & & \\ -1 & 0 & & \\ & & 1 & \\ & & & 1 \end{pmatrix}; \qquad \theta_1' = \begin{pmatrix} 1 & 0 & & \\ -1 & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix}.$$

Set $\alpha_2 = u\alpha_1 u$, $c_2 = uc_1 u$, $\theta_2 = u\theta_1 u$, $l = (w^2\alpha_1\alpha_2^{-1})^{2^{\alpha-1}}$, $m = (\alpha_1\alpha_2^{-1})^{2^{\alpha-1}}$, $n = (\alpha_1\alpha_2)^{2^{\alpha-1}}$. The symbols introduced in this section shall keep their meaning throughout the paper.

2. The case $q \equiv -1 \pmod 4$.

Here we have $\alpha = 1$, $\beta \geqslant 2$, and H_q is a splitting extension of the central product $L_1 L_2$ (i.e., $[L_1, L_2] = 1, L_1 \cap L_2 = t_0$) by the dihedral group $\langle u, w\rangle$. From now on we shall identify H_q with $H = C_G(t)$, the centralizer of t in G in the theorem. Hence $t_0 = t$.

(2.1.1) *S_2-subgroup of H*

It is well-known that $GL(2, q)$, where $q \equiv -1 \pmod 4$, contains elements x, y with $O(x) = 2(q+1)$, $O(y) = 2$ and $\det(x) = \det(y) = -1$ such that $\langle x, y\rangle$ satisfies the relation $yxy = x^q$. Therefore $\langle x^e, y\rangle$ has order $2^{\beta+2}$ and is a S_2-subgroup of $GL(2, q)$. We check that $y^{-1}x^e y = (x^e)^q = (x^e)^{2^\beta - 1}$ since $q \equiv 2^\beta - 1 \pmod{2^{\beta+1}}$ and so $\langle x^e, y\rangle$ is a semidihedral group. We may choose x such that

$$x^{2^{\beta-1}e} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{and} \quad y = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Let β_1 be the image in H_q of the following matrix in H_q':

$$\begin{pmatrix} x & \\ & y \end{pmatrix}.$$

Set $\beta_2 = u\beta_1 u$, $b_i = \beta_i^{2e}$, $v = w^{(q-1)/2}$, $d_i = v\beta_i{}^e$ $(i = 1, 2)$. We compute that $O(b_i) = 2^\beta$, $O(d_i) = 4$ and that the following relations hold: $Q_i = \langle b_i, d_i\rangle \subseteq L_i$ is generalized quaternion; $vb_i v = b_i^{-1}$; $vd_i v = b_i d_i^{-1}$; $uv = vu$ $(i = 1, 2)$. Hence $Q = \langle u, v\rangle Q_1 Q_2$ is an S_2-subgroup of H which has order $2^{2\beta+3}$ and center $Z(Q) = \langle t\rangle$.

(2.1.2) *Conjugate classes of involutions in H*

Every involution $t' \neq t$ in $Q_1 Q_2$ has the form $t' = x_1 y_2$ where $x_1 \in Q_1$, $y_2 \in Q_2$ and $x_1{}^2 = y_2{}^2 = t$. Since all elements of order 4 in $SL(2, q)$ are conjugate, it follows that t' is conjugate to $t_3 = (b_1 b_2)^{2^{\beta-2}} = c_1 c_2$ in H.

By an easy computation all involutions in $uQ_1Q_2 - Q_1Q_2$ have the form $ux_1x_2^{-2} = u^{x_1}$ or $utx_1x_2^{-1} = (ut)^{x_1}$ where $x_i \in Q_i$ and so are conjugate in H to u and ut, respectively. It is easily verified that u is not conjugate to ut in H. Similarly all involutions in $uvQ_1Q_2 - Q_1Q_2$ lie in two conjugate classes of H with representatives uv and uvt. Lastly involutions in $vQ_1Q_2 - Q_1Q_2$ have the form $vb_1{}^i b_2{}^j$ for some integers i and j and are conjugate to v.

Thus we have shown that there are seven classes of involutions in H with representatives t, t_3, u, ut, uv, uvt, and v.

(2.1.3) *Centralizers of involutions in H.*

The centralizer $C_H(t_3)$ of t_3 in H is $A = \langle l, \beta_1^2, \beta_2^2, t_4\rangle\langle u, v\rangle$ where $t_4 = d_1 d_2$. An S_2-subgroup of A is $\tilde{Q} = \langle b_1, b_2, t_4\rangle\langle u, v\rangle$ and is of index 2 in Q. The center $Z(\tilde{Q}) = \langle t, t_3\rangle$ is a four group. The commutator group $\tilde{Q}'$ is $\langle b_1^2, b_1 b_2\rangle$. Every elementary Abelian group of order 16 in Q is conjugate to one of the following:

$$E_1 = \langle t, t_3, t_4, u\rangle,$$
$$E_2 = \langle t, t_3, b_1 d_1 d_2, uv\rangle,$$

and

$$E_3 = \langle t, t_3, u, v\rangle.$$

The centralizer $C_H(u)$ of u in H is $\langle t, u, v\rangle B$ where

$$B = \langle x_1 x_2 \mid x \in SL(2, q)\rangle \cong L_2(q).$$

We have $C_H(u) = C_H(ut)$. Similarly $C_H(uv) = \langle t, u, v\rangle C$ where

$$C = \langle x_1 x_2^v \mid x \in SL(2, q)\rangle \cong L_2(q) \qquad \text{and} \qquad C_H(uv) = C_H(uvt).$$

Finally,

$$C_H(v) = \langle t, t_3, u, v\rangle\langle l, m, n\rangle = E_3\langle l, m, n\rangle.$$

We check that $\langle l, m, n\rangle$ is a normal 2-complement of $C_H(v)$.

(2.1.4) *S_p-subgroups of H.*

Let

$$T_1 = \langle \theta_1^x \mid x \in \langle n, v\rangle\rangle; \quad T_2 = T_1^u$$

and

$$T = \langle (\theta_1\theta_2)^x \mid x \in \langle n, v\rangle\rangle.$$

Clearly $T_1 T_2 = T_1 \times T_2$ is an S_p-subgroup of H and is elementary of order q^2. We have

$$C_H(T_1 T_2) = \langle t, l\rangle\, T_1 T_2$$

and

$$N_H(T_1 T_2) = \langle t, v\rangle\langle l, m, n\rangle\, T_1 T_2 .$$

By direct computation, $(c_2\theta_2)^3 = 1$.

(2.1.5) *The maximal normal subgroup of H of odd order*

It is easily seen that $O(H) = \langle l\rangle$ of order $(q - 1)/2$ and that H does not have a normal subgroup K such that $|\, H/K \,| \neq 1$ and is odd.

Let $X \subseteq \langle l\rangle$. Then $C_H(X) = \langle v, l\rangle L_1 L_2$ and $[H : C_H(l)] = 2$.

2.2 *Fusion of Involutions*

We shall show that G has two classes of involutions when $q \equiv -1 \pmod 4$.

(2.2.1) *A S_2-subgroup of H is an S_2-subgroup of G.*

Proof. This is obvious since Q, an S_2-subgroup of H, has cyclic center $\langle t\rangle$ (2.1.1).

(2.2.2) *The involution t_3 is not conjugate to t in G.*

Proof. By way of contradiction, suppose that t_3 is conjugate to t in G. Then there exists an S_2-subgroup S of $C_G(t_3)$ containing $\tilde{Q} = \langle b_1, b_2, t_4\rangle\langle u, v\rangle$ and $[S : \tilde{Q}] = 2$. Hence $\tilde{Q} \lhd S$. Let $x \in S - \tilde{Q}$. By (2.1.3), we may assume $E_1{}^x \subseteq \tilde{Q}$ is E_1, E_2 or E_3. If $E_1{}^x = E_1$, then $N(E_1) \not\subseteq H$. Suppose that $E_1{}^x = E_2$. It follows that $(E_1\tilde{Q}')^x = E_2\tilde{Q}'$. Both $E_1\tilde{Q}'$ and $E_2\tilde{Q}'$ are normal subgroups of an S_2-subgroup Q of G and so by Burnside's result [3, Ch. 7, 1.1] are conjugate in G if and only if they are conjugate in $N(Q) \subseteq N(Z(Q)) = N\langle t\rangle = H$, a contradiction to the structure of H. If $E_1{}^x = E_3$, then $E_2{}^y = E_2$ for a suitable $y \in S - \tilde{Q}$. Thus either $E_1{}^x = E_1$ or $E_2{}^y = E_2$ for some $x, y \in S - \tilde{Q}$.

(i) Suppose $E_1{}^x = E_1$ and $q \equiv 3 \pmod 8$. Then $|Q| = 2^7$ and $E_1 \lhd Q$. From the structure of H, we have $C(E_1) = E_1$ and so $\mathcal{N} = N(E_1)/E_1$ is isomorphic to a subgroup of $GL(4, 2) \cong A_8$. Clearly Q/E_1, dihedral of order 8, is a S_2-subgroup of $\mathcal{N}$.

Let $\mathcal{M} = O(\mathcal{N})$. Suppose that $\mathcal{M} \neq 1$. Consider the action of the four-group

$$\mathcal{F} = \langle b_1E_1, d_1E_1\rangle \subseteq \mathcal{N} \quad \text{on} \quad \mathcal{M}.$$

There exists an element $\sigma_1\sigma_2$ in $B \subseteq C\langle t, u\rangle$ of order 3 acting fixed-point-free on $\langle t_3, t_4\rangle$ and so $\sigma_1\sigma_2E_1 \in \mathcal{N}$. Moreover $\sigma_1\sigma_2E_1$ also acts fixed-point-free on $\mathcal{F}$. Hence using Brauer–Wilandt's result [7] and the fact that the centralizer of any involution in A_8 has order $2^6 \cdot 3$ or $2^5 \cdot 3$ [8], it follows that $|\mathcal{M}| = 3^3$ or 3. Since $|A_8| = 2^6 \cdot 3^2 \cdot 5 \cdot 7 \cdot$ the first case is not possible. Hence $|\mathcal{M}| = 3$ and so $\mathcal{M}\mathcal{F} = \mathcal{M} \times \mathcal{F}$. We shall now look at $N_{\mathcal{N}}(\mathcal{F}) = N\langle E_1, b_1, d_1\rangle \cap N(E_1)/E_1$. Since $Z\langle E_1, b_1, d_1\rangle = \langle t\rangle$, it follows that $N\langle E_1, b_1, d_1\rangle \subseteq H$ and so

$$N\langle E_1, b_1, d_1\rangle \cap N(E_1)/E_1 \cong A_4,$$

a contradiction to $\mathcal{M}\mathcal{F} \cong \mathcal{M} \times \mathcal{F}$. Thus $\mathcal{M} = 1$.

Next we consider $C_{\mathcal{N}}(b_1E_1) \supseteq Q/E_1$ where $\langle b_1E_1\rangle = Z(Q/E_1)$. Suppose that $Z(S/E_1) \subseteq \tilde{Q}/E_1$ is $\langle vE_1\rangle$ or $\langle b_1vE_1\rangle$. Then $\langle E_1, b_1\rangle$ is conjugate to $\langle E_1, v\rangle$ or $\langle E_1, b_1v\rangle$. This is a contradiction since $Z(E_1, v\rangle = \langle t, t_3, u\rangle$ and $Z\langle E_1, b_1v\rangle = \langle t, t_3, ut_4\rangle$ whereas $Z\langle E_1, b_1\rangle = \langle t, t_3\rangle$. Thus $Z(S/E_1) =$

$\langle b_1E_1\rangle$ showing that $|C_{\mathscr{N}}(b_1E_1)| > 8$ and also $\mathscr{N}$ has two classes of involutions since we already know all involutions in $\langle b_1E_1, d_1E_1\rangle$ are conjugate in $\mathscr{N}$. By our earlier remark about A_8, it follows that $|C_{\mathscr{N}}(b_1E_1)| = 2^3 \cdot 3$ and we may apply Gorenstein–Walter's result [4] to get $\mathscr{N} \cong PGL(2, r)$ where $r \pm 1 = \frac{1}{2}(24)$. But then $|\mathscr{N}|$ does not divide $|A_8|$. Hence E_1 cannot be normal in S.

(ii) $E_1{}^x = E_1$ and $q \equiv 7 \pmod 8$. Again we have $C(E_1) = E_1$ and $\mathscr{N} = N(E_1)/E_1$ is isomorphic to a subgroup of A_8. By an easy computation, $N_H(E_1)/E_1 \cong S_4$ and $\mathscr{F} = \langle c_1E_1, d_1E_1\rangle$ where $c_1 = b_1^{2^{\beta-2}}$ is an S_2-subgroup of $N_H(E_1)/E_1$. Since

$$Z\langle c_1, d_1, E_1\rangle = \langle t\rangle, \quad \langle c_1E_1, d_1E_1\rangle$$

is an S_2-subgroup of $\mathscr{N}$. In particular $\mathscr{N}$ has only one class of involutions. By a similar argument as in (i), $O(\mathscr{N}) = 1$.

Since $E_1{}^x = E_1$, $\langle x, c_1, E_1\rangle \subseteq S \cap N(E_1)$. Hence $\langle x, c_1\rangle E_1/E_1$ is an S_2-subgroup of $\mathscr{N}$ distinct from $\mathscr{F}$. Therefore $|C_{\mathscr{N}}(c_1E_1)| > 2^2$ and thus $|C_{\mathscr{N}}(c_1E_1)| = 2^2 \cdot 3$. By the result of Gorenstein–Waltor [4], it follows that $\mathscr{N} \cong L_2(r)$ where $r \pm 1 = 12$, a contradiction as before. So we have shown that E_1 is not normal in S.

By repeating the same argument to the case when $E_2{}^y = E_2$, this again leads to a contradiction showing the falsity for our assumption that t_3 is conjugate to t.

(2.2.3) *If $2^{\beta+4}$ divides the order of $C(ut)$* or *$C(u)$ then u and ut lie in different conjugate classes of G. Furthermore if $2^{\beta+4} \| C(ut)|$ and u is conjugate to t in G, then there exists an element z_1 in $C(B)$ such that $t^{z_1} = u$; $u^{z_1} = t$, $v^{z_1} = v$, or uvt.*

Proof. Suppose $2^{\beta+4}$ divides $|C(ut)|$. There exists a group $S \subseteq C(ut)$ of order $2^{\beta+4}$ containing

$$U = \langle t, u, v, b_1b_2, d_1d_2\rangle$$

of order $2^{\beta+3}$. It follows that $U \lhd S$. Let $z_1 \in S - U$. We have $Z(U) = \langle t, t_3, u\rangle$ and $U' = \langle b_1b_2\rangle$. Hence $Z(U) \cap U' = \langle t_3\rangle$ char U and so $t_3^{z_1} = t_3$. Now $Z(U)$ being characteristic in U is normalized by z_1. Thus $t^{z_1} \in \{t, tt_3, u, ut_3\}$. Clearly $t^{z_1} \neq t$ or tt_3 since $z_1 \notin H$ and $tt_3 \sim_H t_3$. It follows that $t^{z_1} = u$ or ut_3 and correspondingly $(tt_3)^{z_1} = ut_3$ or u. By (2.2.2) and the fact that $ut_3 \sim_H ut$ we have proved the first part of the lemma. If $2^{\beta+4} \| C(u)|$, we prove in the same way that u and ut lie in different conjugate classes of G.

Suppose $2^{\beta+4} \| C(ut)|$ and $u \sim t$, it follows that $t^{z_1} = u$ and $u^{z_1} = t$ since $z_1{}^2 \in U \subseteq C\langle t, u\rangle$. Thus $z_1 \in N\langle t, u\rangle$ and therefore z_1 normalizes $C\langle t, u\rangle$. Since $B = (C\langle t, u\rangle)'$, $z_1 \in N(B)$. Because $q = p^f \equiv -1 \pmod 4$,

f is odd. The outer automorphism group of $B \simeq L_2(q)$ has order $2f$. Hence replacing z_1 by z_1x, where $x \in \langle v \rangle B$ if necessary, we get that $z_1 \in C(B)$ without affecting our earlier conclusions. Finally we must have $v^{z_1} = vy$ for some $y \in \langle t, u \rangle B$. Since $vz_1^{-1}vz_1$ centralizes B, it follows that $y \in \langle t, u \rangle$. If $y = t$, then $v^{z_1^2} = uvt$, a contradiction since $z_1^2 \in H$ and v is not conjugate to uvt in H. Similarly $y \neq u$, and we are done.

(2.2.4) *If $2^{\beta+4}$ divides the order of $C(uvt)$ or $C(uv)$, then uv and uvt lie in different classes of G. Furthermore if $2^{\beta+4} \mid |C(uv)|$ and uv is conjugate to t in G, then there exists an element z_2 in $C(C)$, such that $t^{z_2} = uv$, $(uv)^{z_2} = t$, $v^{z_2} = v$, or ut.*

Proof. As in (2.2.3).

(2.2.5) *The involution t is conjugate to an element in $\{u, v, uv\}$.*

Proof. By way of contradiction suppose that G is 2-normal. Since $\langle t \rangle$ is the center of an S_2-subgroup Q of G, it follows from Hall–Grün's theorem [3, Ch. 7, 5.2], that the greatest 2-factor group of G is isomorphic to that of $N(Z(Q)) = H$, i.e., to $H/L_1L_2\langle l \rangle$, a four-group. This is a contradiction to condition (a) of the theorem.

Because G is not 2-normal, it implies that there exists x in G such that $t \in Q \cap Q^x$ but $\langle t \rangle$ is not the center of Q^x. So $t^x \neq t$. On the other hand $t \in Q^x$ and hence t and t^x commute, i.e., $t^x \in H$. Without loss of generality we may assume that $t^x \in \{u, ut, v, uv, uvt\}$ by (2.1.2) and (2.2.2). Interchanging u by ut and/or v by vt, if necessary, we get that $t^x \in \{u, v, uv\}$. This completes the proof.

Our next lemma is crucial to the whole paper.

(2.2.6) *The group G has precisely two classes of involutions $\mathscr{K}_1$ and $\mathscr{K}_2$ with the representatives t and ut, respectively: $\mathscr{K}_1 \cap H$ is the union of four conjugate classes of H with representatives t, u, uv, v; $\mathscr{K}_2 \cap H$ is the union of three conjugate classes with representatives t_3, ut, uvt.*

Proof. Suppose that $u \sim t$. Then by the proof of (2.2.3) $ut \sim t_3$. Hence the subgroup $\langle u, b_1, b_2, d_1, d_2 \rangle$, a maximal subgroup of Q, has two classes of involutions in G with representatives t and t_3. Since G has no subgroup of index 2, by Thompson's lemma [3, Ch. 7, Ex. 3], v, uv, uvt are conjugate to t or t_3. By (2.2.4), interchanging v by vt, if necessary, it follows that $uv \sim t$ and $uvt \sim t_3$. To decide whether v is conjugate to t or t_3. we use (2.2.3) and (2.2.4) to get the following possibilities:

(i) $v^{z_1} = v$, $v^{z_2} = ut$. Then $(vt)^{z_1} = uv$. This is a contradiction since $v \sim_H vt$ whereas ut and uv lie in different conjugate classes of G.

(ii) $v^{z_1} = uvt$, $v^{z_2} = v$. Then $(vt)^{z_2} = u$, again a contradiction as before.

(iii) $v^{z_1} = uvt$, $v^{z_2} = ut$. Then $(C\langle t, v\rangle)^{z_1} = C\langle u, uvt\rangle$ and so, by (2.1.3) has an S_2-subgroup of order 2^4. We compute from (2.2.4) that $z_2 \in C\langle u, uvt\rangle$ and $z_2 \in N\langle u, v, t, t_3\rangle$. Hence

$$\langle z_2, u, v, t, t_3\rangle \subseteq C\langle u, uvt\rangle$$

has order at least 2^5, a contradiction.

Thus we must be in case (iv).

(iv) $v^{z_1} = v$, $v^{z_2} = v$. Then it follows $(vt)^{z_1} = uv \sim t$, proving all the assertions of the lemma.

If $uv \sim t$, then using exactly the same argument as before, the lemma follows.

If $v \sim t$, then $M = \langle v, b_1, b_2, d_1, d_2\rangle$ is a maximal subgroup of Q and has two classes of involutions in G by our assumption and (2.2.2). By Thompson's lemma [3] u, ut, uv, uvt are conjugate to t or t_3. Using (2.2.3) and (2.2.4), interchanging u by ut and/or v by vt if necessary, the lemma follows.

Since one of the three cases must happen by (2.2.5), the proof is complete.

As a consequence of the above lemma, $v^{z_1} = v$ and $v^{z_2} = v$.

(2.3) *Centralizer of an involution in $\mathscr{K}_2$.*

We begin this section with a closer look at the structure of an S_2-subgroup $\tilde{Q} = \langle u, v, b_1, b_2, d_1d_2\rangle$ of $C_H(t_3)$. Obviously $\tilde{Q}$ is an S_2-subgroup of $C_G(t_3)$. We note that vd_1d_2 is an element of order 2^β and $(vd_1d_2)^{2^{\beta-1}} = t_3$. The centralizer $C_{\tilde{Q}}(vd_1d_2)$ is $\langle vd_1d_2\rangle \times \langle vb_1d_1d_2, ut\rangle$ of order $2^{2\beta+1}$. The group $\langle vb_1d_1d_2, ut\rangle$ is dihedral of order $2^{\beta+1}$ and all its involutions lie in $\mathscr{K}_2$. The element vd_1d_2 is inverted by elements in $\tilde{Q} - C_{\tilde{Q}}\langle vd_1d_2\rangle$.

Let

$$K = N\langle vd_1d_2, vb_1d_1d_2, ut\rangle \cap C_G(t_3).$$

Since

$$\langle t, t_3\rangle = \Omega_1(Z\langle vd_1d_2, vb_1d_1d_2, ut\rangle),$$

it follows that

$$K \subseteq N\langle t, t_3\rangle \cap C(t_3).$$

By (2.2.2), $K \subseteq C\langle t, t_3\rangle$ and so $K = \tilde{Q} \times \langle l\rangle$.

Now let S be an S_2-subgroup of $C(ut)$ containing $U = \langle t, u, v, b_1b_2, d_1d_2\rangle$. By (2.2.6), $S \simeq \tilde{Q}$. Hence there is an element $s \in S$ conjugate to vd_1d_2 and we have $U \cap \langle s\rangle = \langle ut\rangle$. Clearly $t \notin C(s)$ and so by the structure of $\tilde{Q}$, t inverts s. Since $C_S(s)$ is of index 2 in S, either vt or v belongs to $C_S(s)$. Suppose that $vt \in C_S(s)$. Then $(s^{2^{\beta-2}})^{-1}\, vt \cdot t(s^{2^{\beta-2}}) = uvt$, a contradiction to (2.2.6). Hence $v \in C_S(s)$. Similarly we show that $d_1d_2 \in C_S(s)$. Hence

$$C_S(s) = \langle s\rangle \times \langle uvt\, d_1d_2, uvt\rangle.$$

We note that $\langle uvt\, d_1d_2 , uvt \rangle$ is dihedral of order $2^{\beta+1}$ and all its involutions lie in $\mathcal{K}_2$.

We shall next show a series of minor results in preparation for the determination of the structure of $C(ut)$.

(i) *The involution t is not conjugate to involutions of $\langle ut, t_3\rangle$ in $C(ut)$.*

It is only necessary to show that t is not conjugate to utt_3 in $C(ut)$ since ut is a central involution and $t_3 \in \mathcal{K}_2$.

We have $Z(S) = \langle ut, t_3\rangle$ and so it is conjugate to $Z(\tilde{Q}) = \langle tt_3 , t_3\rangle$. Hence

$$| C\langle ut, t_3\rangle | = | C\langle tt_3 , t_3\rangle | = 2(q-1)(q+1)^2.$$

On the other hand,

$$| C\langle t, ut\rangle | = 2^2 \cdot q(q^2-1).$$

Hence t is not conjugate to utt_3 in $C(ut)$.

(ii) *The group $C(ut)$ has a subgroup M of index 2 such that*

$$\langle s\rangle \times \langle uvt\, d_1d_2 , uvt\rangle \subseteq M.$$

Let S^* be the focal group of S in $C(ut)$. By definition,

$$S^* = \langle xy^{-1} \mid x, y \in S, x \underset{C(ut)}{\sim} y\rangle.$$

Since $B \subseteq C(ut)$; there exists an element $b \in B$ such that $d_1d_2 = t_3{}^b \cdot t_3$ and so $d_1d_2 \in S^*$. By (2.2.4) and (2.2.6), $z_2 \in C(ut)$. Since $tt_3 \in C$ and $z_2 \in C(C)$ we compute that $(uvtt_3)^{z_2} = t_3$. Hence $uvt \in S^*$. Also $s^2 \in S^*$ since t inverts s. Thus

$$\tilde{S} = \langle s^2\rangle \times \langle d_1d_2 , uvt\rangle \subseteq S^*.$$

An element sx in $s\tilde{S}$ is either a root of ut or utt_3 and $O(sx) > 2$. But elements in $t\tilde{S}$ are either involutions or roots of t_3. Since t_3, ut, utt_3 are not conjugate to one another in $C(ut)$, no element in $s\tilde{S}$ can be conjugate to an element in $t\tilde{S}$. Similarly no element in $s\tilde{S}$ can be conjugate to an element in $ts\tilde{S}$ in $C(ut)$. It follows, then, either $S^* = \tilde{S}$ or $S^* = \langle s\rangle \times \langle d_1d_2 , uvt\rangle$. In either case, there exists a subgroup M of index 2 in $C(ut)$ and $\langle s\rangle \times \langle d_1d_2 , uvt\rangle \subseteq M$.

(iii) *Let K be 2-commutator group of M. Then $K/O(K)$ is isomorphic to $L_2(q^2)$.*

By the first theorem of Grün [3, Ch. 7, 4.2], M/K is isomorphic to $\tilde{S}/\tilde{S}^*$ where $\tilde{S}^* = \langle \tilde{S} \cap N_M(\tilde{S})', \tilde{S} \cap (\tilde{S}')^x \mid x \in M\rangle$. The remarks at the beginning show that $N_M(\tilde{S}) = \tilde{S} \times \langle l'\rangle$ and so

$$\tilde{S} \cap N_M(\tilde{S})' = \tilde{S}' = \langle (uvt\, d_1d_2)^2\rangle = \langle b_1b_2\rangle.$$

Since $B \subseteq M$, there is an element $b \in B$ such that $\langle d_1d_2\rangle \subseteq \tilde{S} \cap (\tilde{S}')^b$. Either z_2 or tz_2 is in M. In any case

$$(t_3)^{z_2} = t_3^{z_2t} = uvtt_3\,.$$

Hence $\langle uvt, d_1d_2\rangle \subseteq \tilde{S}^*$.

Suppose there is an $x \in M$ such that $x^{-1}(b_1b_2)^ix = s^jy$ for some $y \in \langle uvt, d_1d_2\rangle$, and $s^j \neq 1$. If $O(s^j) \geqslant O(y)$, then s^jy is a root of ut or utt_3. Hence s^jy cannot be conjugate to $(b_1b_2)^i$ which is a root of t_3. If $O(s^j) < O(y)$, then $O(y) > 2$. Therefore $y = (b_1b_2)^k$. Both $\langle(b_1b_2)^i\rangle$ and $\langle s^j(b_1b_2)^k\rangle$ are normal subgroups of $\tilde{S}$. By Burnside's theorem [3, Ch. 7, 4.3], they are conjugate in $N_M(\tilde{S})$, a contradiction. Thus we have shown that $\tilde{S}^* = \langle d_1d_2\,, uvt\rangle$. Hence an S_2-subgroup $\tilde{S}^*$ of K is dihedral of order $2^{\beta+1}$.

Next we shall show that K has only one class of involutions. Since $B \simeq L_2(q)$ does not have a 2-factor group, $B \subseteq K$ and so d_1d_2 is conjugate to t_3 in K. For a suitable i, $s^iz_2 \in K$ and then $t_3^{s^iz_2} = uvtt_3$. Hence K has only one class of involutions. Since

$$C(t_3) \cap K \subseteq C(t_3) \cap C(ut) \simeq C(t, t_3).$$

$C(t_3) \cap K$ has Abelian 2-complement. By the result of Gorenstein–Walter [4] $K/O(K) \simeq A_7$ or $L_2(r)$. The case $K/O(K) \simeq A_7$ is possible only if $q = 3$ since $K/O(K)$ contains

$$B\langle uvt\rangle\, O(K)/O(K) \simeq PGL(2, q).$$

If $q = 3$, then $|\, C\langle ut, t_3\rangle| = 2^6$. But the centralizer of an involution in A_7 has order $2^3 \cdot 3$, a contradiction. Since $K/O(K)$ contains a subgroup isomorphic to $PGL(2, q)$, it follows that q^2 divides r, [5, Ka. *II*, 8.27]. On the other hand

$$(C(t_3) \cap K)\langle s, t\rangle = C(t_3) \cap C(ut) = C_G\langle t, t_3\rangle$$

and so

$$|\, C(t_3) \cap K\,| = (q^2 - 1)e.$$

Hence $r = q^2$, proving our result.

(iv) *The group K is a direct product of a cyclic group $O(K)$ of order e and a group D isomorphic to $L_2(q^2)$. Moreover, $B\langle uvt\rangle \subseteq D$, $\langle s\rangle\, O(K)$ is cyclic of order $q + 1$ and t inverts $\langle s\rangle\, O(K)$.*

Since $C_{K/O(K)}(t_3O(K)) = C_K(t_3)\, O(K)/O(K)$ and the fact that the centralizer of an involution in $L_2(q^2)$ has order $q^2 - 1$, we have $|\, C_K(t_3)\, O(K)/O(K)| = q^2 - 1$. Since $|\, C_K(t_3)| = (q^2 - 1)e$, $|\, C_{O(K)}(t_3)| = e$.

Because $L_2(q^2)$ is simple, clearly K is the smallest normal subgroup of M

with a 2-factor group. So $O(K)$ char K char M. It follows that $O(K) \lhd C(ut)$. Hence $\langle v, t\rangle$ acts on $O(K)$. Since

$$C(t) \cap C(ut) = \langle t, u, v\rangle B$$

does not have normal subgroup of odd order, $C_{O(K)}(t) = 1$. By (2.2.3) and (2.2.4), z_1, z_2 are in $C(ut)$ and $t^{z_2 z_1} = vt$. So $C_{O(K)}(vt) = 1$. By the theorem of Brauer–Wielandt [7],

$$| O(K)| = | C_{O(K)}(v)| = | C_{O(K)}(uvt)| = | C_{(OK)}(t_3)| = e.$$

Hence

$$O(K) \subseteq C(t_3) \cap C(ut) \cong C\langle t, t_3\rangle$$

and so $O(K)$ is cyclic.

When $e = 1$, the assertions of the lemma are now clear. Suppose $e \neq 1$. Since B does not have a normal subgroup of odd order, $B \cap O(K) = 1$. Therefore $BO(K)$ is a splitting extension of $O(K)$ by B. We have $[K : BO(K)] = q(q^2 + 1)$ which is prime to e. By a result of Gaschütz [5, Ka.I, 17.4], K splits over $O(K)$. This means there exists a subgroup $D \cong L_2(q^2)$ such that $K = DO(K)$ and $D \cap O(K) = 1$. Since centralizers of all involutions of D contains $O(K)$, and D is generated by involutions, $DO(K) = D \times O(K)$. Clearly $B\langle uvt\rangle \subseteq D$.

From the fact that $C(vd_1d_2) \cap C(tt_3)$ is a subgroup of index 2 in $C\langle t, t_3\rangle$ it follows that $C(s) \cap C(t_3)$ is a subgroup of index 2 in $C(ut) \cap C(t_3)$ and $O(K) \subseteq C(s)$, i.e., $O(K)\langle s\rangle$ is cyclic of order $q + 1$. By the structure of $C(t) \cap C(t_3)$ it follows that t invests $O(K)\langle s\rangle$.

Using all the results obtained so far, we are able to prove the following important lemma.

(2.3.1) *The centralizer $C(ut)$ of ut in G has the following structure:*

$$C(ut) = (\langle \kappa\rangle \times D)\langle t\rangle$$

where $\langle \kappa\rangle$ is cyclic of order $q + 1$; $D \cong L_2(q^2)$, $\langle t\rangle D$ is isomorphic to the extension of $L_2(q^2)$ by the field automorphisms of order 2, and t inverts $\langle \kappa\rangle$.

Proof. From (iv), we have $D \lhd C(ut)$. The factor group $\mathscr{F} = C(ut)/(C(D) \cap C(ut))D$ is a 2-group since $O(K) \subseteq C(D) \cap C(ut)$. Because $q = p^f \equiv -1 \pmod 4$, f is odd. It follows that an S_2-subgroup of the outer automorphism group of $L_2(q^2)$ is a four-group. The group $C(ut)$ cannot involve $PGL(2, q^2)$ because an S_2-subgroup of $PGL(2, q^2)$ is dihedral of order $2^{\beta+2}$ and has an element of order $2^{\beta+1}$ whereas $C(ut)$ does not have such an element. Thus $| \mathscr{F} | = 1$ or 2.

Suppose that $t \in (C(D) \cap C(ut))D$. Then $t = xy$ where $x \in C(D) \cap C(ut)$, $y \in D$. Both t and x centralize $B\langle uvt\rangle$ and so y centralizes $B\langle uvt\rangle$. By the structure of $L_2(q^2)$, this implies $y = 1$. Then $t \in C(D)$, a contradiction. Hence $t \notin (C(D) \cap C(ut))D$. So $|\mathscr{F}| = 2$.

Since $(C(D) \cap C(ut))D/D$ is a subgroup of index 2 in $C(ut)/D \simeq \langle t, s, O(K)\rangle$ and $(C(D) \cap C(ut))D/D \simeq C(D) \cap C(ut)$, we get that $C(D) \cap C(ut)$ is either cyclic or dihedral of order $q + 1$. Suppose that it is dihedral. Let $z \neq ut$ be an involution of $C(D) \cap C(ut)$. Clearly $z \in \mathscr{K}_2$ and D is the unique subgroup of $C(z)$ isomorphic to $L_2(q^2)$. Let $K = (C(D) \cap C(z))D$ be a subgroup of index 2 in $C(z)$. We shall look at the centralizer of the four-group $\langle z, v\rangle$. Since

$$|C(v) \cap K| = 2(q^2 - 1), \quad |C(v) \cap C(z)| = 2^2 \cdot (q^2 - 1) \quad \text{or} \quad 2 \cdot (q^2 - 1).$$

But this is a contradiction since $C\langle x, t\rangle$ has order $2(q - 1)(q + 1)^2$ or $2^2q(q^2 - 1)$ for all $x \in \mathscr{K}_2 \cap H$. Hence we have shown that $C(D) \cap C(ut) = \langle\kappa\rangle$ is cyclic of order $q + 1$. Since $\langle\kappa\rangle = Z(\langle\kappa\rangle \times D)$ char $\langle\kappa\rangle \times D$, t normalizes $\langle\kappa\rangle$. Because $C(ut)/D$ is dihedral, t must invert κ. We have $D = (\langle\kappa\rangle \times D)'$ and so is normalized by t inducing outer automorphism on D.

Let $\mathscr{A}$ be the extension of $PGL(2, q)$ by the field automorphism σ of order 2. Let ζ be a primitive element of the finite field F_{q^2}. Set

$$\omega = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}; \qquad \gamma = \begin{pmatrix} \zeta^{de} & 0 \\ 0 & \zeta^{-de} \end{pmatrix}; \qquad \delta = \begin{pmatrix} 1 & \\ & \zeta^{de} \end{pmatrix} \sigma$$

where $q^2 - 1 = 2^{\beta+1} de$. We verify that

$$\omega^2 = 1 = \gamma^{2^\beta}, \quad \omega\gamma\omega = \gamma^{-1}, \quad \delta^{-1}\gamma\delta = \gamma^{-1};$$

$$\delta^2 = \gamma^{-(q+1)/2};$$

$$\delta^{-1}\omega\delta = \gamma^{q\beta} \,(\mathrm{mod}\; Z(GL(2, q^2))).$$

We check that $\langle\omega, \gamma, \delta\rangle$ is an S_2-subgroup of $\langle L_2(q^2), \delta\rangle$. We compute that

$$(\delta\omega)^2 = \delta^2\delta^{-1}\omega\,\delta\omega = \gamma^{-(q+1)/2}\gamma^{q}\omega\omega\gamma^{(q-1)/2}.$$

Since $(q - 1)/2$ is odd $\delta\omega$ has order $2^{\beta+1}$. By our earlier remark, $C(ut)$ does not have an element of order $2^{\beta+1}$. It follows that $D\langle t\rangle \simeq \langle L_2(q^2), \sigma\rangle$ and the lemma is proved.

(2.4) *Some subgroups of G.*

(2.4.1) *There exists an element μ satisfying the following relations*:

$$\mu^2 = v; \quad t^\mu = vt; \quad t_3{}^\mu = uvtt_3; \quad u^\mu = uv,$$

$$\langle l\rangle^\mu = \langle m\rangle; \quad \langle m\rangle^\mu = \langle l\rangle \qquad \text{and} \qquad n^\mu = n.$$

Proof. Let λ' be an element of order $(q^2-1)/2$ in $D \subseteq C(ut)$ such that $uvt \in \langle\lambda'\rangle$. Set $\mu = \kappa^{(q+1)/4}\lambda'^{(q^2-1)/8}$. Then $\mu^2 = v$ and $t^\mu = vt$. Since $\mu \in C(ut)$, $u^\mu = uv$. Because $t_3 \in D$ and $t_3 \in C_D(uvt)$ which is dihedral, by the structure of $L_2(q^2)$, we have $t_3{}^\mu = uvtt_3$.

Suppose that $\langle l\rangle \neq 1$. From the above relations we see that $\mu \in N\langle t, v\rangle$ and so μ normalizes $\langle l, m, n\rangle$, which is the normal 2-complement of $C\langle t, v\rangle$. Since $\langle l\rangle$ centralizes t_3, $\langle l^\mu\rangle$ centralizes $t_3{}^\mu = uvtt_3$. On the other hand

$$C(uvtt_3) \cap \langle l, m, n\rangle = \langle m\rangle.$$

Hence

$$\langle l\rangle^\mu = \langle m\rangle \qquad \text{and} \qquad \langle m\rangle^\mu = \langle l\rangle^{\mu^2} = \langle l\rangle$$

Since $n \in B \subseteq D$ and $\langle n\rangle \subseteq C_D(uvt)$, both κ and λ' centralize n and so $n^\mu = n$. The proof is now complete.

(2.4.2) *Let $F = \langle t, v\rangle\langle l, m, n\rangle$. The normalizer $N = N\langle t, v\rangle$ of $\langle t, v\rangle$ in G is the group $\langle u, c_2, ut, t_3, F\rangle$ and N/F is isomorphic to the symmetric group on four letters. Moreover, $(\mu c_2)^3 = 1 = (c_2\mu ut)^3$.*

Proof. By (2.4.1), $\mu \in N\langle t, v\rangle$ and from the action of μ on $\langle t, v\rangle$, $\mu \notin \langle c_2, C\langle t, v\rangle\rangle$. Since $C\langle v, t\rangle = \langle u, t_3\rangle F$ and because the automorphism group of a four-group has order 6, it follows that N/F has order 24.

Let r_1, r_2, r_3 be the cosets μF, c_2F, and μutF, respectively. We check that

$$r_1{}^2 = r_2{}^2 = r_3{}^2 = 1, \qquad r_1r_3 = r_3r_1.$$

By an easy computation, we verify that $(\mu c_2)^3$ and $(c_2\mu ut)^3$ is in $Z(C\langle t, v\rangle) = \langle v, t\rangle$ and since both μc_2 and $c_2\mu ut$ act fixed-point-free on $\langle v, t\rangle$, it follows $(\mu c_2)^3 = 1 = (c_2\mu ut)^3$ proving our lemma.

(2.5) *S_p-subgroups of G.*

With Lemmas (2.4.1) and (2.4.2), we are now able to determine the structure of a p-subgroup of G, which turns out eventually to be an S_p-subgroup of G.

Let W be the unique S_p-subgroup of D containing

$$T = \langle(\theta_1\theta_2)^x \mid x \in \langle v, n\rangle\rangle.$$

We have $C(ut) \cap C(W) = \langle\kappa\rangle W$ and

$$C(ut) \cap N(W) = \langle t, \kappa, \lambda'\rangle W.$$

Here we have used the fact W is a TI group in D; t, κ, $\langle\lambda'\rangle \supseteq \langle m, uvt\rangle$ normalize a subgroup T of W. Clearly $\langle\kappa^e\rangle$ is an S_2-subgroup of $C(W)$ and is cyclic. By the transfer theorem of Burnside [3, Ch. 7, 4.3], $C(W)$ has a normal 2-complement M and $C(W) = \langle \kappa^e \rangle M$. Since M is a characteristic subgroup of $C(W)$, $M \lhd N(W)$. Furthermore, by the Frattini argument

$$N(W) = (N\langle \kappa^e \rangle \cap N(W))\, C(W) = (C(ut) \cap N(W))\, C(W) = \langle t, \kappa, \lambda' \rangle M.$$

We note that an S_p-subgroup of $C(W)$ is also an S_p-subgroup of $N(W)$.

The four group $\langle u, t \rangle$ acts on M. Consider

$$C_M(t) \subseteq C(T) \cap C(t) = \langle l, t \rangle\, T_1 T_2 .$$

Suppose that a nontrivial subgroup X of $\langle \kappa \rangle$ is in $C_M(t)$. Then $X^\mu \subseteq \langle m \rangle$ is in M since $\mu \in N(W)$. (See 2.4.1). This is a contradiction since no subgroup of $\langle m \rangle$ can centralize T. If $(T_1 T_2 - T) \cap M \neq \varnothing$, it implies that there is $1 \neq x \in T_1 \cap M$. But then

$$T_1 = \langle x^y \mid y \in \langle uvt, n \rangle \rangle \subseteq M$$

since $\langle uvt, n \rangle \subseteq \langle \lambda' \rangle$ and so $C_M(t) = T_1 T_2$. Therefore, either $C_M(t) = T$ or $T_1 T_2$. By the theorem of Brauer–Wielandt [7],

$$| M | \, | C_M \langle t, u \rangle |^2 = | C_M(ut) | \, | C_M(t) | \, | C_M(u) |,$$

i.e., $| M | = q^2 e$ or $q^4 e$ since

$$C_M(u) = (\kappa^{(q+1)/4})^{-1}\, C_M(t)\, \kappa^{(q+1)/4}.$$

Hence an S_p-subgroup of $N(W)$ has order q^2 or q^4.

Suppose $| M | = q^2 e$. This means that W is an S_p-subgroup of G and so is $T_1 T_2$. However,

$$C(T_1 T_2) \cap C(t) = \langle t, l \rangle\, T_1 T_2$$

and clearly $\langle t \rangle$ is an S_2-subgroup of $C(T_1 T_2)$. This is a contradiction since $C(W)$ has an S_2-subgroup $\langle \kappa^e \rangle$ of order 2^β and $\beta > 1$. Thus $| M | = q^4 e$.

Hence we have $C_M(t) = T_1 T_2$. Since $\mu \in N(W)$,

$$C_M(vt) = (C_M(t)^\mu = T_1{}^\mu T_2{}^\mu = T_3 T_4$$

where $T_3 = T_1{}^\mu$, $T_4 = T_2{}^\mu$. By the result of Brauer–Wielandt [7], $| C_M(v) | = e$. Again $\langle ut, uvt \rangle \subseteq N(W)$ acts on M and, by the result of Brauer–Wielandt [7], $| C_M(uvt) | = q^2 e$. Since uvt is conjugate to ut in G, a group of order q^2 is normal in any subgroup of odd order containing it. In other words we have shown that M contains a normal S_p-subgroup R. It follows that $\langle T_1, T_2, T_3, T_4 \rangle = R$ and is elementary Abelian of order q^4 since R is a direct product of W with the normal elementary Abelian group of order q^2 in $C_M(uvt)$. Thus we have proved the following:

(2.5.1) *The group* $R = \langle T_1, T_2, T_1^{\mu}, T_2^{\mu}\rangle$ *is elementary Abelian of order* q^4.

We are interested next in the structure of $C(T_1)$ and prove the following result:

(2.5.2) *Let*

$$\theta_3 = \theta_1^{\mu};\quad \theta_4 = \theta_2^{\mu};\quad \theta_5 = \theta_3^{c_2};\quad \theta_6 = \theta_4^{c_2};$$

$$T_3 = T_1^{\mu};\quad T_4 = T_2^{\mu};\quad T_5 = T_3^{c_2};\quad T_6 = T_5^{c_2}$$

Then

$$P = T_1T_2T_3T_4T_5T_6$$

is a p-subgroup of G *of order* q^6 *and* $B = PF$ *is a subgroup of order* $\frac{1}{2}(q-1)^3 q^6$ *with* $F \subseteq N(P)$.

Proof. We have $C(T_1) \cap C(t) = L_2\langle l\rangle T_1$ where $L_2 \simeq SL(2, q)$. An S_2-subgroup of L_2 is a generalized quaternion group of order $2^{\beta+1}$. Obviously it is also an S_2-subgroup of $C(T_1)$. By the theorem of Brauer–Suzuki [3, Ch. 12, 1.1], $C(T_1) = (C(t) \cap C(T_1))U$ where $U = O(C(T_1))$. Clearly $T_1 \subseteq U$ and since $\langle l\rangle = Z(L_2\langle l\rangle)$ has odd order, $\langle l\rangle \subseteq U$. It follows that $C(T_1) = L_2U$ and $L_2 \cap U = 1$ since L_2 has no nontrivial normal subgroup of odd order.

By (2.5.1), we see that $C(vt) \cap U \supseteq \langle l\rangle T_3T_4$. From the isomorphism of $C(vt)$ with $C(t)$, the largest odd order subgroup containing T_1T_2 in $C(t)$ is $\langle l, m, n\rangle\ T_1T_2$. It follows that

$$C(vt) \cap U \subseteq (\langle l, m, n\rangle\ T_1T_2)^{\mu} = \langle l, m, n\rangle\ T_3T_4$$

and so

$$C(vt) \cap U = \langle l\rangle\ T_3T_4 .$$

Also

$$C(v) \cap U = (C(vt) \cap U)^{c_2} = \langle l\rangle\ T_5T_6$$

where

$$T_5 = T_3^{c_2};\quad T_6 = T_4^{c_2}.$$

By the theorem of Brauer–Wielandt $|U| = q^5 \cdot (q-1)/2$.

Suppose that $\langle l\rangle \neq 1$. Then $\langle l\rangle = \langle m\rangle^{\mu}$ normalizes $(T_1T_2)^{\mu} = T_3T_4$ and similarly $\langle l\rangle^{c_2} = \langle l\rangle$ normalizes $(T_3T_4)^{c_2} = T_5T_6$. By Gorenstein–Walter's lemma [4], every element of U has the unique expression $l^i xyz$ where $x \in T_1$, $y \in T_3T_4$, $z \in T_5T_6$. Let $\langle r\rangle = X \subseteq \langle l\rangle$ and $g_1g_2 \in N_U(X)$ where $g_1 \in T_5T_6$, $g_2 \in T_5T_6$. Then $(g_1g_2)^{-1}\, rg_1g_2 = r^j$, i.e., $rg_1g_2 = r^j(g_1^{r^j})(g_2)^{r^j}$. By the unique expression for elements of U and the fact that $g_1^{r^j} \in T_3T_4$, $g_2^{r^j} \in T_5T_6$, it follows that $r = r^j$, $g_1 = g_1^{r^j}$, $g_2 = g_2^{r^j}$. In other words $N_U(X) = C_U(X)$.

This in turn implies that U has a normal $\tilde{p}$-complement for every prime $\tilde{p}$ dividing $(q-1)/2$ by the transfer theorem of Burnside [3, Ch. 7, 4.3]. It follows that U has a normal p-subgroup V. Obviously

$$\langle T_1, T_3, T_4, T_5, T_6\rangle \subseteq V \qquad \text{and thus} \quad V = T_1T_3T_4T_5T_6 .$$

Since V char U, V is normal in $N(T_1)$.

It is clear now that $P = T_2V$ is a p-group of order q^6. Since $F \subseteq N(T_2)$ and $F \subseteq N(T_1)$, $B = PF$ is a group of order $\frac{1}{2}(q-1)^3 q^6$ and $F \subseteq N(P)$.

3. The case $q \equiv 1 \pmod 4$.

Here $\alpha \geqslant 2, \beta = 1$, and H is a nonsplitting extension of the central product L_1L_2 by the dihedral group $\langle u, w\rangle$ with

$$\langle u, w\rangle \cap L_1L_2 = \langle w^{(q-1)/2}\rangle = \langle(\alpha_1\alpha_2)^{(q-1)/4}\rangle$$

(See Section 1 for notation).

(3.1.1) *S_2-subgroup of H.*

Set

$$a_1 = \alpha_1{}^d; \quad a_2 = ua_1u; \quad c_2 = uc_1u; \quad v = w^d.$$

It is easily seen that

$$Q = \langle u, v\rangle\langle a_1, c_1, a_2, c_2\rangle$$

is an S_2-subgroup of H and $Z\langle Q\rangle = \langle t\rangle$. The group $Q_i = \langle a_i, c_i\rangle$ is a generalized quaternion group. Further we have the following relations:

$$[a_i, v] = 1, \; c_1{}^v = a_1c_1 ; \qquad c_2{}^v = a_2^{-1}c_2 .$$

(3.1.2) *Conjugate classes of involutions in H*

Exactly as in the previous case, involutions in $Q_1Q_2 - \langle t\rangle$ lie in one conjugate class of H with representative $t_3 = c_1c_2$.

Suppose that $uv^{2i}x_1y_2$ is an involution where $x_1 \in L_1$, $y_2 \in L_2$. Then $y_2 = (v^{-2i}x_2^{-1}v^{2i})h$ where $h = 1$ or t. Hence all involutions in $uv^{2i}Q_1Q_2 - Q_1Q_2$ have the forms $(u)^{v^ix_1}$ or $(ut)^{v^ix_1}$. It follows that they all lie in one conjugate class with representative u since $ut = (a_1v)^{-2^{\alpha-2}}u(a_1v)^{2^{\alpha-2}}$. Similarly all involutions in $uv^{2i+1}Q_1Q_2 - Q_1Q_2$ are conjugate to uv in H.

If $q \equiv 5(8)$, $\alpha = 2$. Then $(vQ_1Q_2 \cup v^{-1}Q_1Q_2) - Q_1Q_2$ does not have involutions. If $q \equiv 1(8)$, by a straight-forward but tedious computation, all involutions in $v^iQ_1Q_2 - Q_1Q_2$ are conjugate to $z = v^{2^{\alpha-2}}(a_1a_2)^{2^{\alpha-3}}$.

Hence we have shown that H has four conjugate classes of involutions with representatives t, t_3, u, and uv when $q \equiv 5(8)$. When $q \equiv 1(8)$, H has five conjugate classes of involutions with representatives t, t_3, u, uv, and z.

(3.1.3) *Centralizers of involutions in H*

Let $s = (v)^{2^{\alpha-1}} = (\alpha_1\alpha_2)^{2^{\alpha-2}}$. Then

$$C_H(s) = \langle u, w\rangle\langle\alpha_1, \alpha_2, t_3\rangle$$

where $t_3 = c_1c_2$ of order $(q-1)^3$. Set

$$l = (w^2\alpha_1\alpha_2^{-1})^{2\alpha-1}; \qquad m = (\alpha_1^{\ 1}\alpha_2)^{2\alpha-1}; \qquad n = (\alpha_1\alpha_2)^{2\alpha-1}.$$

We may write

$$C_H(s) = \langle u, v\rangle\langle a_1, a_2, t_3\rangle\langle l, m, n\rangle$$

where $\langle l, m, n\rangle$ is the normal 2-complement of $C_H\langle s\rangle$ of order d^3.

The centralizer $C_H(u)$ of u in H is $\langle t, u\rangle B$ where

$$B = \langle x_1x_2 \mid x \in SL(2, q)\rangle \cong L_2(q).$$

Similarly $C_H(uv) \cong \langle t, uv\rangle C$ where

$$C = \langle x_1v^{-1}x_2v \mid x \in SL(2, q)\rangle \cong L_2(q).$$

In the case $q \equiv 1(8)$, the centralizer $C_H(z)$ of z in H is $L_1\langle w, \alpha_2\rangle$ and $\langle v, a_1, a_2, c_1\rangle$ is an S_2-subgroup of $C_H(z)$, whose commutator group is $\langle a_1\rangle$. It is easily checked that $C_H(z)$ does not contain elementary Abelian groups of order 16.

(3.14) *S_p-subgroups of H*

Let $T_1 = \langle\theta_1^{\ x} \mid x \in \langle v, n\rangle\rangle$ and $T_2 = T_1^{\ u}$. Clearly $T_1T_2 = T_1 \times T_2$ is an S_p-subgroup of H and is elementary Abelian. We have

$$C_H(T_1T_2) = \langle w^2\alpha_1\alpha_2^{-1}\rangle\, T_1T_2$$

and

$$N_H(T_1T_2) = \langle w, u, \alpha_1, \alpha_2\rangle\, T_1T_2 .$$

(3.2) *Fusion of involutions*

We shall show that G has only one class of involutions when $q \equiv 5(8)$ and two classes of involutions when $q \equiv 1(8)$.

(3.2.1) *An S_2-subgroup of H is an S_2-subgroup of G.*

Proof. Obvious, since an S_2-subgroup Q of H has cyclic center $\langle t\rangle$.

(3.2.2) *When $q \equiv 1(8)$, the conjugate class in H containing z does not fuse with other conjugate classes of H.*

Proof. By (3.1.3) an S_2-subgroup of $C_H(z)$ is

$$T = \langle v, a_1, a_2, c_1\rangle$$

of order $2^{3\alpha-1}$. Suppose that z is conjugate to t in G. Then there exists a 2-group S containing T such that $[S : T] = 2$. Since $T' = \langle a_1\rangle$ char T and $T \lhd S$, $\langle a_1\rangle \lhd S$. But then it follows that there is an $x \in S - H$ centralizing $t = (a_1)^{2\alpha-1}$ a contradiction. Hence z is not conjugate to t in G and incidentally, we have also shown that T is an S_2-subgroup of $C_G(z)$.

This implies that z is not conjugate to u, uv, or s since $C(u)$, $C(uv)$, and $C(s)$ all have elementary Abelian groups of order 16 but $C(z)$ does not. This completes the proof.

(3.2.3) *If u is conjugate to t in G, then s is conjugate to t in G.*

Proof. By (3.1.3), $T = \langle t, u\rangle \times \langle a_1a_2, c_1c_2\rangle$ is an S_2-subgroup of $C_H(u)$. By our assumption there exists an element x in a 2-group S of $C(u)$ containing T such that $x \in S - H$, and x normalizes T.

If $q \equiv 5(8)$, T is elementary Abelian. Let

$$S_1 = \{s, ts, t_3, tt_3, st_3, tst_3\}$$

all of whose involutions are conjugate in H. Similarly

$$S_2 = \{u, ut, us, uts, ut_3, utt_3, ust_3, utst_3\}$$

consisting of involutions conjugate in H. We have $S_1 \cup S_2 \cup \{t, 1\} = T$. Since $x \notin H$, $t^x \neq t$. If $t^x \in S_1$ or $s^x \in S_2$, then we are finished. Hence we may assume $t^x \in S_2$ and $s^x \in S_1$. Then $(ts)^x \in S_2$. The result follows because s is conjugate to ts in H and from the assumption that u is conjugate to t.

If $q \equiv 1(8)$, T is non-Abelian and $Z(T) = \langle t, u, s\rangle$. We have $T' = \langle (a_1a_2)^2\rangle$. Thus x normalizes both $Z(T)$ and $Z(T) \cap T' = \langle s\rangle$. Hence $s^x = s$. If $t^x = ts$, then we are finished; otherwise $t^x \in Z(T) - \langle t, s\rangle$. The result follows as before.

(3.2.4) *If uv is conjugate to t in G, then s is conjugate to t in G.*

Proof. As in (3.2.3).

(3.2.5) *If s is conjugate to t in G, then G has only one class of involutions when $q \equiv 5(8)$ and two classes of involutions when $q \equiv 1(8)$.*

Proof. Let $M = \langle a_1, c_1, a_2, c_2\rangle$. It is a maximal subgroup of an S_2-subgroup Q of G. Since G does not have a subgroup of index 2, by Thompson's lemma, [3, Ch. 7, Ex. 3], u and uv are conjugate to some involutions in M. The result follows from (3.1.2) and (3.2.2).

(3.2.6) *When* $q \equiv 5(8)$, G *has only one class of involutions. When* $q \equiv 1(8)$, G *has precisely two classes of involutions.*

Proof. Using exactly the same arguments as in (2.2.5), we can show that t is conjugate to an element in $\{u, uv, s\}$. The result then follows from (3.2.3), (3.2.4), and (3.2.5).

(3.3) *Some subgroups of G)*

The results of this section are needed for the construction of a subgroup G_0, which is a (B, N) pair.

Let i be an involution in H conjugate to t in G. We observe that $N_H\langle i, t\rangle/C\langle i, t\rangle$ has order 2. Consider the four-group $A = \langle t, u\rangle$. Let $x \in N(A) \cap C(u) - C(A)$ which exists because of (3.2.6) and the above observation. Then $t^x = ut$, $ut^x = t$. Since $x \in N(A)$, x normalizes $C(A)$ and hence normalizes $C(A)' = B$, i.e., $B^x = B$.

When $q \equiv 1(8)$, we have $(v^2a_1a_2^{-1})^{2^{\alpha-3}} \in N(A)$ and centralizes B. Put $z' = x^{-1}(v^2a_1a_2^{-1})^{2^{\alpha-3}}x$. Hence z' centralizes $B^x = B$. Let $\nu = z' \cdot (v^2a_1a_2^{-1})^{2^{\alpha-3}}$ and $\mu = [z', v^{2^{\alpha-2}}]$. We compute that the following relations hold:

$$t^\nu = u; \quad u^\nu = ut; \quad ut^\nu = t; \quad \nu \in C(B);$$

$$t^\mu = ts; \quad u^\mu = us; \quad \alpha_1\alpha_2{}^\mu = \alpha_1\alpha_2; \quad t_3{}^\mu = utst_3.$$

Because

$$\mu^2 \in C(t, s, u, t_3\rangle = \langle t, s, u, t_3\rangle$$

and since μ does not fix any element in $\langle t, s, u, t_3\rangle - \langle ut, s\rangle$, $\mu^2 \in \langle ut, s\rangle$. If $\mu^2 = 1$, ut or uts, replacing μ by μu, ut_3 or μut_3, respectively, we may assume that $\mu^2 = s$ without affecting the previous relations.

When $q \equiv 5(8)$, va_1 acts as an outer automorphism of order 2 on B. Hence $(va_1)^x$ acts as an outer automorphism of order 2 on $B^x = B$. Because $q = p^f \equiv 5(8)$, f is odd. The outer automorphism group of $B = L_2(q)$ is Abelian of order $2f$. Hence $(va_1)(va_1)^x$ is inner on B. Therefore $\nu = va_1(va_1)^x b$ centralizes B for a suitable $b \in B$. We check that

$$t^\nu = u; \quad u^\nu = ut; \quad (ut)^\nu = t.$$

Let $z' = (va_1)^\nu$ and $\mu = [z', v]$. Then it is easily verified that μ has the same action on $\langle t, \alpha_1\alpha_2, t_3, u\rangle$ as in the case $q = 1(8)$. Thus we have proved the following result.

(3.3.1) *There exist elements ν, μ in G such that $t^\nu = u$; $u^\nu = ut$; $(ut)^\nu = t$; $\nu \in C(B)$; $t^\mu = ts$; $u^\mu = us$; $(\alpha_1\alpha_2)^\mu = \alpha_1\alpha_2$; $t_3{}^\mu = ustt_3$ and $\mu^2 = s$.*

(3.3.2) *Let $F = \langle w, \alpha_1, \alpha_2\rangle$ and $N = N\langle t, s\rangle$. Then N/F is isomorphic to the symmetric group on four letters. Moreover we have $(\mu c_2)^3 = 1 = (c_2\mu ut)^3$.*

Proof. From (3.3.1) we see that $\mu \in N\langle t, s\rangle$. Therefore μ normalizes $C(t, s)$, $C(t, s)'$ and

$$C(t, s)' \cap C(t, s) = F.$$

Since $| C\langle t, s\rangle/F | = 4$ and from the fact $\mu \notin N_H\langle t, s\rangle$, it follows that $| B/F | = 24$.

Let r_1, r_2, r_3 denote the cosets μF, c_2F, and $c_2\mu utF$, respectively. Clearly $r_1{}^2 = r_2{}^2 = r_3{}^2 = 1$ and $r_1r_3 = r_3r_1$. Both $(\mu c_2)^3$ and

$$(c_2\mu tu)^3 \in C\langle t, s, u, t_3\rangle = \langle t, s, u, t_3\rangle.$$

Since μc_2 and $c_2\mu ut$ *act* fixed-point-free on $\langle t, s, u, t_3\rangle$, it follows then,

$$(\mu x_2)^3 = 1 = (c_2\mu ut)^3.$$

Hence we have also shown that $\langle r_1, r_2, r_3\rangle$ satisfies Moore's relations and so $\langle r_1, r_2, r_3\rangle \cong S_4$ proving our lemma.

(3.3.3) *Suppose $|\langle l\rangle| \neq 1$. Let Y be a nontrivial subgroup of $\langle l\rangle$. Then $C(Y) \subsetneq C(t) = H$.*

Proof. From the structure of H, $C_H(Y) = L_1L_2\langle w\rangle$, a subgroup of index 2 in H. Since $S = \langle a_1, c_1, a_2, c_2, v\rangle$ is an S_2-subgroup of $C_H(Y)$ and has cyclic center $\langle v^2a_1a_2{}^{-1}\rangle \supsetneq \langle t\rangle$, it is clear that S is an S_2-subgroup of $C(Y)$. By (3.3.2), involutions in $S - \langle a_1, c_1, a_2, c_2\rangle$, if they exist, are not conjugate to t. By the structure of $SL(2, q)$ involutions in $\langle a_1, c_1, a_2, c_2\rangle$ lie in two conjugate classes of $C_H(Y)$ with representatives t and s. Suppose s is conjugate to t in $C(Y)$. Then there is a 2-group $T \subsetneq C(s) \cap C(Y)$ and

$$S \cap C(s) = \langle a_1, a_2, c_1c_2, v\rangle \subset T.$$

Hence there is $x \in T - S \cap C(s)$ and $x \in N(S \cap C(s))$. Since

$$\Omega_1((S \cap C(s))') = \langle t, s\rangle, \qquad x \in N\langle t, s\rangle,$$

it follows that $t^x = ts$; $(ts)^x = t$. Thus $\mu x^{-1} \in C\langle t, s\rangle$ [See (3.3.1)]. But $C(t, s) \subseteq N(Y)$. Hence $Y^\mu = Y^x = Y$. Since $t_3 \in C(Y)$, $ustt_3 = t_3{}^\mu \in C(Y^\mu) = C(Y)$, a contradiction. Therefore we have shown that t is not conjugate to other involutions of S in $C(Y)$.

By the result of Glaubermann [2],

$$C(Y) = (C(Y) \cap C(t))\, O(C(Y)).$$

Set $M = O(C(Y))$. The four-group $\langle t, s\rangle$ acts on M. By the result of Brauer–Wielandt [4], $M = C_M(t)\, C_M(ts)\, C_M(s)$. By (3.3.1),

$$C_M(ts) = (C(t) \cap O(C_G(Y^{\mu}))^{\mu^{-1}}.$$

Since

$$\langle l, m, n\rangle = O(C(t, s)),$$

and $\mu \in N\langle t, s\rangle$, we have $\mu \in N\langle l, m, n\rangle$. Since

$$\langle l\rangle = C(t_3) \cap \langle l, m, n\rangle, \qquad \langle l^{\mu}\rangle = C(ustt_3) \cap \langle l, m, n\rangle = \langle m\rangle.$$

In particular, $X = Y^{\mu} \subseteq \langle m\rangle$. Thus

$$C(t) \cap C(X) = \langle \alpha_1, \alpha_2, w, ut_3\rangle$$

which has the normal 2-complement $\langle l, m, n\rangle$. So

$$C(t) \cap O(C(X)) \subseteq \langle l, m, n\rangle$$

and

$$C_M(ts) \subseteq \langle l, m, n\rangle^{\mu^{-1}} = \langle l, m, n\rangle.$$

Also

$$C_M(s) = (C_M(ts))^{c_2} \subseteq \langle l, m, n\rangle.$$

Lastly

$$C(t) \cap O(C(Y)) \subseteq \langle l\rangle$$

since $\langle l\rangle$ is the maximal normal subgroup of odd order in $C(t) \cap C(Y)$. It follows then

$$M \subseteq \langle l, m, n\rangle \subseteq C(t),$$

proving the result $C(Y) \subseteq C(t)$.

(3.3.4) *The centralizer $C(B)$ of B in G is isomorphic to $L_2(q)$.*

Proof. We have $C(B) \cap C(t) = \langle w^2\alpha_1\alpha_2^{-1}, u\rangle$, a dihedral group of order $(q-1)$. If $q \equiv 5(8)$, $\langle t, u\rangle$ is an S_2-subgroup of $C_H(B)$. By (3.3.1), we have $\nu \in C(B)$ acting fixed-point-free on $\langle t, u\rangle$. This implies, in particular, that $\langle t, u\rangle$ is an S_2-subgroup of $C(B)$. If $q \equiv 1(8)$, an S_2-subgroup of $C_H(B)$ is $\langle u, v'\rangle$ where $v' = \langle v^2 a_1 a_2^{-1}\rangle$ and has the center $\langle t\rangle$. Hence $\langle u, v'\rangle$ is an S_2-subgroup of $C(B)$. Again by (3.3.1), u is conjugate to t in $C(B)$. Since

$$va_1 \in N(B), \qquad \nu' = \nu^{va_1}$$

centralizes $B^{va_1} = B$. We compute $t^{\nu'} = uv'$. Thus in this case too, $C(B)$ has only one class of involutions.

Since $C(t) \cap C(B)$ has Abelian 2-complement, by the result of Gorenstein–Walter [4],

$$C(B)/O(C(B)) \simeq L_2(r)$$

for some odd r or A_7.

We show next that $M = O(C(B)) = 1$. By the Brauer–Wielandt's formula [7], and the fact $C(B)$ has only one class of involutions, $|M| = |C_M(t)|^3$. Suppose that $1 \neq C_M(t) \subseteq \langle l \rangle$. Let h be an element of prime order in $C_M(t)$. Then we have $C_M(t) \subset C_M(h) \not\subseteq H$, a contradiction to (3.3.3). Hence $M = 1$.

By the structure of $L_2(r)$,

$$|C(t) \cap C(B)| = q - 1 = r \pm 1.$$

The cases $C(B) \simeq L_2(q + 2)$ or A_7 are not possible as this would imply that $C\langle s, t_3 \rangle$ contains a subgroup isomorphic to $L_2(q + 2)$ or A_7 contrary to (3.1.3) and (3.2.6). This completes the proof that $C(B) \simeq L_2(q)$.

(3.4) S_p-*subgroups of* G.

We shall now construct a p-subgroup of G which will turn out to be an S_p-subgroup of G.

(3.4.1) *The group* $\langle T_1, T_2, T_1^u, T_2^u \rangle$ *is elementary Abelian of order* q^4.

Proof. Let

$$T = \langle xuxu \mid x \in T_1 \rangle \qquad \text{and} \qquad \tilde{T} = \langle x^{-1}uxu \mid x \in T_1 \rangle.$$

Then we have

$$C_H(T) = \langle w^2 \alpha_1 \alpha_2^{-1}, u \rangle \, T_1 T_2 .$$

For the same reason as in the proof of (3.3.4), $\langle v^2 a_1 a_2^{-1}, u \rangle$ is an S_2-subgroup $C(T)$. Since

$$\langle w^2 \alpha_1 \alpha_2^{-1}, u \rangle \subseteq C(B) \simeq L_2(q)$$

by (3.3.4), $C(T)$ has only one class of involutions. Further $C(t) \cap C(T)$ has Abelian 2-complement. Therefore by the result of Gorenstein–Walter [4], $C(T)/M$ is isomorphic to A_7 or $L_2(r)$ where $M = O(C(T))$. When $q \neq 5$, $C(T)/M$ cannot be isomorphic to A_7 since $C(T)/M$ contains a subgroup $C(B)M/M$ isomorphic to $L_2(r)$. If $q = 5$, $C(T)/M$ has an S_2-subgroup of order 4 whereas an S_2-subgroup of A_7 has order 8. Thus we have shown that $C(T)/M$ is isomorphic to $L_2(r)$ for some odd r.

Suppose $q \neq 5$. Since $C(T)/M$ contains a subgroup isomorphic to $L_2(q)$, this implies that $r = q^k$ for some integer k. But, on the other hand, $(C(t) \cap C(T))M/M$ has order at most $q^2 - q$ since $T \subseteq M$. It follows that $r = q$.

When $q = 5$, $C(T)/M$ is isomorphic to $L_2(5)$ or $L_2(19)$. If the latter is the case, we obtain $M = T$. Since $C(T) \supset C(B)T$; $C(B)T$ is a split extension of T, by the result of [5, Ka. II, 17.4],

$$C(T) = K \times T, \qquad K \cong L_2(19).$$

Now $a_1a_2 \in N(T)$ and so normalizes

$$C(T)' = K \supseteq C(B)' = C(B).$$

Since $\langle v^2a_1a_2^{-1}, u, a_1a_2\rangle$ is not dihedral, $K\langle a_1a_2\rangle$ is not isomorphic to $PGL(2, 19)$. In other words, a_1a_2x centralizes K for a suitable $x \in K$. Both a_1a_2x and a_1a_2 centralize $C(B)$. Therefore x centralizes $C(B) \subseteq K$. It follows $x = 1$ since no nontrivial element of K can centralize a subgroup isomorphic to $L_2(5)$. Thus $a_1a_2 \in C(K)$, a contradiction to the structure of H.

Thus $C(T)/M \cong L_2(q)$ for all q. In particular

$$C(t) \cap M = T_1T_2 = \langle T, \tilde{T}\rangle.$$

In the proof of (3.3.1), we have an element $z' \in N(T)$ such that $t^{z'} = u$. Since M char $C(T)$, $z' \in N(M)$. Therefore $C_M(u) = \langle T, \tilde{T}^{z'}\rangle$ and $C_M(ut) = \langle T, \tilde{T}^{v^2}\rangle$. Hence $M = \langle T, \tilde{T}, \tilde{T}^{z^1}, \tilde{T}^{v^2}\rangle$ of order q^4.

Using information in (3.3.1), we get $v^2ts = usv^2$ and $z'ts = usz'$. Since $us \in C(\tilde{T})$, it follows that

$$\langle \tilde{T}^{z'}, \tilde{T}^{v^2}\rangle \subseteq C_M(ts).$$

The order of

$$\langle \tilde{T}^{z'}, \tilde{T}^{v^2}\rangle \subseteq M$$

is at least q^2. But an S_p-subgroup of $C(ts)$ has order q^2. It follows

$$\langle \tilde{T}^{z}, \tilde{T}^{v^2}\rangle = C_M(ts).$$

Applying Brauer–Wielandt's formula on M using the four-group $\langle t, s\rangle$, we get $C_M(s) = 1$. Hence by the result of Zassenhaus, M is Abelian and so elementary Abelian of order q^4.

To complete the proof, we shall show that $C_M(ts)^\mu = \langle T_1, T_2\rangle$. Since

$$(ts)^\mu = t, \qquad C_M(ts)^\mu \subseteq C(t).$$

We have

$$z'\mu = z'[z', v^{2\alpha-2}] = (v^{2\alpha-2})^{-1} z'v^{2\alpha-2}.$$

Since $z' \in N(T)$, $z'\mu \in N(T)^{v^{2^{\alpha-2}}} = N(\tilde{T})$. Therefore $C_M(ts)^\mu$ contains $\tilde{T}^{z'\mu} = \tilde{T}$. But $\langle T_1, T_2\rangle$ is the unique S_p-subgroup of $C(t)$ containing $\tilde{T}$. It follows that $C_M(ts)^\mu = \langle T_1, T_2\rangle$ and so

$$C_M(ts)^{\mu^2} = C_M(ts) = \langle T_1{}^\mu, T_2{}^\mu\rangle$$

because $\mu^2 = s \in N(T)$ and $\mu^2 \in N(M)$.

(3.4.2) *Let* $\theta_3 = \theta_1{}^\mu$; $\theta_4 = \theta_2{}^\mu$; $\theta_5 = \theta_3^{c_2}$; $\theta_6 = \theta_4^{c_2}$; $T_3 = T_1{}^\mu$; $T_4 = T_2{}^\mu$; $T_5 = T_3^{c_2}$; $T_6 = T_4^{c_2}$. *Then* $P = T_1T_2T_3T_4T_5T_6$ *is a p-subgroup of order* q^6 *and* $B = PF$ *is a subgroup of order* $\frac{1}{4}(q-1)^3 q^6$ *with* $F \subseteq N(P)$.

Proof. Almost identical to that of (2.5.2).

4. The subgroup G_0

From now on, we shall assume that q is any odd prime power. We shall show that BNB is a subgroup and a (B, N) pair.

(4.1) *Let* $V_1 = \langle T_1, T_2, T_3, T_4, T_5\rangle$;

$$V_2 = \langle T_1, T_3, T_4, T_5, T_6\rangle \quad \textit{and} \quad V_3 = \langle T_1, T_2, T_3, T_4, T_6\rangle.$$

Then $\mu \in N(V_1)$, $c_2 \in N(V_2)$, *and* $\mu ut \in N(V_3)$.

Proof. From (2.4.1) and (3.3.1), it is immediate that

$$T_1{}^\mu = T_3, \quad T_2{}^\mu = T_4, \quad T_3{}^\mu = T_1, \quad T_4{}^\mu = T_2.$$

By (2.4.2) and (3.3.2), we have $(\mu c_2)^3 = 1$. Hence

$$\mu^{-1}\theta_5\mu = (\mu^{-1}c_2^{-1}\mu^{-1})\,\theta(\mu c_2\mu) = c_2\mu(c_2\theta_1c_2^{-1})\,\mu^{-1}c_2^{-1} = \theta_5\,.$$

Since w acts fixed-point-free on T_1, $w^{\mu c_2}$ acts fixed-point-free on T_5. Let $x \in T_5$. Then $x = h^{-1}\theta_5 h$ for some $h \in \langle w^{\mu c_2}\rangle \subseteq F$ and

$$\mu^{-1}x\mu = (h^\mu)^{-1}\,(\mu^{-1}\theta_5\mu)h^\mu \in T_5$$

because $h^\mu \in F$ and $F \subseteq N(T_i)$ for all i. Thus $\mu \in N(V_1)$. The other assertions may be proved similarly.

For later use, we exhibit the action of μ, c_2, μut on V_1, V_2, V_3 by the following table:

TABLE I

	T_1	T_2	T_3	T_4	T_5	T_6
μ	T_3	T_4	T_1	T_2	T_5	
c_2	T_1		T_5	T_6	T_3	T_4
μut	T_4	T_3	T_2	T_1		T_6

(4.2) *The following relations hold in the group G:*

$$(c_2\theta_2)^3 = (\mu\theta_6)^3 = (\mu ut\theta_5)^3 = 1.$$

Proof. From the structure of H, $(c_2\theta_2)^3 = 1$. We have

$$(c_2\theta_2)^{\mu c_2} = (c_2^{-1}\mu^{-1}c_2\mu c_2)\,\theta_6 = \mu\theta_6$$

and

$$(c_2\theta_2)^{u\mu c_2} = (c_1c_2c_2^{-1}\theta_1)^{\mu c_2}\,\mu ut\theta_5$$

by (2.4.1), (3.3.1), (2.4.2), and (3.3.2) proving the lemma.

Put

$$W = N/F, \quad r_1 = \mu F, \quad r_2 = c_2F, \quad r_3 = \mu utF.$$

By (2.4.2) and (3.3.2), $W \cong S_4$, the symmetric group on four letters. For any $x \in W$, let $l(x) = l$ denote the smallest positive integer such that $x = r_{i_1} \cdots r_{i_l}$ where $r_{i_j} \in \{r_1, r_2, r_3\}$. Let

$$\omega(r_1) = \mu; \quad \omega(r_2) = c_2; \quad \omega(r_3) = \mu ut.$$

For any $x \in W$ where $x = r_{i_1} \cdots r_{i_l}$, let $\omega(x) = \omega(r_{i_1}) \cdots \omega(r_{i_l})$. As usual BxB shall denote $B\omega(x)B$.

By (2.4.2), (2.5.2), (3.3.2), and (3.4.2), we have $B \cap N = F$ and $F \lhd N$. We shall now show the following result.

(4.3) *The set of elements BNB is a (B, N) pair of type A_3.*

Proof. First we show that $G_i = B \cup Br_iB$ are subgroups of G. Consider $G_1 = B \cup B\mu B$. The group B may be written in the form $B = (FV_1)\,T_6$. Since $\mu \in N(FV_1)$ and $\mu^2 = v^{2^{\alpha-1}} \in B$, it is sufficient to show that

$$\mu x\mu \in B \cup B\mu B \qquad \text{for} \quad x \in T_6 - 1.$$

As $w^{\mu c_2}$ acts fixed-point-free on T_6, $x = h^{-1}\theta_6 h$ for some $h \in \langle w^{\mu c_2}\rangle$. Then

$$\mu x\mu = k^{-1}\mu\theta_6\mu k$$

where $k = h^{\mu^{-1}} \in F \subseteq B$. Since $(\mu\theta_6)^3 = 1$, by (4.2), it follows that

$$\mu x \mu = k^{-1}\theta_6^{-1}\mu^{-1}\theta_6^{-1}k \in B\mu B.$$

Hence G_1 is a group. Similarly G_2, G_3 are subgroups of BNB.

We shall show next that for any i and $x \in W$, if $l(r_i k) \geqslant l(x)$, then $r_i B x \subseteq B r_i x B$. Put

$$X_1 = T_6, \quad X_2 = T_2, \quad X_3 = T_5.$$

Since $W \simeq S_4$ and r_1, r_2, r_3 satisfy the Moore's relations we may identify r_1, r_2, r_3 with the transpositions (12), (23), (34), respectively. Let

$$C_0 = \{1\}, \qquad C_1 = \{r_1, r_2, r_3\}.$$

Let $\tilde{C}_n$ be the set of words of length n. Then

$$C_n = \tilde{C}_n - \bigcup_{0 \leqslant i \leqslant n-1} C_i$$

is clearly the set of elements x in W with $l(x) = n$. To prove our result, it is only necessary to show that, for those $x \in N$ such that $l(r_i x) \geqslant l(x)$, $r_i X_i x \subseteq B r_i x B$. By an easy computation using the table, we see that this is the case.

Now by the theorem of Tits [6], BNB is a (B, N) pair of type A_3.

(4.4) *The group G contains a subgroup G_0 isomorphic to $L_4(q)$.*

Proof. By a result of Abe [1], BNB contains subgroups K and G_0 such that $G_0/K \simeq L_4(q)$. Now K is necessarily odd and G_0 contains a four-group $\langle t', v' \rangle$, all of whose involutions are conjugate in G_0. Comparing $|C_G(t')|$ with $|C_{G_0}(t')K/K|$, it follows that $C_G(t') \cap K = 1$ and $C_G(t') \subseteq G_0$. By the theorem of Brauer–Wielandt, $|K| = 1$. Thus we have $G_0 \simeq L_4(q)$.

Before proving the identity, we show that G is simple.

5. Identity $G = G_0$

(5.1) *The group G is simple.*

Proof. Suppose $M = O(G) \neq 1$. Act on M by the four-group $\langle t, v^{2^{\alpha-1}} \rangle$. We note the involutions in $\langle t, v^{2^{\alpha-1}} \rangle$ all lie in a conjugate class of G by (2.2.6) and (3.2.6). Since $O(C(t)) = \langle l \rangle$, it follows that $C_M(t) \subseteq \langle l \rangle$. If $C_M(t) = 1$ then by Brauer–Wielandt's result, $M = 1$, a contradiction. If $C_M(t) \neq 1$, again by Brauer–Wielandt, $M = C_M(t)$. Consider $C(M)$. It is normal in G and has an S_2-subgroup of index 2 in an S_2-subgroup of G. In other words

$G/C(M)$ has cyclic S_2-subgroup of order 2. By Burnside's transfer result [3, Ch. 7, 4.3], $G/C(M)$ has a normal 2-complement in contradiction to condition (a) of the theorem. Hence $O(G) = 1$.

Suppose next that G has a proper normal subgroup K with odd factor group G/K. Since $C(t)$ does not have a proper normal subgroup with odd index in $C(t)$, $C(t) \subseteq K$. The Frattini argument shows that $G = KN_G(Q)$. But $N_G(Q) \subseteq C(t)$ and hence $G = N$, a contradiction.

Suppose G has a normal subgroup M such that both $|M|$ and $|G/M|$ are even. Now $Q \cap M$ is an S_2-subgroup of M and is normal in Q. Hence it contains $Z(Q) = \langle t \rangle$ and also u which is conjugate to t and ut. Thus M contains all involutions conjugate to t and ut. This implies that $Q \subseteq M$ since, by direct computation, M contains subgroups generated by involutions conjugate to t or ut and M contains conjugates of these subgroups. It follows that $|G/M|$ is odd, a contradiction. This completes the proof.

To complete the proof of the theorem, we prove the following:

(5.2) $G_0 = G$.

Suppose by way on contradiction that $G - G_0 \neq \varnothing$. We have three cases to consider.

(i) $q \equiv -1 \pmod 4$.

By (2.3.1), (4.4), and (5.1) G_0 is a strongly embedded subgroup of G, and hence by the result of Suzuki–Thompson [3, Ch. 9, 2.2], G has only one class of involutions, a contradiction. Hence $G = G_0$.

(ii) $q \equiv 1 \pmod 8$.

Let i be an involution in $G - G_0$ conjugate to z (See 2.2.2). Then $\langle i, t \rangle$ is dihedral and its order is divisible by 8. Let j be a central involution of $\langle i, t \rangle$. Suppose j is conjugate to t in G. First we have $j \in C(t) \subseteq G_0$. By our assumption $C(j) \subseteq G_0$ since G_0 contains the centralizers of its involutions conjugate to t. Thus $i \in G_0$, a contradiction. Hence j is conjugate to z in G. The four-group $\langle t, j \rangle$ contains two involutions conjugate to t and one conjugate to z. But $\langle t, j \rangle$ is conjugate to $\langle t, z \rangle$ in H and $\langle t, z \rangle$ contains two involutions conjugate to z, a contradiction. Thus $G = G_0$.

(iii) $q \equiv 5 \pmod 8$.

In this case G has only one class of involutions and G_0 is a strongly embedded subgroup of G. Hence by Suzuki–Thompson [3, Ch. 9, 2.2], $G_0 = C(t)K$, where K has odd order. Since $G_o \simeq L_4(q)$,

$$|K| = \tfrac{1}{2}(q^2 + 1)(1 + q + q^2)q^4 \, |C(t) \cap K|.$$

Let p^x be the maximal power of p dividing $|K|$. Since K is solvable a Hall subgroup of M of order $\frac{1}{2}(q^2 + 1)(q^2 + q + 1)\,p^x$ exists. By [5, Ka. II, 7.3],

G_0 contains a cyclic Hall subgroup T^* of order $\frac{1}{2}(q^2 + 1)$. By a result of Wielandt, [5, Ka. III, 5.8] we may assume $T^* \subseteq M$. Suppose $1 \neq \langle x \rangle = T^* \cap T^{*g}$ for some $g \in M$, by [5, Ka. II, 7.3], $N_M\langle x \rangle = T^*$ and so $T^* = T^{*g}$. Also $N_M(T^*) = T^*$. Thus M is a Frobenious group with the Froberious kernel of order $(q^2 + q + 1)\, p^x$ which is nilpotent by a result of Thompson [5, Ka. V, 8.13]. This gives a contradiction since the centralizer of an element of order p in $L_4(q)$ is not divisible by $q^2 + q + 1$.

Thus we have shown that $G = G_0$ for all odd q.

References

1. E. Abe, Finite groups admitting Bruhat decompositions of type (A_n), *Tôhoku Math. J.* **16** (1964), 130–141.
2. G. Glaubermann, Central elements in core-free groups, *J. Algebra* **4** (1966), 403–420.
3. D. Gorenstein, "Finite Groups," Harper & Row, New York, 1968.
4. D. Gorenstein and J. H. Walter, On finite groups with dihedral Sylow 2-subgroups, *Illinois J. Math.* **6** (1962), 553–593.
5. B. Huppert, "Endliche Gruppen," Springer Pub., New York, 1967.
6. J. Tits, Théorème de Bruhat et sous-groupes paraboliques, *C. R. Acad. Sci. Paris* **254** (1962), 2910–2912.
7. H. Wielandt, Beziehungen zwischen den Fixpunktzahler von Automorphismengruppen einer endlichen Gruppe, *Math. Z.* **73** (1960), 146–158.
8. W. J. Wong, A characterization of the alternating group of degree 8, *Proc. London Math. Soc.* **50** (1963), 359–383.