On Finite Groups which Contain a Frobenius Subgroup*

MARCEL HERZOG

Department of Mathematics, University of Illinois, Urbana, Illinois 61801
Communicated by Walter Feit
Received May 31, 1966

1. INTRODUCTION

Let $G$ be a finite group. A nontrivial proper subgroup $M$ of $G$ will be called a CC-subgroup if $M$ contains the centralizer of each of its non-unit elements. If, in addition, $M$ is a TI-set in $G$ then $M$ will be called a CCT-subgroup of $G$.

Finite groups $G$, containing a CC-subgroup $M$, were studied by W. Feit in [3], and important information concerning the relation between the characters of $G$ and those of the normalizer $N(M)$ of $M$ in $G$ was furnished there under the assumptions

(i) $N(M) \neq M$,
(ii) $|N(M)| \neq (|M| - 1) |M|$, 
(iii) $M$ is not a non-Abelian $p$-group with $[M : M'] < 4[N(M) : M]^2$.

Our aim was originally to characterize finite groups satisfying Conditions (i)-(iii) and, in addition;

(iv) $3 | M$,
(v) $M$ is noncyclic

as a step in proving the following conjecture of W. Feit:

Let $G$ be a finite group, and suppose that $G$ contains a CC-subgroup $M$ satisfying Conditions (i), (ii), (iv), (v). Then $G$ is either a Frobenius group with $M$ as the Frobenius kernel or it is isomorphic to a simple group $PSL(2, 3^n), n \geq 2$.

If $M$ is normal in $G$, then $G$ is a Frobenius group with $M$ as the Frobenius kernel by the definition. If $M$ is not normal in $G$, we are successful in proving that $G$ is isomorphic to a simple group $PSL(2, 3^n), n \geq 2$, under the assumptions that $M$ satisfies Conditions (i)-(v) and in addition

(vi) $[N(M) : M]$ is odd (Theorem 5.1).

* During the summer of 1965 this research was supported by the National Science Foundation.
The proof requires five successive steps in which it is shown that

(a) \(M\) is Abelian,
(b) \(M\) is an elementary Abelian 3-group,
(c) \([N(M) : M] = \frac{1}{3} (|M| - 1)\),
(d) \(|G| = \frac{1}{3} (|M| - 1) |M| (|M| - 1)\),
(e) \(G \cong PSL(2, \mathbb{Z}).\)

If \([N(M) : M]\) is even, (a) certainly holds, and assuming (d), the proof of (e) does not use Assumption (vi). Also, (c) is deduced from (b) without applying Condition (vi). Thus in order to eliminate Condition (vi), it remains only to prove (b) and (d). The elimination of Condition (iii) appears to be a much more difficult problem.

Section 2 deals with general properties of groups containing a CC-subgroup, most of which seem to be known. In Section 3 some useful conclusions are derived from the results in [3].

The object of Section 4 is to study groups satisfying Conditions (i)-(iv). In this case, Theorem 1 of [5] is of fundamental importance. Our work supplies a second example, after the one of the above-mentioned authors, of utilizing the knowledge about the infinite polyhedral group

\[(3,3,3) = \langle x, y, z \mid x^3 = y^3 = z^3 = xyz = 1 \rangle\]

for the investigation of finite groups.

The main Theorem 5.1 is proved in Section 5. It follows from a long series of lemmas, in which the characters of \(G\) are analyzed.

The nilpotency of the Frobenius kernel of a Frobenius group is frequently used throughout this work. The solvability of groups of odd order is applied at least once in Section 5. These famous and well-known results of Feit and Thompson are used without reference.

**Definitions and Notations**

The group \(H\) will be called a CP-group if its odd Sylow subgroups are all cyclic and the Sylow 2-subgroup is either cyclic or generalized quaternion. \(H \in \text{Hypothesis } A\), \(H \in \text{Theorem 1}\) will mean respectively: \(H\) satisfies Hypothesis \(A\), \(H\) satisfies the assumptions of Theorem 1. If a group \(G\) contains the CCT-subgroup \(M\), \(G \in (*)\) will mean that \(N(M)\) has no normal complement in \(G\). For any subset \(T\) of a group \(G\), \(C_G(T), Z(T), N_G(T)\), and \(|T|\) will denote, respectively; the centralizer, center, normalizer, and the number of elements in \(T\). If \(M\) is a subgroup of \(G\) and \(y \in G\), then \(M'\),
\(M^y, M^#, Cl_G(y),\) and \(n_G(y)\) will denote, respectively; the commutator subgroup of \(M, y^{M^y}^{-1}, M - \{1\},\) the conjugate class of \(y\) in \(G,\) and \(|N_G(y)|;\) and \(M \prec G\) will mean that \(M\) is normal in \(G.\) If \(i, j\) are integers, \(\delta_{ij}, (i, j),\) and \(i \divides j\) will denote, respectively; the Kronecker Delta, the greatest common divisor of \(i\) and \(j,\) and \(i\) divides \(j.\) If \(u, v, z \in G,\) then \(\delta_{uv}(G)\) will have value 1 if \(u\) and \(v\) belong to the same conjugate class in \(G\) and value 0 otherwise. The coefficient of \(Cl_G(z)\) in \(Cl_G(u) Cl_G(v)\) will be denoted by \(c_{av}(G).\) If \(Cl_G(x) = C_G,\) then \(C_G^* = Cl_G(x^{-1}).\) For any two characters \(X_1, X_2\) of \(G,\) the Hermitian product \((X_1, X_2)\) is defined by

\[ (X_1, X_2)_G = \left(\frac{1}{|G|}\right) \sum_G X_1(x) \overline{X_2(x)}. \]

The subscript \(G\) will be dropped in cases where it is clear from the context which group is involved. For any character \(\xi\) of a subgroup of \(G,\) \(\xi^*\) will denote the character of \(G\) induced by \(\xi.\) \(\sum_x\) will denote summation over all the characters of \(G.\) The symbol \(\forall\) reads "for all".

2. Groups with either \(CC\) or \(CCT\) Subgroups—General Properties

The following theorems seem to be known, but were never summarized before. Most of them will be used in the following sections.

**Theorem 2.1.** Let \(G\) be a finite group and suppose that \(G\) contains a subgroup \(M\) with the following properties:

(i) \(\forall x \in M^#, C_G(x) \subseteq M;\)

(ii) \(Z(M) \neq \{1\}.)

Then \(M\) is a TI-set.

**Proof.** Suppose that \(z \in M \cap M^#, z \neq 1;\) we will show that then \(M = M^v.\) It follows from (i) that \(\forall u \in M^#, C_G(u) \subseteq M^v.\) Obviously \(C_G(z) \supseteq Z(M) \cup Z(M^v);\) thus \(Z(M) \cup Z(M^v) \subseteq M \cap M^v.\) Let \(w \in Z(M^v),\) \(w \neq 1;\) then \(w \in M\) and \(C_G(w) = M^v \subseteq M;\) therefore \(M = M^v\) as required.

**Corollary 2.1.** Theorem 2.1 holds true when, for (ii), we substitute

(ii)* \(N(M) \neq M.\)

**Proof.** \(N(M)\) is a Frobenius group, with the Frobenius kernel \(M.\) Hence \(M\) is nilpotent and \(Z(M) \neq \{1\}.)
THEOREM 2.2. Let $N$ be a Frobenius group of order $qm$ with the Frobenius kernel $M$ of order $m$, and suppose that $N = QM$, $|Q| = q$ and $q, m \neq 1$. Then:

(a) if $h \in M^\#$ and $u, v \in N - M$, then

$$c_{uv^{-1}h} = \frac{\delta_{uv}mq}{n(u)} ;$$

(b) $N' \supseteq M$; $N' = M$ if and only if $Q$ is cyclic;

(c) if $M$ is a CP-group, then $M$ is a cyclic group of odd order and $Q$ is cyclic;

(d) if $q$ is even and $u$ is an involution in $N$, then $n(u) = q$;

(e) if $q > m^{1/2} - 1$, then $M$ is elementary Abelian and no nontrivial proper subgroup of $M$ is normal in $N$.

Proof. (a) It follows from [3], Lemma 2.2, that

$$c_{uv^{-1}h} = \frac{mq}{n(u) n(v)} \delta_{uv} n(v) = \frac{\delta_{uv}mq}{n(u)} .$$

(b) As $c_{uv^{-1}h} > 0$ for $u \in N - M$, $h \in M^\#$, it follows that $h = wzw^{-1}x^{-1}$, where $w$ and $x$ are elements of $N$ and $wv$ is conjugate to $u$. Therefore $M \subseteq N'$ and consequently $N' = M$ if and only if $N/M = Q$ is Abelian. It is well-known that this implies that $Q$ is cyclic.

(c) $M$ is a nilpotent CP-group. Since $q > 1$ $M$ is of odd order, and hence cyclic. Therefore the group of automorphisms of $M$ is cyclic, implying that $Q$ is cyclic.

(d) Since $Q$ has only one involution, this involution is contained in the center of $Q$. Hence $n(u) = q$.

(e) Deny; then $M$ being nilpotent contains a subgroup $M_0$ of order $m_0 \neq 1$, $m$ which is normal in $N$. Obviously $q | m - 1$, $q | m_0 - 1$; hence $g | m - m_0 = m_0(m/m_0 - 1)$. Since $(q, m_0) = 1$, $q | m/m_0 - 1$. Therefore $(q + 1)^2 \leq m_0 m/m_0 = m$ or $q \leq m^{1/2} - 1$, which is not the case.

The following theorem is a generalization of Theorem 4F in [2], and of some results in [1], Section 2.

THEOREM 2.3. Let $G$ be a finite group of order $g$, and suppose that $G$ contains a CCT-subgroup $M$ of order $m$. Then the following hold.

(a) $M$ is a Hall subgroup of $G$;

(b) $|N(M)| = qm$ where $m - 1 = qv$, $q$, $v$-rational integers and there exists a subgroup $Q$ of $N(M)$ of order $q$ such that

$$N(M) = QM, \quad Q \cap M = \{1\} ;$$
(c) \( g = qm(nm + 1) \), where \( n \) is a nonnegative rational integer; if \( M \triangleleft G \) then \( n > 1 \) and \( g > qm^2 \) and if \( G \in (\ast) \) then \( q > 1 \), \( n > 1 \).

(d) If \( x, y \in M^\# \) and \( x = yu^{-1}, u \in G \), then \( u \in N(M) \).

(e) If \( G_0 \triangleleft G \), \( |G_0| = g_0 \) and \( G_0 \trianglerighteq M \), then \( g_0 = q_0m(nm + 1) \). If \( G \in (\ast) \) then the conclusion is true it we assume only that \( G_0 \triangleleft G \), \( G_0 \cap M \neq \{1\} \); moreover, then \( q_0 > 1 \) and \( G_0 \in (\ast) \).

(f) If \( N(M) \neq M \) then \( G' \supseteq M \) and \( [G : G'] \leq q \).

(g) If \( G \in (\ast) \) then \( G' \supseteq M \) and \( [G : G'] < q \) and \( G \) is nonsolvable.

(h) If \( N(M) \neq M, \{1\} \neq G_1 \triangleleft G, \quad |G_1| = g_1 \) and \( G_1 \cap M = \{1\} \), then \( M \) is a cyclic group of odd order, \( Q \) is a cyclic group, \( G_1 \) is a nilpotent group, \( g_1 = um + 1 \mid nm + 1 \) and \( n = wu + v, v \) a nonnegative integer. Moreover, \( G_1 \) is contained in the kernel of all characters of \( G \) nonvanishing on \( M^\# \), and the group \( \bar{G} = G/G_1 \) itself satisfies the assumptions of this theorem with respect to \( \bar{M} \), the image of \( M \) in \( \bar{G} \) under the natural projection. The orders of \( \bar{M} \) and its normalizer in \( \bar{G} \) are, respectively, \( m \) and \( qm \).

If \( G \in (\ast) \) then \( u < n, v > 0 \) and consequently \( n > m + 2 \). Moreover, \( G_1 \in (\ast) \).

Proof. (a) Since \( M \) contains the centralizer of each of its non-unit elements, it is a Hall subgroup of \( G \).

(b) \( N(M) \) is either equal or unequal to \( M \). In the first case, (b) is trivial; in the second case, \( N(M) \) is a Frobenius group with the Frobenius kernel \( M \), and the properties (b) are well known.

(c) Let \( \{M_i\} \) be the set of all conjugates of \( M \) other than \( M \). \( M \) acts as a permutation group on \( \{M_i\} \) by \( x : M_i \to xM_ix^{-1} \) for every \( x \in M \) and \( M_i \in \{M_i\} \). Let \( xM_ix^{-1} = M_i \) for some \( x \in M \), then \( x \in M \cap N(M_i) = \{1\} \). Thus no element of \( \{M_i\} \) is fixed by an \( x \in M^\# \) and hence the cardinality of \( \{M_i\} \) is \( nm, n \geq 0 \). Therefore \( g/qm = nm + 1 \). If \( q = 1 \) then, by the Frobenius Theorem, \( G \notin (\ast) \) and if \( n = 0 \) then certainly \( G \notin (\ast) \) [\( (c) \) then follows].

(d) \( uMiu^{-1} \cap M \neq \{1\} \); hence \( uMiu^{-1} = M, u \in N(M) \).

(e) Let \( g_0 = q_0m(n_0m + 1) \). As \( M \subseteq G_0 \), \( r = g/g_0 < m \) and \( r(n_0m + 1) = (q/q_0)(nm + 1) \); obviously \( q_0 \mid g \). Since \( r \) and \( q/q_0 \) are positive integers, less than \( m \), it follows that \( r = q/q_0 \) and \( n = n_0 \).

Assume that \( G \in (\ast) \) and \( G_0 \cap M = M_0 \neq \{1\} \). Suppose that \( N_{G_0}(M_0) \neq M_0 \); then by Theorem 2.2 (a), \( G_0 \supseteq M \) and \( g_0 = q_0m(nm + 1) \), \( q_0 > 1 \). Also \( G_0 \in (\ast) \), since otherwise the normal complement of \( N_{G_0}(M) \) in \( G_0 \) would be a normal complement of \( N_G(M) \) in \( G \), contrary to the assumption that \( G \in (\ast) \). Thus it remains only to show that the case \( N_{G_0}(M_0) = M_0 \) is impossible. But then by the Frobenius Theorem \( M_0 \) has a normal complement \( D \) in \( G_0 \) such that \( G_0 = M_0D, M_0 \cap D = \{1\} \). \( D \) is a characteristic
subgroup of $G_0$, hence normal in $G$ and $D \cap N_\sigma(M) = \{1\}$. As $M_0$ is a Hall subgroup of $G_0$ and the normalizer in $G$ of any Sylow subgroup of $M_0$ is contained in $N_\sigma(M)$, it follows, by [6], p. 136, that $G = N_\sigma(M)G_0 = N_\sigma(M)D$ in contradiction to $G \in (\ast)$.

(f) Follows immediately from Theorem 2.2 (b) and Part (e) of this theorem.

(g) If $G \in (\ast)$ then $N(M) \neq M$; hence (g) follows from Parts (f) and (e) of this theorem.

(h) Since $G_1 \cap M = \{1\}$, it follows from Theorem 2.2 (a) that $G_1 \cap N(M) = \{1\}$. Therefore $G_1M$ is a Frobenius group with the Frobenius kernel $G_1$ and consequently $G_1$ is nilpotent, its order is $nm + 1$ and $M$ is a CP-group. It follows by Theorem 2.2 (c) and the assumption $N(M) \neq M$ that $M$ is a cyclic group of odd order and $Q$ is a cyclic group. Moreover, the order of the group $G_1N(M)$ is $qmG_1$ and consequently $G_1 \mid nm + 1$. Let $r = (nm + 1)/(um + 1)$; then $r \equiv 1 \pmod{m}$ and $r = vm + 1$. Hence $n = wmn + u + v$. Let $h \in M^\#$; then $C_G(h) \cap G_1 = \{1\}$ and it follows from [4], Lemma 2.1 that $G_1$ is contained in the kernel of all characters of $G$ nonvanishing on $M^\#$. The above lemma and the fact that $M \cap G_1 = \{1\}$ imply that $M \cap G_1 = \{1\}$ contains the centralizer of each of its non-unit elements and $\overline{M} = M$. Let $\overline{q}m$ be the order of the normalizer of $M$ in $G$. Since $N(M) \cap G_1 = \{1\}, q \leq \overline{q} \leq m - 1$, and by Corollary 2.1 $M$ is a TI-set in $G$. Now the order of $G$ can be expressed in two forms:

$$\overline{g} = \overline{q}m(\overline{q}m + 1) = qm(vm + 1).$$

Hence $\overline{q} = q$ and the order of the normalizer of $\overline{M}$ in $\overline{G}$ is $qm$.

Assume that $G \in (\ast)$ and $u = n$; then $G_1$ is a normal complement of $N(M)$ in $G$ in contradiction to $G \in (\ast)$. Thus $u < n, v > 0$ and $n \geq m + 2$. Finally it follows from the isomorphism theorems that if $G \not\in (\ast)$ then also $G \not\in (\ast)$. This remark completes the proof of Part (h) and of the theorem.

**COROLLARY 2.2.** Let $G \in$ Theorem 2.3 and suppose that $N(M) \neq M, G$ and $M$ is not a cyclic group of odd order. Then:

(a) If $\{1\} \neq G_0 \subset G, \mid G_0 \mid = g_0$ then $G_0 \cap M$ and $g_0 = qG_0(mnm + 1), g_0 \mid q, g_0 > 1.$ Hence $G$ is nonsolvable.

(b) $G$ contains a normal simple non-cyclic subgroup $G^*$ of order $q^*m(nm + 1), q^* \neq 1$. If $p$ is the least prime number dividing $q$ then $[G : G^*] \leq q/p$. In particular, if $q$ is a prime number, then $G$ is a simple group.

**Proof.** Since $N(M) \neq M$ and $M$ is not a cyclic group of odd order, it follows from Theorem 2.3 (h), (e) that $G \in (\ast)$ and that (a) holds. Let $G^*$ be the minimal normal non-trivial subgroup of $G$. Then, by [6], Theorem 4.4.4
and Part (a) of this corollary, \( G^* \) is a noncyclic simple group. The rest of Part (b) follows easily.

**Corollary 2.3.** Let \( G \in \text{Theorem 2.3} \) and suppose that \( G \) is solvable. Then one of the following statements is true:

(I) \( N(M) = G; \) \( G \) is a Frobenius group and \( M \) is its Frobenius kernel. \( M \) is nilpotent.

(II) \( N(M) = M; \) \( G \) is a Frobenius group and the normal complement of \( M \) in \( G \) is the Frobenius kernel. \( M \) is a CP-group.

(III) \( N(M) \neq M, G; \) \( G \neq (\ast) \), \( M \) is a cyclic group of odd order and \( N(M) \) is metacyclic.

**Proof.** If either \( N(M) = G \) or \( N(M) = M \) then certainly (I) or (II), respectively, hold. If \( N(M) \neq M, G \) then it follows from Theorem 2.3 (g) that \( G \neq (\ast) \). The normal complement of \( N(M) \) in \( G \) being nontrivial implies, by Theorem 2.3 (h), that \( M \) is a cyclic group of odd order and \( N(M) \) is metacyclic.

### 3. Groups with a CCT-Subgroup

In this section we will derive some simple, but very important for us, conclusions from Theorem 2 and its Corollaries in [3].

Groups satisfying the following assumptions will be studied.

**Hypothesis A.** The finite group \( G \) contains a CC-subgroup \( M \) of order \( m \). Furthermore, if \( |N(M)| = qm \) then \( q \neq 1, m - 1 \) and \( M \) is neither normal in \( G \) nor a non-Abelian \( p \)-group with \( [M : M'] < 4q^2 \).

By Corollary 2.1 the group \( G \) satisfies Hypothesis II in [3] with \( h = 1 \); also the assumptions of Theorem 2 in [3] are fulfilled with respect to \( G \). In this and the following sections the results and notation of [3], Section 2 will be used, sometimes without any further reference. An additional notation will be now introduced.

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>( C_i ) (( i = 1, \ldots, t ))</td>
<td>the number of conjugate classes in ( N(M) ) and in ( G ) meeting ( M^# ) [see Theorem 2.3 (d)].</td>
</tr>
<tr>
<td>( \bar{C}_i ) (( i = 1, \ldots, t ))</td>
<td>the conjugate classes of ( G ) meeting ( M^# ).</td>
</tr>
<tr>
<td>( h_i ) (( i = 1, \ldots, t ))</td>
<td>the conjugate classes of ( N(M) ) meeting ( M^# ); ( \bar{C}_i = C_i \cap M ).</td>
</tr>
<tr>
<td>( \tilde{C}_i ) (( i = 1, \ldots, t ))</td>
<td>a set of representatives of ( C_i ) and of ( \bar{C}_i, \ i = 1, \ldots, t. )</td>
</tr>
<tr>
<td>( \tilde{\zeta}_i ) (( i = 1, \ldots, t ))</td>
<td>the irreducible characters of ( N(M) ), vanishing outside ( M ).</td>
</tr>
</tbody>
</table>
\( \zeta_i (i = 1, \ldots, t) \)  a set of irreducible characters of \( M \) inducing \( \zeta_i \) in \( N(M) \). Let \( z_i = \zeta_i(1) \) for \( i = 1, \ldots, t \). Since \( M \) is nilpotent, we may assume that \( z_1 = 1 \).

\( X_i (i = 1, \ldots, t) \) the exceptional characters of \( G \), associated with \( \zeta_i \) 
\( \theta_i (i = 1, \ldots, d) \) the nonexceptional irreducible characters of \( G \), non-vanishing on \( M^\# \); \( \theta_1 = 1_G \).

\( s_{ijk} (1 \leq i, j, k \leq t) \) the coefficient of \( \bar{C}_h \) in \( \bar{C}_i \bar{C}_j \).

\( e_{ijk} (1 \leq i, j, k \leq t) \) the coefficient of \( C_h \) in \( C_iC_j \).

We know from [3], Corollary 2.4 that

\[
X_i(h) = e\zeta_i(h) + z_i c, \quad \forall h \in M^\#, \quad i = 1, \ldots, t,
\]

\[
\theta_i(h) = c_i, \quad \forall h \in M^\#, \quad i = 1, \ldots, d,
\]

where \( c, c_i (i = 1, \ldots, d) \) are rational integers and \( \varepsilon = \pm 1 \).

Furthermore, it follows from Corollary 2.1 and Lemma 2.2 of [3] that:

\[
z_s x_1 = z_s x_1 = x_s, \quad \zeta_s(1) = q z_s, \quad s = 1, \ldots, t,
\]

\[
\sum_s \zeta_s(h_i) \zeta_s(h_i^{-1}) = \delta_{i, n(h_i)} - q,
\]

\[
\sum_s \zeta_s(h_i) z_s = -1, \quad \sum_s z_s^2 = \frac{m-1}{q},
\]

where \( n(h_i) = n_C(h_i) = n_M(h_i) \) and the summation ranges over \( s = 1, \ldots, t \).

Let \( v = (m - 1)/q \). It follows from

\[
am = \sum_M X_i(h) = x_1 + \varepsilon \sum_{M^\#} \bar{\zeta}_i(h) + (m - 1) c = x_1 - eq + qvc
\]

that

\[
x_1 = am + q(\varepsilon - vc), \quad a \geq 0.
\]

As \( x_s = z_s x_1 \), we get

\[
x_s = z_s [am + q(\varepsilon - vc)], \quad a \geq 0.
\]

Let

\[
T = \sum_i c_i^3, \quad S = \sum_i \frac{c_i^3}{\theta_i(1)}
\]

where \( \sum_i \) denotes summation over \( i = 1, \ldots, d \). This notation, together with \( \sum_s \) denoting summation over \( s = 1, \ldots, t \), will be used throughout this work.
Since \[ \theta_i(1) + (m - 1) c_i = b_i n, \quad b_i \geq 0, \]

it follows that
\[ \frac{c_i}{\theta_i(1)} \geq - \frac{1}{m - 1}, \]

and consequently
\[ S \geq 1 - \frac{T - 1}{m - 1}. \]

Also if \( \theta_i(1) < m - 1 \), then \( \theta_i(1) = c_i \).

Let
\[
B_{ijk} = \sum_{s} \frac{\xi_s(h_i) \xi_s(h_j) \xi_s(h_k^{-1})}{\xi_s(1)} , \quad 1 \leq i, j, k \leq t, \\
A_{ijk} = \sum_{s} \frac{X_s(h_i) X_s(h_j) X_s(h_k^{-1})}{x_s} , \quad 1 \leq i, j, k \leq t.
\]

It is well-known that, for all \( 1 \leq i, j, k \leq t, \)
\[ s_{ijk} = \frac{q^m}{n(h_i)n(h_j)} (B_{ijk} + q) , \quad c_{ijk} = \frac{g}{n(h_i)n(h_j)} (A_{ijk} + S). \quad (1) \]

Finally let
\[ \delta_{ijk} = \delta_{ik} + \delta_{jk} + \delta_{ij^*} , \quad 1 \leq i, j, k \leq t \]

and
\[ K = \nu \sigma^3 - 3c^2 \varepsilon - 3cq. \]

Our first result in this section is

**Theorem 3.1.** Let \( G \in \text{Hypothesis A}. \) Then at least one of the following statements is true:

(I) \( q < (m - 1)^{1/2}, \ c = 0, \ T = q, \)

(II) \( q > m^{1/2} - 1, \ M \) is elementary Abelian and contains no nontrivial proper subgroups which are normal in \( N(M). \)

**Proof.** We need the following lemma, which is important by itself.
Lemma 3.1. Let $G \in \text{Hypothesis } A$. Then

(a) $(vc - e)^2 + vT = m$,
(b) $T \leq q$, $S \geq 1 - (q - 1)(m - 1) > \frac{1}{2}$,
(c) $c \leq (1/v) [(m - 2v)^{1/2} + 1]$,
(d) if $q < (m - 1)^{1/2}$, then $c = 0$, $T = q$.

Proof of Lemma 3.1. (a) Let $h \in M^#$; then

$$n(h) = \sum_{s} X_s(h) X_s(h^{-1}) + T = \sum_{s} (e \xi_s(h) + z_s c) (e \xi_s(h^{-1}) + z_s c) + T$$

$$= \sum_{s} \xi_s(h) \xi_s(h^{-1}) + ec \sum_{s} (\xi_s(h) z_s + \xi_s(h^{-1}) z_s) + c^2 \sum_{s} z_s^2 + T$$

$$= n(h) - q - 2ec + c^2 \frac{m - 1}{q} + T,$$

$$m - 1 = vq = c^2 v^2 - 2ecv + Tv, \quad m = (vc - e)^2 + vT.$$

(b) By (a), $T \leq (m - 1)/v = q$. The rest of (b) follows.

(c) Obviously $T \geq 1$. If $T = 1$, then

$$0 = \sum_{s} X_s(h_i) x_s + 1 = x_1 \sum_{s} X_s(h_i) x_s + 1,$$

which is impossible since $1/x_1$ is not an algebraic integer. Hence $T \geq 2$ and by Part (a), $|c| \leq (1/v) [(m - 2v)^{1/2} + 1]$.

(d) $vq = m - 1$; since $q < (m - 1)^{1/2}$, $\nu > (m - 1)^{1/2}$ and

$$|c|^2 < \left[ \frac{1}{(m - 1)} \right] [m - 2(m - 1)^{1/2} + 1 + 2(m - 1)^{1/2} - 2] = 1.$$  

Hence $c = 0$, and by (a), $T = q$.

Theorem 3.1 is an immediate consequence of Lemma 3.1 (d) and Theorem 2.2 (e).

Theorem 3.2. If $G \in \text{Hypothesis } A$ then the following relation holds

$$A_{ijk} = \frac{1}{x_1} \{eqB_{ijk} + c[\delta_{ij}n(h_i) + \delta_{ik}n(h_i) + \delta_{jk}n(h_k)] + K\}$$

for all $1 \leq i, j, k \leq t$. 


Proof.

\[ x_1 A_{ijk} = x_1 \sum_h \left( e^{\tilde{h}}_{\alpha}(h_i) + z_{\alpha} \right) \left( e^{\tilde{h}}_{\beta}(h_j) + z_{\beta} \right) \left( e^{\tilde{h}}_{\gamma}(h_k^{-1}) + z_{\gamma} \right) / x_1 \]

\[ = eq \sum_s \xi_s(h_i) \xi_s(h_j) \xi_s(h_k^{-1}) / \xi_s(1) \]

\[ + c \sum_s [ \xi_s(h_i) \xi_s(h_j) + \xi_s(h_i) \xi_s(h_k^{-1}) + \xi_s(h_j) \xi_s(h_k^{-1}) ] \]

\[ + c^2 \sum_s [ \xi_s(h_i) + \xi_s(h_j) + \xi_s(h_k^{-1}) ] z_s + c^3 \sum_s z_s^3 \]

\[ = eq B_{ijk} + c [ \delta_{ij} n(h_i) + \delta_{ik} n(h_i) + \delta_{jk} n(h_i) - 3q ] - 3c^2 \epsilon + c^3 \nu. \]

Theorems 3.1 and 3.2 immediately yield

**Corollary 3.1.** Let \( G \in \text{Hypothesis A} \). Then for all \( 1 \leq i, j, k \leq t \) the following statements are true:

1. If \( M \) is Abelian, then:

\[ x_1 A_{ijk} = eq B_{ijk} + cm \delta_{ijk} + K. \]

In particular, the formula holds if \( q > m^{1/2} - 1 \).

2. If \( q < (m-1)^{1/2} \), then

\[ A_{ijk} = eq x_1 B_{ijk}, \quad c_{ijk} = \frac{eq}{n(h_i) n(h_j)} \left( \frac{eq}{x_1} B_{ijk} + S \right). \]

**Theorem 3.3.** Let \( G \in \text{Hypothesis A} \) and suppose that \( c_{ijk} = 0 \) for some \( (i, j, k) \). Then one of the following statements is true:

1. \( q > m^{1/2} - 1, \) \( M \) is elementary Abelian and no nontrivial proper subgroup of \( M \) is normal in \( N(M) \).

2. \( q \leq m^{1/2} - 1, \) \( G \) is solvable, \( N(M) \) is metacyclic and has a nilpotent normal complement in \( G, M \) is cyclic of odd order.

**Proof.** If \( q > m^{1/2} - 1 \) then (I) holds by Theorem 2.2 (e). Thus assume that \( q \leq m^{1/2} - 1 \). If \( G \notin (\ast) \) then (II) holds by Theorem 2.2 (h). Now let \( G \) be a group of minimal order satisfying the assumptions of this theorem together with \( q \leq m^{1/2} - 1 \) and \( G \in (\ast) \). We will show that such \( G \) does not exist, thus proving the theorem. By Theorem 3.1, \( e = 0 \) and \( T = q \). Since \( c_{ijk} = 0 \) also \( s_{ijk} = 0 \), and Eq. (1) together with Corollary 3.1 yield \( B_{ijk} = -q, S = eq^2 / x_1 \). As \( S > 0, e = 1 \) and consequently \( x_1 = am + q \). If \( a > 1 \), then

\[ \frac{eq^2}{m+q} > S \geq 1 - \frac{q-1}{m-1}, \quad q^2 \geq m, \]
in contradiction to the assumption that $q \leq m^{3/2} - 1$. Hence $x_1 = q$, $S = q$ and $q = S \leq T = q$. Therefore $\theta_i(1) = c_i$ for all $i$ and $M$ is contained in the kernel of each $\theta_i$, $i = 1, \ldots, d$. Let $U = \ker \theta_2$, since $T = q > 1$, $\theta_2$ exists. It follows from Theorem 2.3 (c) that $|U| = q_m(mn + 1)$, $1 < q_u < q \leq m^{3/2} - 1$. $U$ satisfies the assumptions of this theorem and $q_u \leq m^{3/2} - 1$, $U \in (\ast)$ in contradiction to the minimality of $G$. The proof is complete.

**Corollary 3.2.** In Theorem 3.3 assume that $G$ is nonsolvable. Then (I) holds.

4. **Groups with a CCT-Subgroup $M$ whose Order is Divisible by 3**

In most of this section the group $G$ will be supposed to satisfy the following conditions:

**Hypothesis B.** The finite group $G$ satisfies Hypothesis A. Furthermore, $3 \mid m$.

We introduce the following additional notation:

- $t_0$ the number of conjugate classes of elements of order 3 in $N(M)$ and in $G$.
- $C_i (i = 1, \ldots, t_0)$ the conjugate classes of elements of order 3 in $G$.
- $C_i (i = 1, \ldots, t_0)$ the conjugate classes of elements of order 3 in $N(M)$.

$$B = \{(i, i, i^\ast) \mid 1 \leq i \leq t_0 \}.$$
$$E = \{(i, j, k) \mid 1 \leq i, j, k \leq t_0 \}.$$

**Theorem 4.1.** Let $G \in$ Hypothesis B and suppose that $(i, j, k) \in E - B$. Then

$$c_{ijk} = s_{ijk}.$$

**Proof.** Let $x \in C_i$, $y \in C_j$, $z \in C_k$ and $xy = z$. We will show that then $x$, $y$ and $z$ all belong to $M^u$ for some $u \in G$, thus proving the theorem since $M$ is a TI-set.

We may assume that $x \in M$. Suppose that $y, z \notin M$. By Theorem 1 of [5], $K = \langle x, y \rangle$ is a solvable subgroup of $G$, being a homomorphic image of the solvable infinite polyhedral group $(3, 3, 3)$. Let $L = K \cap M$; $L$ is a nilpotent group and $L$ must be a CP-group, since otherwise, by Corollary 2.3, $L < K$ and $K \subseteq N_G(L) = N(M)$ which was assumed not to be the case. Thus the Sylow 3-group of $L$ is cyclic, and hence either $|N_K(L)| = 2 |L|$ or $N_K(L) = L$. In the first case, $2 \mid q$, $v^* = v$ for all $v \sim t$ and $K$ has only one class of ele-
ments of order 3, in contradiction to the assumption that \((i, j, k) \in E - B\). In the second case, \(N_k(L) = L\) and, by the Frobenius theorem, \(L\) has a normal complement \(R\) in \(K\). Since \(L\) is nilpotent and its Sylow 3-group is cyclic, \(x, y \in Z(L)\). Hence the cosets \(xR\) and \(yR\) are equal to the conjugate classes \(Cl_k(x)\) and \(Cl_k(y)\) respectively, since for \(u = x\) or \(y\) we have

\[
luRl^{-1}R = (lu^{-1})R = uR \quad \text{for all} \quad l \in L
\]

and \(|uR| = |Cl_k(u)|\). If \(xR = yR\), then \(x = x^{-1}R = x^{-1}R\) and \((i, j, k) \in B\), which is not the case. Finally, if \(xR \neq yR\), then \(yR = x^{-1}R\) and \(x \in x^{-1}R = R\), in contradiction to the definition of \(R\). Thus \(y, z \notin M\) is impossible, and the proof is complete.

**Corollary 4.1.** Let \(G \in \text{Hypothesis B}\) and suppose that \(s_{ijk} = 0\) for some \((i, j, k) \in E - B\). Then \(q > m^{1/2} - 1\) and \(M\) is elementary Abelian.

**Proof.** By Theorem 4.1 \(c_{ijk} = 0\). As \(E - B\) is not the empty set, \(M\) is noncyclic, in which case Theorem 3.3 implies the result.

**Corollary 4.2.** Let \(G \in \text{Hypothesis B}\). Then the set of all elements of order 3 in \(M\), together with 1, form an Abelian characteristic subgroup \(M_0\) of \(M\), contained in \(Z(M)\).

**Proof.** Let \(x \in M - Z(M)\) and suppose that \(x\) has order 3. Choose any \(y\) of order 3 in \(Z(M)\) and let \(x \in \mathcal{C}_x, y \in \mathcal{C}_y\). Then \((j, j, i) \in E - B\) and \(s_{jji} = 0\). It follows from Corollary 4.1 that \(M\) is elementary Abelian, contradicting the existence of \(x\). Therefore all the elements of order 3 in \(M\) are contained in \(Z(M)\), where they form, together with 1, a characteristic subgroup \(M_0\), which is also characteristic in \(M\).

**Corollary 4.3.** Let \(G \in \text{Hypothesis B}\) and suppose that \(q\) is odd. Then \(t_0\) is even.

**Proof.** By Corollary 4.2 \(t_0 = (m_0 - 1)/q\), where \(m_0 = |M_0|\). Since \(m_0\) is odd, not 1, and \(q\) is odd, \(t_0\) must be even.

**Corollary 4.4.** Let \(G \in \text{Hypothesis B}\) and suppose that \(q < (m - 1)^{1/2}\) and \((i, j, k) \in E - B\). Let Case I mean that either \(t_0 > 2\) or \(t_0 = 2, 2 \mid q\), and let Case II mean that \(t_0 = 2, 2 \not\mid q\). Then:

in Case I:

\[
B_{ijk} = \frac{m}{t_0} - q, \quad s_{ijk} = \frac{q}{t_0};
\]

in Case II:

\[
B_{ijk} = \frac{q - 1}{q} \frac{m}{t_0} - q, \quad s_{ijk} = \frac{q - 1}{t_0}.
\]
Proof. First we will show that all $B_{ijk}, (i, j, k) \in E - B$ are equal to each other. By Theorem 4.1, Corollary 3.1, and Eq. (1), each $B_{ijk}, (i, j, k) \in E - B$ is a root of the linear equation

$$X + q = \frac{g}{qm} \left( \frac{eq}{x_1} X + S \right).$$

But $\epsilon qq/\epsilon mx_1 \neq 1$, since otherwise $g = mx_1 < mg^{1/2}$ and $g < m^2$, in contradiction to Theorem 2.3 (c). Thus the above equation has one root only, and the $B_{ijk}, (i, j, k) \in E - B$ are all equal to each other. So are the $s_{ijk}, (i, j, k) \in E - B$.

By Corollary 4.2, the classes $\bar{C}_i (i = 1, \ldots, t_0)$ are in the center of $M$, and therefore a product of two elements of order 3 in $N(M)$ is again an element of order 3.

Case I. In view of our opening remark we may assume that $k \neq j, j^*$. Then

$$q = \sum_{u=1}^{t_0} s_{ijk} = t_0 \frac{q}{m} (B_{ijk} + q); \quad B_{ijk} = \frac{m}{t_0} - q, \quad s_{ijk} = \frac{q}{t_0}.$$

Case II. Since $1^* = 2$, we may assume that $(i, j, k) = (1, 2, 2)$. Then

$$q = 1 + \sum_{u=1}^{t_0} s_{ijk} = 1 + t_0 \frac{q}{m} (B_{ijk} + q);$$

$$B_{ijk} = \frac{g - 1}{q} \frac{m}{t_0} - q, \quad s_{ijk} = \frac{g - 1}{t_0}.$$

Corollary 4.5. Let $G \in Hypothesis B$ and suppose that $q < (m - 1)^{1/2}$ and $t_0 > 1$. Then $\epsilon = -1$ and, for each $(i, j, k) \in E - B$,

$$g = mq(B_{ijk} + q) x_1(- qB_{ijk} + x_1 S)^{-1}.$$

Proof. It was shown in the proof of Corollary 4.4 that:

$$g = mq(B_{ijk} + q) x_1(eqB_{ijk} + x_1 S)^{-1};$$

thus it remains only to show that $\epsilon = -1$. It follows from Corollary 4.4 that $B_{ijk} > 0$ for $(i, j, k) \in E - B$; in Case I this is obvious, while in Case II it results from

$$B_{ijk} = \frac{q - 1}{q} \frac{m}{t_0} - q \geq \frac{m}{q} - q \geq \frac{q^2 + 1}{q} - q > 0.$$
Thus if \( \epsilon = 1 \), we would have in both cases:

\[
g \leq \frac{m^2 q}{S t_0} \leq \frac{m^2 q}{t_0 [1 - q/(m - 1)]} \leq \frac{m^2 q}{t_0 (1 - 1/t_0)} \leq m^2 q,
\]

in contradiction to Theorem 2.3 (c). Hence \( \epsilon = -1 \) and the proof is complete.

COROLLARY 4.6. Let \( G \in \text{Hypothesis B} \) and suppose that \( q \) is odd. Then \( q \geq (m - 1)^{1/2} \) and \( M \) is elementary Abelian.

Proof. By Corollary 4.3, \( t_0 \) is even. Suppose that \( q < (m - 1)^{1/2} \). Case I of Corollary 4.4 is impossible, since then there exists \((i, j, k) \in E - B\) to which there corresponds the rational integer \( s_{ijk} = q/t_0 \), in contradiction to the assumption that \( q \) is odd. Therefore we will assume having Case II of Corollary 4.4. Then: \( t_0 = 2 \), \( s_{122} = s_{222} = s_{121} = \frac{1}{2} (q - 1) \), and since \( q = s_{112} + s_{122} \), we get \( s_{112} = \frac{1}{2} (q + 1) \) and \( B_{112} = m(q + 1)/2q - q \).

For all \((i, j, k) \in E\), obviously \( s_{ijk} \leq c_{ijk} \); hence by Eq. (1) and Corollary 3.1, \( 0 < s_{ijk} \) implies that

\[
gm(R_{ijk} + q) \leq g \left( \frac{eq}{x_1} R_{ijk} + S \right), \quad g \geq \frac{gm(B_{ijk} + q) x_1}{eq B_{ijk} + x_1 S} > 0
\]

with equality at least for \((i, j, k) \in E - B\). Since \( s_{112} , s_{122} > 0 \), it follows that

\[
g \geq \frac{gm(B_{112} + q) x_1}{-q B_{112} + x_1 S}, \quad g = \frac{gm(B_{122} + q) x_1}{-q B_{122} + x_1 S}.
\]

We will consider now the function:

\[
f(x) = \frac{mg(x + q) x_1}{-q x + x_1 S}.
\]

This is an increasing function for \( x < x_1 S/q \). As \( s_{112} > s_{122} > 0 \), also \( B_{112} > B_{122} \), and \( B_{112} , B_{122} < x_1 S/q \). Hence

\[
g \geq f(B_{112}) > f(B_{122}) = g,
\]

a contradiction. This contradiction proves that \( q \geq (m - 1)^{1/2} \) and the corollary follows by Theorem 2.2 (e).

THEOREM 4.2. Let \( G \in \text{Hypothesis B} \). Then \( M \) is an Abelian group of odd order.

Proof. If \( q \) is odd, the theorem follows from Corollary 4.6; if \( q \) is even, it is well-known.
Corollary 4.7. Let $G \in \text{Hypothesis } B$ and suppose that $t_0 > 2$. Then

$$c = K = 0, \quad T = q.$$ 

Proof. $M$ being Abelian, $v = t$, and Eq. (1) becomes

$$s_{ijk} = \frac{1}{m} (q B_{ijk} + q^2), \quad c_{ijk} = \frac{g}{m^2} (A_{ijk} + S) \quad (3)$$

for all $1 \leq i, j, k \leq t$. Let $(i, k, k) \in E - B, k \neq i, i^*$ and let $j$ be different from either of $i, i^*, k, k^*$. Obviously also $(i, j, k) \in E - B$. Since $t_0 > 2$ it was possible to make such a choice; because if $2 \mid q$ then $i = i^*, k = k^*$ and there are at least two possibilities for $j$; while if $2 \not\mid q$, then $t_0 \geq 8$ since if $4 \mid m_0 - 1$ then also $8 \mid m_0 - 1$, and if $4 \not\mid m_0 - 1$ then $t_0 \geq 2.5 > 8$, and there are at least 4 possibilities for choosing $j$.

By Theorem 4.1, $s_{ijk} = c_{ijk}$ and $s_{ikk} = c_{ikk}$. It follows from Corollary 3.1 and Eq. (3) that

$$q B_{ikk} + q^2 = \frac{g}{m x_1} (eq B_{ikk} + K + x_1 S + cm),$$

$$q B_{ijk} + q^2 = \frac{g}{m x_1} (eq B_{ijk} + K + x_1 S),$$

which by subtraction yield

$$q(B_{ikk} - B_{ijk}) = \frac{g}{m x_1} [eq(B_{ikk} - B_{ijk}) + cm]. \quad (4)$$

It follows from Eq. (3) that

$$q(B_{ikk} - B_{ijk}) = m(s_{ikk} - s_{ijk}) = mL, \quad L \text{-an integer.}$$

Suppose that $L \neq 0$; then Eq. (4) yields

$$g = \frac{m^2 L x_1}{L m e + cm} = \frac{m x_1}{e + c / L} \leq \frac{m x_1}{e + c / L} \left(1 - \left|\frac{c}{|c| + 1}\right|\right)^{-1}$$

the last inequality following from the fact that both $c$ and $L$ are integers. Thus by Lemma 3.1:

$$g \leq mx_1 (|c| + 1) \leq \frac{mx_1}{t} [(m - 2)^{1/2} + 1 + \ell]. \quad (5)$$

Since for $q \leq m^{1/2} - 1$ the corollary follows from Theorem 3.1, it suffices
to prove it for the case when \( q > m^{1/2} - 1 \) and \( t < m^{1/2} + 1 \). As \( x_1^2 < g/t \), (5) yields then

\[
g^2 \leq \frac{9m^2 (m - 1)}{t},
\]

\[
g \leq \frac{9}{t^2} \frac{m - 1}{t} m^2 \leq \frac{9}{16} qm^2 <qm^2,
\]

in contradiction to Theorem 2.3 (c).

Thus, if \( q > m^{1/2} - 1 \), then \( L = 0 \) and Eq. (4) implies that also \( c = K = 0 \); \( T = q \) by Lemma 3.1. The proof is complete.

**Corollary 4.8.** Let \( G \in \) Hypothesis B and suppose that \( t_0 > 2 \). Then

\[
g = m^{-3} g x_1 (q(m - q) + t_0 x_1 S)^{-1}
\]

and \( \epsilon = -1 \).

**Proof.** It follows from Theorem 4.1, Eq. (3), and Corollary 4.7 that, for all \((i, j, k) \in E - B\),

\[
qB_{ijk} + q^2 = \frac{g}{mx_1} (eqB_{ijk} + x_j S).
\]

It is impossible that \( g / mx_1 = 1 \) since then \( g - mx_1 < mg^{1/2} \), \( g < m^2 \) in contradiction to Theorem 2.3 (c). Thus Eq. (6) implies that \( B_{ijk} \), \((i, j, k) \in E - B\) are all equal to each other; so are the \( s_{ijk} \), \((i, j, k) \in E - B\).

Let \((i, j, k) \in E - B\), \( k \neq j, j^* \); such \((i, j, k) \) exists since \( t_0 > 2 \). Then by Eq. (3)

\[
q = \sum_{w=1}^{t_0} s_{ijk} = \frac{t_0}{m} (qB_{ijk} + q^2), \quad qB_{ijk} = \frac{mq}{t_0} - q^2,
\]

which, when inserted into (6), yields

\[
g = mx_1 mq [q(m - q t_0) \epsilon + t_0 x_1 S]^{-1}.
\]

If \( \epsilon = 1 \), then

\[
g < \frac{m^2 q}{2[1 - (q - 1)/(m - 1)]} < m^2 q,
\]

in contradiction to Theorem 2.3 (c). Hence \( \epsilon = -1 \) and the formula for \( g \) follows.
**Theorem 4.3.** Let $G \in \text{Hypothesis B}$ and suppose that $M$ is elementary Abelian. Then $q = \frac{1}{2} (m - 1)$ and $G$ is a simple group.

**Proof.** First we will show that $q = \frac{1}{2} (m - 1)$ by assuming that $t \neq 2$ and deriving a contradiction. Since $q < m - 1, t > 1$ and we may assume that $t > 2$. As $t = t_0$, Corollary 4.8 yields

$$g = m^2 q^2 \left[ -\frac{q^2}{x_1} + (m - 1) S \right]^{-1}.$$ 

Since $x = -1$, $x_1 \geq m - q$, $-q^2/x_1 \geq -q^2/(m - q)$ and

$$(m - 1) S > m - 1 - (q - 1) = m - q.$$ 

These facts yield

$$g \leq \frac{m^2 q^2}{-q^2/(m - q) + m - q} = \frac{m^2 q^2 (m - q)}{m(m - 2q)} < \frac{m^2 q^2}{q} = q^m,$$

in contradiction to Theorem 2.3 (c). This contradiction proves that $q = \frac{1}{2} (m - 1)$.

It remains to show that $G$ is a simple group. By Corollary 2.2 (a), if $G_0$ is a nontrivial normal subgroup of $G$, then $G_0$ contains $M$ and $[G_0 : M] = q_0 m (nm + 1)$, where $q_0 \neq 1$ and $q_0 | q$. Thus $G_0 \in \text{Hypothesis B}$ with the same $M$, and by the first part of this proof $q_0 = \frac{1}{2} (m - 1)$.

We are now able to prove the following classification theorem:

**Theorem 4.4.** Let $G$ be a finite group containing a subgroup $M$ which satisfies the following conditions:

(I) $M$ is a noncyclic, elementary Abelian 3-group.

(II) $\forall x \in M^G$, $C(x) \subseteq M$.

Then one of the following statements is true:

(i) $g = qm, M \triangleleft G$, $G$ is a Frobenius group.

(ii) $[N(M) : M] = q = \frac{1}{2} (m - 1)$, $G$ is a simple group.

(iii) $[N(M) : M] = q = m - 1$, $G$ is a simple group.

(iv) $[N(M) : M] - q - m - 1$, $G$ contains a simple normal subgroup of index 2 and of Type (ii).

**Proof.** If $M \triangleleft G$, obviously (i) holds. The case $M \triangleleft G, q = 1$ is impossible, since then, by Theorem 2.1, $M$ is a TI-set with $N(M) = M \neq G$ and hence $G$ is a Frobenius group and $M$ is a cyclic group, which is not the
case. Finally, if $M \triangleleft G$, $q \neq 1$, $m - 1$, then $G \in \text{Hypothesis B}$ and (ii) holds by Theorem 4.3. Thus it remains only to show that, if $M \triangleleft G$, $q = m - 1$, then either Case (iii) or Case (iv) holds. Suppose that $\{1\} \neq G_0 \lhd G$; then if $G_0 \neq G$, Corollary 2.2 yields that $|G_0| = q_0 m (nm + 1)$, $q_0 \neq 1$, $m - 1$ and hence $G_0 \in \text{Hypothesis B}$. Theorem 4.3 then implies that $G_n$ is a simple group of Type (ii) and $[G : G_n] = 2$. Hence either $G$ is a simple group of Type (iii), or (iv) holds. The proof is complete.

5. Groups with a CCT-Subgroup $M$ Whose Order is Divisible by 3 and Whose Index in its Normalizer is Odd

In this section the group $G$ will be supposed to satisfy the following conditions:

**HYPOTHESIS C.** The finite group $G$ satisfies Hypothesis B. Furthermore, $Q$ is a group of odd order.

Finite groups satisfying Hypothesis C will be now completely determined. It is well known that this hypothesis is satisfied by the family of simple groups $PSL(2, 3^w)$, $w > 1$ and odd. On the other hand, we have

**THEOREM 5.1.** Let $G \in \text{Hypothesis C}$. Then $m = 3^w$, $q = \frac{1}{2}(m - 1)$ and $G \cong PSL(2, 3^w)$, $w > 1$ and odd.

**Proof.** Corollary 4.6 and Theorem 4.3 yield the following basic

**LEMMA 5.1.** Let $G \in \text{Hypothesis C}$. Then $M$ is an elementary Abelian 3-group, $q = \frac{1}{2}(m - 1)$ and $G$ is a simple group. Moreover,

$$g = m^2(m - 3) \left\{2 \left[\frac{(2c - s)(m - T)}{x_1} + 2S\right]\right\}^{-1} \leq (q - 1) qm^2. \quad (7)$$

**Proof of Lemma 5.1.** By Corollary 4.6, $M$ is an elementary Abelian 3-group, and therefore, by Theorem 4.3, $q = \frac{1}{2}(m - 1)$ and $G$ is a simple group. It remains only to prove Eq. (7).

First we will prove the formula for $g$. It follows from Theorem 4.1, Corollary 3.1 and Eq. (3) that for all $(i, j, k) \in E - B$:

$$qB_{ijk} + q^2 = \frac{g}{mx_1} (eqB_{ijk} + K + \delta_{ijk} cm + x_1 S). \quad (8)$$

As $t = 2$ and $q$ is odd, $\delta_{ii} = 2$ for all $(i, j, k) \in E - B$. Since $ge/mx_1 = 1$ is impossible, all $B_{ijk}, (i, j, k) \in E - B$ are equal to each other; so are the $s_{ijk}$. 
Consequently
\[ \frac{1}{k}(m - 1) = q = 1 + s_{122} + s_{222}, \quad s_{ijk} = \frac{1}{k}(m - 3), \quad qB_{ijk} = -\frac{1}{k}(m + 1) \]
both for all \((i, j, k) \in E - B\). A substitution in (8) yields:
\[ g = m^2(m - 3) \left\{ 2 \left[ \frac{-(m + 1)\epsilon + 4K + 8cm}{2x_1} + 2S \right] \right\}^{-1}. \]

Let \( A = -(m + 1)\epsilon + 4K + 8cm \); it remains to show that
\[ A = 2(2c - \epsilon)(m - T). \]
Since, by Lemma 3.1, \((2c - \epsilon)^2 + 2T = m\) and \((2c - \epsilon)^3 = (2c - \epsilon)(m - 2T)\), we have
\[ A = -m\epsilon - \epsilon + 8c^3 - 12c^2\epsilon + 6c(m - 1) + 8cm \]
\[ = -m\epsilon + (8c^3 - 12c^2\epsilon + 6c - \epsilon) + 2cm \]
\[ = (2c - \epsilon)^3 + (2c - \epsilon)\ m = 2(2c - \epsilon)(m - T). \]

To prove the inequality (7) we notice first that \(2c - \epsilon \leq 1\), since otherwise the formula for \(g\) yields
\[ g \leq m^2(m - 3) \left\{ 4 \left[ 1 - \frac{q}{m - 1} \right] \right\}^{-1} = \frac{1}{2} (m - 3) m^2, \]
in contradiction to Theorem 2.3 (c). Therefore \(x_1 \geq -(2c - \epsilon)q\). Moreover, since:
\[ 0 = x_2X_2(h_1) + x_1X_2(h_1) + \sum_{i} c_i\theta_i(1), \quad \sum_{i \neq 1} c_i\theta_i(1) = -(2c - \epsilon) x - 1 > 0, \]
the last inequality following from the fact that \(x_1 \geq q > 1\), at least one \(c_i, i \neq 1\) is positive, hence not less than 1. Taking into account the last three remarks, the formula for \(g\) yields
\[ g \leq m^2(m - 3)/2 \left\{ -\frac{m - T}{q} + 2 - 2 \frac{T - 2}{m - 1} \right\} = \frac{m^2(m - 3)(m - 1)}{2(2m - 3 + 2m - 2 + 4)} \]
\[ = (q - 1)qm^2. \]

The proof of the lemma is complete.

In view of Lemma 5.1, to prove Theorem 5.1 it suffices to prove the following proposition:

**Proposition 5.1.** Let \(G \in \text{Hypothesis C}\) and suppose that \(M\) is an elementary Abelian 3-group and \(q = \frac{1}{k}(m - 1)\). Then \(G \cong \text{PSL}(2, m)\).
Proof of Proposition 5.1. The following additional notation will be now introduced:

\( P_i (i = 1, \ldots) \) the subset \( \{ \theta_i \mid \theta_i \neq 1_G, c_i > 1 \} \) of \( \{ \theta_i \mid i = 1, \ldots, d \} \);

\( P_i (h_i) = c_i \).

\( Y_1 \) the set of \( P_i, i = 1, \ldots; |Y_1| = y_1 \).

\( R_i (i = 1, \ldots) \) the subset \( \{ \theta_i \mid c_i \leq -1 \} \) of \( \{ \theta_i \mid i = 1, \ldots, d \} \);

\( R_i (h_i) = c_i \).

\( Y_2 \) the set of \( R_i, i = 1, \ldots; |Y_2| = y_2 \).

\( D_i (i = 1, \ldots) \) the irreducible characters of \( G \) vanishing on \( M^\# \). The corresponding degrees are \( v_i m(i = 1, \ldots) \).

\( Y_3 \) the set of \( D_i, i = 1, \ldots; |Y_3| = y_3 \). \( \sum_i D_i^2 (1) = zm^2 \).

\( T_1 = \sum_i c_i^2 \quad T_2 = \sum_i c_i^2 \quad T = T_1 + T_2 + 1. \)

Furthermore, \( x \) will denote \( x_1 = x_2 \), and \( \sum_i P_i (\theta) \) or \( \sum_i P_i (\theta) P_i (u) \) will denote summation over all \( P_i \in Y_1 \); a similar notation will be used with respect to \( R_i \in Y_2 \) and \( D_i \in Y_3 \). \( \sum P_i (\epsilon) \) will denote summation over all \( \epsilon \in \Omega^\# \).

In the following lemmas we always assume that \( G \in \) Proposition 5.1.

**Lemma 5.2.** (a) \( x = f g + a m, \) where \( f = -(2c - \epsilon) \geq 1 \) and \( a \) is a nonnegative integer.

(b) If \( P_i \in Y_1 \), then \( P_i (1) = r_i m + c_i \), where \( r_i \) is a positive integer.

(c) If \( R_i \in Y_2 \), then \( R_i (1) = u_i m - |c_i| \), where \( u_i \) is a positive integer such that \( u_i \geq |c_i| \).

**Proof.** (a) By the proof of Lemma 5.1, \( 2c - \epsilon = -f < 0 \); the rest of (a) follows from the general formula for \( x \).

(b) \( P_i (1) + (m - 1) c_i = w_i m, w_i \) — a nonnegative integer. Hence \( P_i (1) = (w_i - c_i) m + c_i \). As \( c_i < m, w_i - c_i \geq 0 \); since \( P_i \) has a trivial kernel, \( r_i = w_i - c_i > 0 \).

(c) is proved similarly.

**Lemma 5.3.** \( Y_1 \) is not empty and if \( P \in Y_1 \), \( P (1) = r m + s \), then

\[
g \leq \frac{q(q - 1) m^2}{[(m - 1) s^3] / (r m + s) + s^2}, \quad nm + 1 \leq \frac{(q - 1) m}{[(m - 1) s^3] / (r m + s) + s^2}.
\]

Further, \( q \neq r m + s \).

**Proof.** It was shown in the last part of the proof of Lemma 5.1 that there exists \( \theta_1 \neq 1_G \) such that \( c_i \geq 1 \). Hence \( Y_1 \) is nonempty.
Lemma 5.1 yields the following inequality:

\[
g \leq \frac{m^2(m - 3)}{2 \left[ \frac{m - T}{q} + 2 + \frac{2s^2}{rm + s} - \frac{2 T - 1 - s^2}{m - 1} \right]} = \frac{q(q - 1) m^2}{(m - 1) s^3 + s^2},
\]

which is the first part of (9); since \( g = qm(nm + 1) \), the second part follows.

Suppose that \( q \mid rm + s \); then, since \( q \mid r(m - 1) \), \( q \mid r + s \). It follows, from the definition of \( T \) and from Lemma 3.1 (a), that \( s^2 < T \leq q \); since by (9) \( r < q \), we must have \( q = r + s \). Furthermore, by (9)

\[(rm + s)^2 < g < (qm/s)^2, \quad s(rm + s) < qm, \quad sr < q.\]

Hence

\[s(q - s) < q, \quad q(s - 1) < s^2 < q, \quad s = 1.\]

It follows that \( P(1) = q(m - 2) \) and \( m - 2 \mid nm + 1 \). Hence \( m - 2 \mid 2n + 1 \), \( n \geq \frac{1}{2} (m - 3) = q - 1 \), contradicting (9). Therefore \( q \nmid rm + s \) and the proof is complete.

**Lemma 5.4.** Assume that \( R \in Y_2 \) with \( R(1) = um - w, \ u > w. \) Then

\[
g \leq \frac{q(q - 1) m^2}{w^3 - (w^3/u)}, \quad nm + 1 \leq \frac{(q - 1) m}{w^3 - (w^3/u)}. \tag{10}
\]

Furthermore, \( q \nmid um - w. \)

**Proof.** Lemma 5.1 yields the following inequality:

\[
g \leq \frac{m^2(m - 3)}{2 \left[ \frac{m - T}{q} + 2 - \frac{w^3}{um - w} \right]} \leq \frac{m^2(m - 1) (m - 3)}{2 \left[ -2m + 2T + 2m - 2 - 2T + 2 + 2w^2 - 2(2w^3/u) \right]} = \frac{q(q - 1) m^2}{w^3 - (w^3/u)},
\]

which is the first part of (10); the second part follows.

Suppose that \( q \mid um - w. \) Then, since \( q \mid u(m - 1) \), \( q \mid u - w \) and consequently

\[u \geq q + w, \quad g > (um - w)^2 \geq (u - 1)^2 m^2 \geq q^2 m^2,
\]

in contradiction to inequality (7). Therefore \( q \nmid um - w \) and the proof is complete.
Lemma 5.5. Under the assumptions of Lemma 5.3,

\[ P(1) = s(nm + 1). \]

Proof. Let \( d_1 = (q, rm + s), d_2 = (m, rm + s), d_3 = (nm + 1, rm + s). \) Then \( rm + s \mid d_1d_2d_3 \) and \( d_1 \mid r + s, d_2 \mid s, d_3 \mid sn - r. \) Hence

\[ rm + s \mid (r + s)s \mid sn - r. \] (11)

It will be shown that this implies that \( r = sn, \) thus proving the lemma.

Suppose that \( sn > r. \) Then by (11) \( rm + s < s^2rn + s^2n; \) since by (9) \( s^2n < q - 1, \) this yields \( rm + s < (q - 1)r + s^2n \) and consequently

\[ s^2n > (q + 2)r + s. \]

This inequality, together with (9), yields:

\[ \frac{r(q + 2)}{s^2} < n < \frac{q - 1}{[(m - 1)s^2]/(rm + s) + s^2}. \]

It follows that

\[ \frac{r(m - 1)}{rm + s} + \frac{r}{s} < 1 \]

and consequently

\[ srm - sr + r^2m + sr < srm + s^2, \]

\( r^2m < s^2 < q, \)

a contradiction.

Suppose that \( sn < r. \) Then, by (11), \( rm + s < sr(r + s). \) Since

\[ r^2m^2 < (rm + s)^2 < g = qm^2n + qm, \]

it follows that \( snr < s^2 \leq qn, sr < q. \) Thus

\[ rm + s < q(r + s) < 2qr, \]

a contradiction. The proof is complete.

Lemma 5.6. Suppose that \( R \in Y_2 \) with \( R(1) = um - w. \) Then

\( u = w. \)

Proof. By Lemma 5.2, \( u \geq w; \) thus in order to prove the lemma it suffices to assume that \( u > w \) and to derive a contradiction based on this assumption. Let \( d_1 = (q, um - w), d_2 = (m, um - w), d_3 = (nm + 1, um - w). \)
Then \( um - w \mid d_1d_2d_3 \) and \( d_1 \mid u - w, \ d_2 \mid w, \ d_3 \mid wn + u \). Consequently, as \( u > w \), it follows that

\[
um - w \leq (uw^2 - w^3) n + (uw - w^2) u.
\]

(12)

Furthermore, Lemma 5.4 yields

\[
(uw^2 - w^3) n \leq (q - 1) u.
\]

(13)

A contradiction will be derived separately for the following two cases:

**Case I.** Suppose that \( u \leq nw \); then by (13) \( uw - w^2 \leq q - 1 \) and it follows from (12) and (13) that

\[
um - w \leq (q - 1) u + (q - 1) u = um - 3u,
\]
a contradiction.

**Case II.** Suppose that \( u > nw \). It follows from

\[
(u - 1)^2 m^2 < (um - w^2) < g = qnm^2 + qm
\]

and from \( u - 1 \geq nw \) that

\[
w(u - 1) \leq (u - 1)^2 \leq qn, \quad w(u - 1) \leq q.
\]

The last inequality and the assumption that \( u > nw \) allow us to rewrite (12) in the form

\[
um - w \leq w(u - 1) wn + w(u - 1) u < qu + qu = um - u,
\]
a contradiction. The proof is complete.

**Lemma 5.7.**

\[
x = fq,
\]

\[
q = T_1n + T_1 + 1,
\]

and \( Q \) is a Hall subgroup of \( G \).

**Proof.** By Lemma 5.2 \( x = am + fq, \ a \geq 0 \). In view of Lemmas 5.5 and 5.6, we have

\[
0 = \sum_X X(h_1) X(1)
\]

\[
= 1 + (fq + am)(-f) + T_1(nm + 1) - (T - T_1 - 1)(m - 1).
\]
Part (a) of Lemma 3.1 yields \( f^2q - T = (m - 2T)q - T = m(q - T) \).

It follows from these facts that

\[
q = T_1n + T_1 + 1 - af.
\]

(15)

It remains only to show that \( a = 0 \) and \( (q, nm + 1) = 1 \).

It follows from Lemmas 5.1, 5.5, and 5.6 that

\[
g \leq \frac{m^3(m - 3)(m - 1)}{2\{-2m + 2T + 2m - 2 + [2(m - 1)/(nm + 1)] T_1 - 2(T - T_1 - 1)\}}
\]

\[
= \frac{m^3(q - 1)q(nm + 1)}{m(1 + n) T_1}.
\]

Hence \( T_1(n + 1) \leq q - 1 \); since, by (15), \( q - 1 = T_1(n + 1) - af \), it follows that \( a = 0 \). Let \( b = (q, nm + 1) \); then \( b \mid (m - 1)n, b \mid nm + 1 \), hence \( b \mid n + 1 \). Since, by Eq. (14), \( n + 1 \mid q - 1 \), then \( b = 1 \). The proof is complete.

**Lemma 5.8.** (a) \( X_{i|N}, i = 1, 2, \) contain only \( \xi_1 \) and \( \xi_2 \) as their irreducible constituents. Consequently, \( X_i(e) = 0 \) for all \( e \in Q^# \), \( i = 1, 2 \).

(b) If \( R \in Y_2 \), then \( R_{i|N} \) contains only \( \xi_1 \) and \( \xi_2 \) as its irreducible constituents. Consequently, \( R(e) = 0 \) for all \( e \in Q^# \).

(c) If \( \xi \) is a nonprincipal irreducible character of \( N \) containing \( M \) in its kernel, then \( \xi^* \) is a sum of characters from \( Y_1 \). Consequently, if \( \xi \) is linear then \( \xi^* \in Y_1 \).

(d) \( D_i(e) = v_i \) for all \( e \in Q^# , i = 1, \ldots \). Furthermore, \( z = \sum v_i^2 = n \) and \( \sum \xi_i = 1_\mathbb{G} + \sum v_i D_i \).

(e) If \( P \in Y_1, P(1) = r(nm + 1), \) then

\[
\sum_{e} P(e) = -r(n + 1).
\]

**Proof.** (a) \( (X_{i|N}, \xi_{i1} + \xi_{i2})_N = (\frac{1}{qm}) (f_2q + q) = f \). Since \( x = fg \), the assertions follow.

(b) Let \( R(1) = u(m - 1) \). Then:

\[
(R_{i|N}, \xi_{i1} + \xi_{i2})_N = \frac{1}{qm} [u(m - 1) 2q + (m - 1) u] - 2u.
\]

Since \( R(1) = u(m - 1) \), the assertions follow.

(c) Let \( \xi(1) = d \); then \( \xi^*(1) = d(nm + 1) \) and \( \xi^*(h) = d \). Since by (a) and (b) \( \xi^* \) contains elements of \( Y_1 \) and \( Y_2 \) only, as its irreducible constituents,
it is easy to check (inspecting the values taken on $M^*$ by the various characters) that $\xi^*$ contains no elements of $Y_3$. The assertions follow.

(d) \((D_{i_N}, \xi_1 + \xi_N) = (1/\eta m) v_1 m z = 2v_1\). Hence, in view of (c), \(D_{iN}\) contains \(1_N v_1 - (m - 1) v_1 = v_1\) times, and no other character of $N$ nonvanishing on $Q^*$. Therefore \(D_i(e) = v_1\) for all \(e \in Q^*\). Moreover, it follows by the Frobenius Reciprocity Theorem that \(1_N^* = 1_g + \sum_i v_i D_i\). Consequently, \(1 + nm = 1 + \sum_i v_i^* m, z = n\).

(e) As \(P(1) = r(n^2 + 1)\) and \(1_N^*(1) = nm + 1, (P, 1_N^*)_G = 0\); hence also \((P, 1_N^*)_N = 0\) and \(0 = (1/\eta m) [r(nm + 1) + (m - 1) r + m \sum_i P(e)]\), \(\sum_i P(e) = - r(n + 1)\).

**Lemma 5.9.** The following table of characters and relations hold true:

<table>
<thead>
<tr>
<th></th>
<th>$h_1$</th>
<th>$h_2$</th>
<th>$e$</th>
<th>$o$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1_G$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$X_1$</td>
<td>$f(q)$</td>
<td>$\xi_1(h_1) + c$</td>
<td>$\xi_2(h_2) + c$</td>
<td>0</td>
</tr>
<tr>
<td>$X_2$</td>
<td>$f(q)$</td>
<td>$\xi_2(h_1) + c$</td>
<td>$\xi_2(h_2) + c$</td>
<td>0</td>
</tr>
<tr>
<td>$P_i$</td>
<td>$r_i(nm + 1)$</td>
<td>$r_i$</td>
<td>$P_i(e)$</td>
<td>$P_i(o)$</td>
</tr>
<tr>
<td>$R_i$</td>
<td>$u_i(m - 1)$</td>
<td>$-u_i$</td>
<td>$-u_i$</td>
<td>0</td>
</tr>
<tr>
<td>$D_i$</td>
<td>$v_i m$</td>
<td>0</td>
<td>$v_i$</td>
<td>$D_i(o)$</td>
</tr>
</tbody>
</table>

\[\sum_i P_i(e) P_i(o) = \sum_i r_i P_i(o) = 0,\] (16)

\[\sum_i r_i P_i(e) = \sum_i v_i D_i(o) = -1,\] (17)

where $e$ represents elements belonging to some conjugate of $Q^*$, and $o$ represents elements not included in the first four sets. (The set of all elements of the last kind will be denoted by $O$).

**Proof.** The table of characters summarizes the results of Lemmas 5.5-5.8. In order to prove (16) and (17) several orthogonal relations will be used:

\[0 = \sum_X \langle X(h_1) X(e) = 1 + \sum_i r_i P_i(e),\]

\[0 = \sum_X \langle X(o) X(1) + (m - 1) X(o) X(h_1)\]

\[= m + m(n + 1) \sum_i r_i P_i(o) + m \sum_i v_i D_i(o),\]

\[0 = \sum_X \langle X(e) X(o) = 1 + \sum_i P_i(e) P_i(o) + \sum_i v_i D_i(o).\]
It follows from the last two equations that
\[ \sum_i P_i(e)P_i(o) = (n + 1) \sum_i r_iP_i(o); \]
summation over \( e \in Q^\# \) yields, in view of Lemma 5.8 (e),
\[ -(n + 1) \sum_i r_iP_i(o) = (q - 1)(n + 1) \sum_i r_iP_i(o). \]
Hence \( \sum_i r_iP_i(o) \to 0 \) and (16), (17) follow from the above orthogonal relations.

**Lemma 5.10.** Let \( e \in Q^\# \) and \( u \) be an involution of \( G \). Then
\[ n(e) \mid q, \quad n(u) \mid nm + 1. \]

**Proof.** Let \( h \in M^\# \) and \( o \in O \). By Lemma 5.9 and the well known formula for \( c_{o,h} \) we get \( c_{o,h} = \frac{g}{n(o) n(e)} \). Since \( c_{o,h} \) is an integer and \( m \) is prime to \( n(e) n(o) \), it follows that
\[ n(o) n(e) \mid q(nm + 1). \]
As \( q \) is prime to \( nm + 1 \) and the divisibility condition holds for every \( e \in Q^\# \) and \( o \in O \), it follows from the fact that the center of a Sylow group is non-trivial that
\[ n(e) \mid q, \quad n(o) \mid nm + 1. \]
In particular, \( n(u) \mid nm + 1. \)

**Lemma 5.11.** Let \( u \) be an involution of \( G \). Then
\[ P_i(u) = 0 \quad \text{for all} \quad P_i \in Y_1 \]
and
\[ n(u) = m + \sum_i D_i^u(u). \]

**Proof.** It is well known that \( 2 \notn \mid N_G(M) \) implies that \( c_{u,h} = 0 \) for all \( h \in M^\# \). Hence
\[ 0 = 1 - \frac{fX_1^u(u)}{f_q} + \frac{1}{nm + 1} \sum_i P_i^u(u) - \frac{1}{m - 1} \sum_i R_i^u(u) \]
and
\[ 0 = 2q - 2X_1^u(u) + \frac{m - 1}{nm + 1} \sum_i P_i^u(u) - \sum_i R_i^u(u). \] (18)
As $X_1(u)$ and $R_i(u)$ are integers and $(q, nm + 1) = 1$, it follows that:

$$nm + 1 \mid 2 \sum_i P_i^2(u).$$

Since $n(u) \leq nm + 1$, $\sum_i P_i^2(u) < nm + 1$. Hence either

$$\sum_i P_i^2(u) = \frac{1}{2} (nm + 1) \quad \text{or} \quad \sum_i P_i^2(u) = 0.$$

We will show that the first case is impossible, thus proving the first result of this lemma.

If $\sum_i P_i^2(u) = \frac{1}{2} (nm + 1)$, then $n(u) = nm + 1$ and by (18) we get

$$nm + 1 = 1 + 2X_1^2(u) + \sum_i P_i^2(u) + \sum_i R_i^2(u) + \sum_i D_i^2(u)$$

$$= 1 + 2X_1^2(u) + \frac{1}{2} (nm + 1) + 2q - 2X_1^2(u)$$

$$+ \frac{1}{2} (m - 1) + \sum_i D_i^2(u)$$

$$\sum_i D_i^2(u) = \frac{1}{2} (nm - 3m + 2).$$

It follows, using Lemma 5.8 (e) and Lemma 5.9, that

$$\sum_e c_{ue} = g[q - 1 - \frac{1}{2} (n + 1) + (q - 1) (nm - 3m + 2)/2m](nm + 1)$$

$$= \frac{1}{2} \left[ q^2(nm + 1) + q^2(1 - m) - 2q(nm + 1) \right] (nm + 1).$$

Hence $nm + 1$ divides $2q^3$, a contradiction. Therefore $P_i(u) = 0$ for all $P_i \in Y_1$. The formula for $n(u)$ follows immediately from (18).

**Lemma 5.12.** Let $e \in Q^*$ and $u$ be an involution of $G$. Then

$$n(e) = q, \quad n(u) = nm + 1,$$

and $e$ is a real element in $G$.

**Proof.** By Lemma 5.10, $n(e)$ is an odd integer. Furthermore, it follows from Lemmas 5.9, 5.10, and 5.11 that

$$c_{ue} = \frac{g}{n^2(u)} \left[ 1 + \frac{1}{m} \sum_i D_i^2(u) \right] = \frac{g}{mn(u)}. \quad (19)$$

Hence $e$ can be represented as a product of two involutions and therefore $e$
is a real element in $G$. Under these conditions, Lemma (4A) of [2] implies that $c_{\text{use}} = n(e)$. It follows by (19) that

$$g = mn(e)n(u).$$

As $n(e) \leq q$ and $n(u) \leq nm + 1$, we must have

$$n(e) = q \quad \text{and} \quad n(u) = nm + 1.$$

**Lemma 5.13.** $Q$ is a CCT-subgroup of $G$.

**Proof.** Being simple, $G$ is of even order. Let $e \in Q$; since $e$ is a real element in $G$ with a centralizer of odd order, there exists an involution $u$ in the normalizer of $C_G(e)$ in $G$ (see [2], pp. 566-7). Since $(n(e), n(u)) = 1$, $u$ leaves no non-unit element of $C_G(e)$ invariant, and consequently $C_G(e)$ is Abelian. Since $C_G(e)$ is also a Hall subgroup of $G$, it follows from [7] that $Q$ is conjugate to $C_G(e)$, and hence Abelian. Lemma 5.12 then implies that $Q = C_G(e)$ for all $e \in Q$, and by Theorem 2.1, $Q$ is a CCT-subgroup of $G$.

**Lemma 5.14.** $g = qm(m + 1)$.

**Proof.** Lemma 5.13 implies that

$$g = qm(nm + 1) = wq(yq + 1), \quad w \mid q - 1.$$

Therefore $m(nm + 1) = wq(yq + 1)$, and, modulo $q$, $n \mid 1 = w$. Since both sides are positive and less than $q$, it follows that $w = n + 1$. Hence

$$2nm + 2(n + 1) = (n + 1)y, \quad n + 1 \mid 2m = 4q + 2.$$

But since $n + 1 = w \mid 4q - 4$ it follows that $n + 1 \mid 6$. As $n$ is odd, either $n + 1 = 2$ or $n + 1 = 6$. If $n + 1 = 6$, the 3-Sylow subgroup of $N_G(Q)$ is its own normalizer in $N_G(Q)$ and the Sylow Theorem implies that $3 \mid 2q - 1$, a contradiction. Hence $n + 1 = 2$, $n = 1$, and the proof is complete.

**Proof of Proposition 5.1 (continued).** To prove Proposition 5.1 it suffices to show that $G$ can be represented as a doubly transitive permutation group on $m + 1$ letters, in which no nontrivial permutation leaves three letters fixed. This follows from the fact that $q = \frac{1}{2}(m - 1)$ and from the results of Zassenhaus ([8], pp. 37-38).

We will represent $G$ as a permutation group on the $m + 1$ cosets of $N(M) = N$ in $G$. For $x \in G$, let $P(x)$ be the permutation sending $Ny$ onto $Nyx$, and let $P = \{P(x) \mid x \in G\}$. Obviously $N = \{x \mid x \in G, Nx = N\}$. Furthermore, $N$ acts transitively on the remaining $m$ cosets, because if $Nx \neq N$ and $h_1, h_2 \in M, h_1 \neq h_2$, then also $Nhx_1 \neq Nhx_2$ since otherwise $xhx_1^{-1}x^{-1} \in N$, hence $x \in N$, in contradiction to our assumption that $Nx \neq N$. 
Let $P_1$ be equal to $P$ restricted to $N$, acting on the $m$ cosets of $N$ different from $N$. $P_1$ is a transitive group of permutations on $m$ letters, and being a Frobenius group no non-unit element of $P_1$ leaves two letters fixed. Thus $P$ is a doubly transitive permutation group on $m+1$ letters in which no nontrivial permutation leaves three letters fixed. The proposition follows.

ACKNOWLEDGMENTS

Since a portion of this paper constituted part of my doctoral dissertation at Cornell University in 1965, I wish to express my thanks to Professor Walter Feit under whom it was written; I also wish to thank Professor James B. Ax for being so kind to serve as the chairman of my special committee. An earlier version of part of this paper was presented to the American Mathematical Society on September 3, 1965, under the title “On finite groups with a CCT-subgroup.”

REFERENCES