Some linear actions of finite groups with $q'$-orbits

Carlo Casolo

(Communicated by F. de Giovanni)

Abstract. Let $G$ be a finite group acting faithfully on a finite vector space $M$ in such a way that the centralizer of every element of $M$ contains a Sylow $q$-subgroup of $G$ as a central subgroup (for a fixed prime divisor $q$ of $|G|$ with $(q, |M|) = 1$). Then $G$ is isomorphic to a subgroup of the semi-linear group on $M$.

1 Introduction

Let $G$ be a finite group acting faithfully on a module $M$ over a finite field, and let $q$ be a prime divisor of the order of $G$. An orbit condition of relevance in the representation theory of finite soluble groups (e.g. see the book [9]) is that the length of every $G$-orbit on $M$ is not divisible by $q$, or in other words that the centralizer in $G$ of every element of $M$ contains a Sylow $q$-subgroup of $G$. When $G$ is soluble, this situation is rather well understood, and it is described in detail by Manz and Wolf in [9, §§9, 10]: if the action of $G$ on $M$ is primitive or $q \geq 5$, then, apart from two exceptions, $G$ is a subgroup of the semi-linear group $\Gamma(M)$. On the other hand, if $G$ is not soluble many more cases occur in principle. Consider for example the general linear group $G = \text{GL}(n, p)$ acting on its natural module $M$: the centralizer in $G$ of any non-trivial element of $M$ has index $p^n - 1$ in $G$, and thus contains a Sylow $q$-subgroup of $G$ for every prime $q$ such that $(q, p - 1) = 1$ and $q$ divides $p^k - 1$ for $2 \leq k \leq n$ and $(k, n) = 1$.

One way to make the problem more amenable for arbitrary finite groups is to impose further conditions on the embedding of a Sylow $q$-subgroup in the centralizers of non-trivial elements of the module. We fix the following notation.

Definition. Let $G$ be a finite group acting on a module $M$ over a finite field, and $q$ a prime divisor of the order of $G$. We write that

the pair $(G, M)$ satisfies $\mathcal{N}_q$ if for every $v \in M \setminus \{0\}$, $C_G(v)$ contains a Sylow $q$-subgroup of $G$ as a normal subgroup;

the pair $(G, M)$ satisfies $\mathcal{C}_q$ if for every $v \in M \setminus \{0\}$, $C_G(v)$ contains a Sylow $q$-subgroup of $G$ as a central subgroup.
Condition $N_q$ has been recently considered by Zhang [12], by Lewis and White [8], and by Palfy [10], in connection with questions about the set of character degrees of finite groups. The description of the pairs $(G, M)$ satisfying $N_q$ when $G$ is soluble (Corollary 10, see also [10]) is a fairly easy application of the aforementioned results of Manz and Wolf. For arbitrary groups, in this paper we just make a few preliminary remarks concerning $N_q$. The situation is much better when $\mathcal{C}_q$ is assumed: in this case we provide a complete description when $q$ is coprime to $|M|$.

**Main Theorem.** Let the pair $(G, M)$ satisfy $\mathcal{C}_q$, with $q$ coprime to the order of $M$. Then $G/C_G(M)$ is a $q$-nilpotent irreducible subgroup of the semi-linear group $\Gamma(M)$.

The same conclusion need not hold if $q$ coincides with the characteristic of the ground field of $M$, as shown for instance by the group $\text{SL}(2, q)$ acting on its natural module. We leave this case for further investigation. As in [8] and [12], where the property $N_q$ was introduced, motivation comes from its relevance to questions regarding conjugacy class sizes and degrees of irreducible characters. Our Main Theorem is used as a central tool in [3], in order to describe finite groups $G$ in which no conjugacy class size is divisible by the product of two fixed prime divisors of the order of $G$.

In the course of the proof we will apply an independent result, which also concerns actions with large centralizers.

**Theorem 1.** Let $G$ be a finite group and $\alpha$ an automorphism of $G$ such that $(|G|, |\alpha|) = 1$ and 2 does not divide $|\alpha|$. Suppose that $|P, \alpha|$ is cyclic for every $\alpha$-invariant Sylow subgroup $P$ of $G$ (for any prime divisor of $|G|$). Then $[G, \alpha]$ is cyclic.

Our proofs are independent of the classification of finite simple groups, but for Theorem 1 we use Bender’s classification of groups with a strongly embedded subgroup. All groups considered in this paper are finite.

## 2 Preliminaries

In this section we recall some known results that will be repeatedly used and we prove a technical lemma needed later in the paper.

**Lemma 2** (see [5, (15.16)]). Let $G = KH$ be a Frobenius group, with kernel $K$ and complement $H$. Let $F$ be a field whose characteristic does not divide $|K|$, and $M$ an $FG$-module such that $C_M(K) = 0$. If $T \leq H$, then

$$\dim C_M(T) = |H : T| \dim C_M(H).$$

In particular, $\dim M = |H| \dim C_M(H)$.

**Lemma 3** (quadratic action, see [7, p. 226]). Let $\alpha$ be an involution acting on the elementary abelian 2-group $M$. Then $|C_M(\alpha)| \geq \sqrt{|M|}$. 

Unauthenticated
Download Date | 7/11/19 3:10 AM
Let $M = \text{GF}(r^m)$ be a finite field (with $r$ prime). Following [9], we denote by $\Gamma(M)$ the semi-linear group on $M$, which consists of all transformations of $M$ of the form $x \mapsto ax^\sigma$, where $a \in M \setminus \{0\}$ and $\sigma$ is an element of the Galois group $\text{Gal}(M, \text{GF}(r))$ of $M$ over $\text{GF}(r)$. For a detailed description of semi-linear groups, we refer to [9]; here, we just mention that $\Gamma(M)$ has a normal cyclic subgroup $\Gamma_0(M)$ isomorphic to the multiplicative group of $M$, with elements the maps $x \mapsto ax$ for $a \in M \setminus \{0\}$, and that $\Gamma(M)/\Gamma_0(M)$ is isomorphic to $\text{Gal}(M, \text{GF}(r))$ (hence it is cyclic). Let the group $G$ act faithfully on a $\text{GF}(r)$-module $M$; we say that $G$ embeds in $\Gamma(M)$ (and write $G \leq \Gamma(M)$) if there is a labelling of the elements of $M$ as $\text{GF}(r^m)$ such that $G$ becomes a subgroup of $\Gamma(M)$. In this sense, we will also often write $\Gamma(r^m)$ for $\Gamma(\text{GF}(r^m))$.

**Lemma 4** ([9, Theorem 2.1 and Corollary 2.3]). Let the group $G$ act faithfully on a finite vector space $V$ and let $A$ be a normal abelian subgroup of $G$.

1. If $A$ is irreducible on $V$, then $G$ may be identified with a subgroup of $\Gamma(V)$ (with $A$ a subgroup of $\Gamma_0(V)$).

2. If $G$ is soluble, $A = \text{Fit}(G)$, and $A$ is homogeneous on $V$, then $G \leq \Gamma(V)$.

We recall that for $a, n \in \mathbb{N}$ and $a, n > 1$, a primitive divisor of $a^n - 1$ is a prime that divides $a^n - 1$ but divides no $a^k - 1$ with $1 \leq k \leq n - 1$. The existence of primitive divisors in most cases is assured by a famous and much applied theorem of Zsigmondy.

**Lemma 5.** Let $a, n \in \mathbb{N}$ and $a, n > 1$. Then $a^n - 1$ has a primitive divisor except in the following cases:

(i) $a = 2^k - 1$ and $n = 2$;

(ii) $a = 2$ and $n = 6$.

The following lemma is certainly known; we provide a proof for the convenience of the reader.

**Lemma 6.** Let $r$ be a prime, $2 \leq m \in \mathbb{N}$, and $t$ a primitive divisor of $r^m - 1$ (if one exists). Let $T$ be a subgroup of order $t$ of $\text{GL}(m, r)$, and suppose that $T$ normalizes a non-trivial $p$-subgroup $P$ of $\text{GL}(m, r)$, with $p$ an odd prime. Then $T$ centralizes $P$ and $P$ is cyclic.

**Proof.** We let $V$ be the natural vector space acted on by $\text{GL}(m, r)$, and we argue by induction on $|P|$. Observe that, as $t$ is a primitive divisor of $r^m - 1$, $m$ divides $t - 1$. Recall also that in $\text{GL}(m, r)$ the centralizer of an element of order $t$ is cyclic of order $r^m - 1$. Thus it will be enough to show that $[P, T] = 1$; moreover, as the Sylow $t$-subgroups of $\text{GL}(m, r)$ are cyclic, we may assume that $p \neq t$. Let $H = \Omega_1(C)$, where $C$ is a critical subgroup of $P$ (see [1, §§23, 24]). If $T$ centralizes $H$ then $T$ centralizes $P$; thus we may assume that $H = P$. Let $A = Z(P)$; then $A \supseteq \phi(P)$ and $AT$ is
irreducible on \( V \), as \( t \) is a primitive divisor of \( r^m - 1 \). If the restriction of \( V \) to \( A \) were not homogeneous, then it would have \( t \) homogeneous components, and this would imply that \( \text{dim } V \geq t > m \), a contradiction. Thus \( V|_A \) is homogeneous, and so \( A \) is cyclic. If \( [A, T] \neq 1 \), then \( A \) is the Fitting subgroup of \( AT \), and so by Lemma 4 (2), the group \( AT \) embeds in \( \Gamma(V) \), and in particular \( t|m \), which is a contradiction. Therefore \( [A, T] = 1 \). Thus we assume that \( P \neq A \), which implies that \( P \) is extraspecial and \( T \) centralizes \( Z(P) \). Let \( |P : Z(P)| = p^{2n} \); then \( p^n|m \) by [9, Corollary 2.6]. It follows that \( t - 1 \geq p^n \). But, by the inductive assumption, and coprime action of \( T \) on \( P/\phi(P) \), \( P/\phi(P) \) is irreducible for \( T \), whence \( t | p^n + 1 \). We thus have \( t \leq p^n + 1 \leq t \), and this forces \( t = p^n + 1 \), which is a contradiction because \( t \) is prime and \( p \) is odd. \( \square \)

For the statement of the announced technical lemma, let us fix the following notation. Let \( p \) be a prime, and \( \alpha \) an automorphism of the \( p \)-group \( P \); we set

\[
N^\alpha_1(P) = \{ X \leq P \mid [X, \alpha] = X, |X| = p \}.
\]

**Lemma 7.** Let \( p, q \) be distinct primes, with \( p \geq 5 \) and \( q | p - 1 \). Let \( \alpha \) be an automorphism of order \( q \) of the \( p \)-group \( P \). If \( |N^\alpha_1(P)| \leq 1 \), then \( [P, \alpha] \) is cyclic.

**Proof.** Firstly, since \( q | p - 1 \) and \( \alpha \neq 1 \), it is easy to see that \( N^\alpha_1(P) \neq \emptyset \). Thus \( |N^\alpha_1(P)| = 1 \). We proceed by induction on \( |P| \). Since \( q | p - 1 \) the center \( Z(P) \) of \( P \) has an \( \alpha \)-invariant subgroup \( X \) of with \( |X| = p \).

Suppose that \( [X, \alpha] = 1 \). Then \( \alpha \) is not trivial on \( P/X \), and so there exists \( U/X \in N^\alpha_1(P/X) \). Now \( U \) is abelian (of order \( p^2 \)), and \( U/X = [U, \alpha]X/X \); thus \( U = [U, \alpha] \times X \), and so \([U, \alpha] \) is the (unique) element of \( N^\alpha_1(P) \), and this shows that \( |N^\alpha_1(P/X)| = 1 \). Therefore, by the inductive assumption, \( [P, \alpha]X/X = [P/X, \alpha] \) is cyclic. Hence \( P_1 = [P, \alpha]X \) is abelian and so \( [P, \alpha] = [P, \alpha, X] = [P_1, \alpha] \) is cyclic.

Now suppose that \( [X, \alpha] = X \), i.e. \( N^\alpha_1(P) = \{ X \} \). Assume by contradiction that \( |N^\alpha_1(P/X)| \geq 2 \), and let \( U/X, V/X \) be distinct elements of \( N^\alpha_1(P/X) \). Then \( U, V \) are abelian, \([U, \alpha] = U \) and \([V, \alpha] = V \). Since \( q | p - 1 \) and \( N^\alpha_1(P) = \{ X \} \) it follows that \( U \) and \( V \) are both cyclic of order \( p^2 \). Choose \( u, v \) with \( U = \langle u \rangle \) and \( V = \langle v \rangle \), and with \( u^\alpha = v^\alpha \). By the inductive assumption (as \( U \) and \( V \) are \( \alpha \)-invariant), we may assume that \( P = \langle u, v \rangle \). Then \( X \leq \phi(P) \), \( P = \phi(P) \) has order \( p^2 \), and \( P = [P, \alpha] \). In particular

\[
C_{\phi(P)}(\alpha) = 1.
\]

Let \( A = \phi(P)U, B = \phi(P)V \). These are proper \( \alpha \)-invariant subgroups, and so, by the inductive assumption, \([A, \alpha] \) and \([B, \alpha] \) are cyclic. In particular

\[
U = [U, \alpha] \char[A, \alpha] \leq A,
\]
whence $U \leq A$. Since $U \cap \phi(P) = X$, we get $[U, \phi(P)] \leq X$. Similarly, $[V, \phi(P)] \leq X$. Hence $[P, \phi(P)] \leq X$, and thus $P$ has nilpotency class at most 3. Since $p \geq 5$, $P$ is regular (see [4, (10.2)]), and therefore (by [4, (10.5)])

$$(uv^{-1})^p = u^p(v^p)^{-1} = 1,$$

that is, $1 \neq uv^{-1} \in \Omega_1(P)$. Since, by regularity, $\Omega_1(P)$ has exponent $p$, $\Omega_1(P)$ is a proper subgroup of $P$ and, by the inductive assumption, $[\Omega_1(P), x]$ is cyclic of order $p$, forcing $[\Omega_1(P), x] = X \leq \phi(P)$. Hence, if $R = \Omega_1(P)\phi(P)$, then $[R, x] \leq \phi(P)$. By what we have observed above, this yields $\Omega_1(P) \leq R \leq \phi(P)$. In particular we get the contradiction $uv^{-1} \in \phi(P)$.

Hence $|N_2^3(P/X)| = 1$, and by the inductive assumption, $[P/X, x] = [P, x]X/X$ is cyclic. The argument used before now shows that $[P, x]$ is cyclic. □

Remarks. (1) Lemma 6 does not hold for $p = 2$. Let $r$ be a prime such that $r^2 \equiv -1 \pmod 5$. Then $t = 5$ is a primitive divisor of $r^4 - 1$, while the group $\text{GL}(4, r)$ admits non-nilpotent subgroups which are the extension of an extraspecial group $P$ of order $2^5$ by a cyclic group $T$ of order 5 (see [11, §2.4]). Examples can be found for $m = 2$ by taking $r \equiv -1 \pmod 3$, $t = 3$, and recalling that $\text{GL}(2, r)$ has subgroups isomorphic to $\text{SL}(2, 3)$.

(2) Lemma 7 does not hold for $p = 3$ (and $q = 2$). For instance, let

$$P = \langle a, b \mid a^9 = b^9 = [a, b]^3 = 1, a^3 = b^{-3}, [a, b, a] = a^3, [a, b, b] = b^3 \rangle.$$

Then $|P| = 81$, and $P$ has an automorphism $x$ of order 2 such that $a^2 = a^{-1}$ and $b^x = b^{-1}$. Also, one checks that $\Omega_1(P) = \langle [a, b], a^3 \rangle$ is elementary abelian of order 9. Since $[a, b]^3 = [a, b]$ and $(a^3)^x = (a^3)^{-1}$, it follows that $\langle a^3 \rangle$ is the only element in $N_2^3(P)$. On the other hand, $[P, x]$ contains $[a, x] = a^{-2}$ and $[b, x] = b^{-2}$, and so $[P, x] = P$.

3 The condition $\mathcal{N}_q$

We begin by recollecting some known easy basic facts.

Proposition 8. Let $F$ be a finite field, $G$ a finite group, and $M$ an FG-module such that $(G, M)$ satisfies $\mathcal{N}_q$. Let $Q$ be a Sylow $q$-subgroup of $G$. Then the following assertions hold:

(1) $M$ is irreducible as an FG-module;

(2) if $q = 2$ then $\text{char}(F) = 2$;

(3) $|G : N_G(Q)| = (|M| - 1)/(|C_M(Q)| - 1);$

(4) if $N \leq G$ and $q$ divides $|N/C_N(M)|$, then $(N, M)$ satisfies $\mathcal{N}_q$. 
Proof. (1) This is part of [12, Lemma 4].
(2) See, for instance [9, Lemma 9.2].
(3) This follows from the fact that the centralizers of the Sylow \(q\)-subgroups of \(G\) form a partition of the set \(M\setminus\{1\}\).
(4) This is easy. □

We now treat soluble groups. The main result in this case essentially appears in a paper of Palfy ([10, Main Lemma]), although with a slightly different hypothesis. We include a proof for completeness.

Proposition 9. Let \(G, M\) satisfy \(\mathcal{N}_q\), and assume that \(G\) is soluble and faithful on \(M\), with \(G = O^q\Gamma(G)\). Then one of the following holds:

1. \(O^q\Gamma(G)\) is a cyclic \(q\)-group, and \(G \leq \Gamma(M)\);
2. \(G = \text{SL}(2, 3), q = 3,\) and \(|M| = 3^2\).

Proof. Let \(Q\) be a Sylow \(q\)-subgroup of \(G\).

Assume first that \(G\) is not quasi-primitive on \(M\). We apply [9, Theorem 9.3] (with the same notation except that we write \(M\) instead of \(V\)); in particular we have \(q = 2, 3\).

Let \(q = 2\). Then \(G/C\) is isomorphic either to \(D_6\) or to \(D_{10}\), and so \(N_G(Q) \leq CQ = K\), where \(K\) is the normalizer of a homogeneous component \(V_1\) of \(M\) as a \(C\)-module. Also \(|M|\) is a power of 2 by Proposition 8(2). If \(|V_1| = 2^k\), then \(|M| = 2^{nk}\) where \(n = |G: K| = 3, 5\). Since \(M|_C\) is not irreducible 2 does not divide \(|C|\), by Proposition 8(1), (4); hence \(|Q| = 2\). If \(1 \neq v \in V_1\), then \(C_G(v) \leq K\), therefore \((K, V_1)\) satisfies \(\mathcal{N}_q\). In particular

\[
|C : C_G(Q)| = |K : N_K(Q)| = \frac{|V_1| - 1}{|C_{V_1}(Q)| - 1} = 2^{k/2} + 1
\]

as, by quadratic action, we must have \(|C_{V_1}(Q)| = \sqrt{|V_1|} = 2^{k/2}\). It follows that

\[
\frac{2^{nk} - 1}{|C_M(Q)| - 1} = |G : N_G(Q)| = n(2^{k/2} + 1).
\]

If \(n = 5\), then \(|C_M(Q)| = 2^{5k/2}\), and the above equality becomes

\[
2^{5k/2} + 1 = 5(2^{k/2} + 1),
\]

which has no integral even solutions \(k\). If \(n = 3\), then \(|C_M(Q)| = 2^{3k/2}\) and the equality becomes \(2^{3k/2} + 1 = 3(2^{k/2} + 1)\), which admits the solution \(k = 2\). Then \(|V_1| = 4\) and \(K/C_K(V_1) \simeq S_3\). It follows that \(|C : C_C(V_1)| = 3\) and \(C_C(V_1) = C_C(Q)\). By faithfulness on \(M\), \(C\) is therefore an elementary abelian 3-group. Let \(Y\) be a Sylow 3-subgroup of \(G\); then \(C \leq Y \leq G\), and \(G = YQ\). Since \(O^3(G) = G\) we have
\[ [Y, Q] = Y. \] Now
\[ |Y : C_Y(Q)| = |G : C_G(Q)| = 9; \]
hence if \( Y \) is not cyclic then \( \phi(Y) = C_Y(Q) \leq C_G(V_1); \) but \( \phi(Y) \leq G, \) and thus \( \phi(Y) = 1. \) But \( Y \) is irreducible on \( M \) and so it cannot be elementary abelian of order 9. Thus \( Y \) is cyclic of order 9, and by Lemma 4, \( G \leq \Gamma(M) \) (and so it is quasi-primitive).

Let \( q = 3. \) Then \( G/C \simeq A\Gamma(2^3), \) and \( N_{G/C}(QC/C) \) has order 6. Since \( C \) is not irreducible on \( M, \) 3 does not divide \( |C|. \) Let \( 1 \neq v \in V_1. \) If \( r^a = |V_1| \) (with \( r \) a prime), then \( |M| = r^{8a}, \) and \( |C : C_C(v)| = r^a - 1 \) by [9, Theorem 9.3]. Let \( Q \) be a Sylow 3-subgroup of \( G \) contained in \( C_G(v). \) Then \( C_C(v) \) normalizes \( Q, \) and so
\[ 28(r^a - 1) \geq |G : N_G(Q)| = \frac{r^{8a} - 1}{r^a - 1} \geq r^{4a} + 1 \]
where \( r^s = |C_M(Q)|. \) It follows that \( r^a(28 - r^{3a}) \geq 29, \) which in turn implies \( r^a = 2. \) But then \( C = 1, \) \( |M| = 2^8, \) \( |C_M(Q)| = 2^4, \) and finally we have the contradiction
\[ 17 = \frac{2^8 - 1}{2^4 - 1} = |G : N_G(Q)| = 28. \]

Thus \( G \) is quasi-primitive on \( M. \) Then [9, Theorem 10.4] gives us the desired conclusion, unless we have \( q = 2 = |Q|, K = O^q(G) \) extraspecial of order \( 3^3 \) and exponent 3, \( Z(G) = Z(K) \) and \( |M| = 2^6. \) But in this case there exist elements \( g \in K \setminus Z(K) \) such that \( C_M(g) \neq 1, \) and this is not compatible with condition \( \mathcal{N}_q, \) since \( N_G(Q) = Z(G)Q. \)

**Corollary 10.** Let \( G \) be soluble, and \((G, M)\) satisfy \( \mathcal{N}_q. \) Let \( K = C_G(M), \) and \( \bar{G} = G/K. \) Then
1. \( \bar{G} \leq \Gamma(M) \) and \( O^{q'-q}(\bar{G}) \) is a cyclic \( q'-\)group; or
2. \( q = 3, \bar{G} = SL(2, 3) \) or \( GL(2, 3), \) and \( |M| = 3^2. \)

**Proof.** This follows from the proof of [9, Theorem 10.5], bearing in mind that in our case \( O^{q'}(G) \) is quasi-primitive on \( M, \) and that case (iii) cannot occur. \( \square \)

Although we will use the next lemma under the stronger condition \( \mathcal{N}_q, \) we prove it for \( \mathcal{N}_q' \) as this is not much more difficult. In it we no longer assume that \( G \) is soluble.

**Lemma 11.** Let \((G, M)\) satisfy \( \mathcal{N}_q', \) with \( G \) faithful on \( M. \) Suppose that \( G \) is not \( GL(2, 3) \) acting on its natural module.
1. If \( O^{q'}(G) \) is \( q-\)nilpotent, then \( G \) is \( q-\)nilpotent.
2. If, furthermore, \( O^{q'}(G) \) embeds in \( \Gamma(M), \) then \( G \) embeds in \( \Gamma(M). \)
Proof. (1) Let $N = O^{q'}(G)$, and let $Q$ be a Sylow $q$-subgroup of $G$. By the Frattini argument, $G = NN_G(Q)$, and by Proposition 8,

$$|G : N_G(Q)| = |N : N_N(Q)| = \frac{r^m - 1}{r^s - 1},$$

where $r^m = |M|$ and $r^s = |C_M(Q)|$.

If $m = 2$ then $s = 1$, and $|G : N_G(Q)| = r + 1$, which forces $q = r$. Thus $G$ is an $r$-soluble subgroup of $GL(2, r)$, with $O_r(G) = 1$ (by condition $N_r$ and faithfulness), and so the only possible cases are $r = 2, 3$ (see [7, (8.6.12)]); furthermore, if $G$ is not $r$-nilpotent, then $r = 3$ and $G = GL(2, 3)$, which is excluded by assumption.

Let $r^m = 2^b$; then $s \in \{1, 2, 3\}$. If $q = 2$, then $G$ is soluble and we refer to Corollary 10. Thus let $q$ be odd. Since

$$k = \frac{2^b - 1}{2^s - 1} = 9, 21, 63 \equiv 1 \pmod{q},$$

the possible cases are $k = 21$, $q = 5$, or $k = 63$, $q = 31$. Since $G \leq GL(6, 2)$, in both cases $Q$ is cyclic. Let $Y = O_{q'}(G)$; then $G/Y \leq \text{Aut}(Q)$ since $G$ is $q$-soluble of $q$-length 1. In both cases, 7 does not divide $|G/Y|$, and so, if $T$ is a Sylow 7-subgroup of $G$, then $T \leq O_{q'}(G)$ (observe that $T \neq 1$ because $7|k$). By the Frattini argument, we may then assume that $T$ is normalized by $Q$. But $|T| \leq 7^2$, as a Sylow 7-subgroup of $GL(6, 2)$ has order $7^2$, and consequently neither 5 nor 31 divides $|\text{Aut}(T)|$. Therefore $Q$ centralizes $T$, and this is a contradiction since 7 divides $|G : N_G(Q)|$.

In all other cases there exists a primitive prime divisor $p$ of $r^m - 1$ (which therefore divides $|G : N_G(Q)|$). Let $P$ be a Sylow $p$-subgroup of $G$. Then $P$ is cyclic and contained in $K = O^q(N)$. By the Frattini argument, $G = KN_G(P)$, and thus we may assume that $Q \leq N_G(P) \cap N = N_N(P)$. Hence

$$N_G(P) = (N_G(P) \cap N)N_{N_G(P)}(Q) \quad \text{and} \quad G = NN_{N_G(P)}(Q).$$

Let $X = N_{N_G(P)}(Q)$. Since $N_G(P)/C_G(P)$ is abelian, we have

$$[Q, X] \leq N_G(P) \cap Q \leq C_G(P) \cap Q = C_Q(P).$$

Also, $N_G(Q) = NX \cap N_G(Q) = X(N \cap N_G(Q)) = XC_N(Q)$. Since $P$ does not normalize $Q$ we get

$$[N_G(Q), Q] = [X, Q] \leq C_Q(P).$$

Now $P$ is irreducible on $M$, and $C_M(C_Q(P))$ is $P$-invariant and non-trivial; therefore $C_M(C_Q(P)) = M$ and, by faithfulness, $C_Q(P) = 1$. Thus $[N_G(Q), Q] = 1$ and so, by Burnside’s criterion, $G$ is $q$-nilpotent.
Suppose further that $N = O^q(G) \subseteq \Gamma(M)$. Assume first that $r^m - 1$ has a primitive prime divisor $p$, and let $P$ be a Sylow $p$-subgroup of $G$. Then $P \leq N$, and so $P \unlhd N$ (in fact $P \leq \Gamma_0(M)$). Thus $P$ is an abelian normal subgroup of $G$ that is irreducible on $M$, and, by Lemma 4, $G$ is embedded in $\Gamma(M)$. Assume then that $r^m - 1$ has no primitive prime divisors. By the proof of (1) we may thus suppose that $r^m = 2^6$ and $q = 2$. In this case $N \leq \Gamma(2^6)$, and so $N = O^2(N)Q$ with $|Q| = 2$. It follows that $r^1 = |C_M(Q)| = 2^3$ and $|G : NG(Q)| = 9$. Thus, if $K$ is a Sylow $3$-subgroup of $N \cap \Gamma_0(2^6)$, then $|K| = 9$, $K \unlhd G$ and $K$ is irreducible on $M$. Again by Lemma 4, we conclude that $G \leq \Gamma(M)$. □

4 The case $G = \text{SL}(2, p^k)$

At one stage of the proof of the Main Theorem we need to discuss separately the case in which the Sylow 2-subgroups of $G$ are dihedral or quaternion groups. In this case either $G$ is soluble or it has a normal section isomorphic to $\text{SL}(2, p)$, $\text{PSL}(2, p)$ or $A_7$. This motivates the following preliminary discussion of the case of $\text{SL}(2, p)$, for which the occurrence of condition $N_q$ may be completely described.

Lemma 12. Let $r$, $p$ be prime numbers such that, for some positive integers $a$, $b$,

$$\frac{r^a - 1}{r^b - 1} = \frac{p(p + 1)}{2}.$$

Then one of the following holds:

(i) $a$ is the order of $r$ modulo $p$;

(ii) $r = 3$, $b = 2$, $a = 2k$, and $p = \frac{1}{2} (3^k - 1)$;

(iii) $r = p = a = 2$, and $b = 1$.

Proof. If $p = 2$ it is immediately seen that case (iii) occurs. Thus let $p \neq 2$, and let $k = \zeta_p(r)$ be the order of $r$ modulo $p$ (then $k | a$).

Assume that $k \neq a$; hence $a = ku$, with $u \geq 2$. Let $d = (b, k)$ (the greatest common divisor), and $b = dw$ (with $1 \leq w \in \mathbb{N}$). We have

$$\frac{p(p + 1)}{2} = \frac{(r^k - 1)(r^{k(u-1)} + \cdots + r^k + 1)}{(r^d - 1)(r^{d(w-1)} + \cdots + r^d + 1)}. \quad (1)$$

First suppose that $d = k$. Then $p$ divides $r^{k(u-1)} + \cdots + r^k + 1$. Since, by definition, $r^k \equiv 1 \pmod{p}$, we have

$$u \equiv r^{k(u-1)} + \cdots + r^k + 1 \equiv 0 \pmod{p}$$
whence, in particular, \(u \geq p\). From this, by considering separately the cases when \(p \mid b\) and \(p \not\mid b\), one gets

\[
\frac{p(p + 1)}{2} = \frac{r^a - 1}{r^b - 1} \geq r^p + 1, 
\]

which is not possible as \(r \geq 2\) and \(p \geq 3\).

Now suppose that \(d < k\). Then \(p\) divides \((r^k - 1)/(r^d - 1)\), and it follows from (1) that

\[
\frac{p + 1}{2} \geq \frac{r^{k(u-1)}}{r^{d(w-1)}} + \ldots + \frac{r^k}{r^d + 1}. 
\]

Consequently

\[
\frac{r^{k(u-1)}}{r^{dw}} \leq \frac{p + 1}{2} \leq \frac{1}{2} \left(\frac{r^k - 1}{r^d - 1} + 1\right) < r^k, 
\]

whence \(ku - k < k + dw\), which we rewrite as

\[
a < b + 2k. 
\]

Let \(u \geq 3\). Then \(2k = 2a/u \leq 2a/3\), and (2) becomes \(a < 3b\). Since \(b \mid a\), the only possibility is \(a = 2b\). Hence the initial assumption reduces to

\[
\frac{p(p + 1)}{2} = r^b + 1; 
\]

we write this in the form \(2r^b = (p - 1)(p + 2)\). Since \(p \neq 2\), the only possible cases that occur are when \(p = 3\), \(r^b = 5\) or \(p = 7\), \(r^b = 3^3\). In both cases \(a = 2b\) is the order of \(r\) modulo \(p\).

Now let \(u = 2\). Then \(a = 2k\), and so \(d = (b,k)\) is either \(b\) or \(b/2\).

Assume first that \(d = b/2\). Then, setting \(x = r^k\) and \(y = r^{b/2}\), formula (1) becomes

\[
\frac{p(p + 1)}{2} = \frac{(x - 1)(x + 1)}{(y - 1)(y + 1)}. 
\]

Therefore

\[
\frac{x + 1}{y + 1} \leq \frac{p + 1}{2} \leq \frac{1}{2} \left(\frac{x - 1}{y - 1} + 1\right). 
\]
thus yielding

\[(x - y)(y - 3) \leq 0.\]

Since \(y < x\), this forces \(y = 2, 3\). If \(y = 2\), then

\[
\frac{p(p + 1)}{2} = \frac{2^{2k} - 1}{2^2 - 1} = \frac{(2^k - 1)(2^k + 1)}{3}
\]

which is not possible for \(p\) a prime divisor of \(2^k - 1\). Thus \(y = r^{b/2} = 3\), whence \(r = 3, b = 2, k \) is odd, and

\[
\frac{p(p + 1)}{2} = \frac{3^{2k} - 1}{3^2 - 1} = \frac{(3^k - 1)(3^k + 1)}{8}.
\]

This may happen if \(p = \frac{1}{3}(3^k - 1)\) is a prime, and we are in case (ii).

Finally, let \(d = (b, k) = b\). Then \(b|k\) (and \(b < k\)), and from (1) we have

\[
\frac{p(p + 1)}{2} = \frac{r^k - 1}{r^b - 1}, (r^k + 1),
\]

and \(p\) divides \((r^k - 1)/(r^b - 1)\). This yields the contradiction

\[
\frac{p + 1}{2} \geq r^k + 1 > p
\]

and completes the proof. \(\Box\)

**Proposition 13.** Let \(G = \text{SL}(2, p^k)\) (with \(p\) an odd prime) act on the elementary abelian \(r\)-group \(M\), and suppose that \((G, M)\) satisfies \(N_q\) for some prime divisor \(q > 2\) of \(|G|\). Then \(G\) is faithful on \(M\), and one of the following holds:

(i) \(p = q = r\), and \(M\) is the natural module for \(G\);
(ii) \(G = \text{SL}(2, 5), q = 3, \) and \(|M| = 3^4\);
(iii) \(G = \text{SL}(2, 13), q = 3, \) and \(|M| = 3^6\).

Observe that, as we make no assumption of faithfulness, the proposition includes the case of \(\text{PSL}(2, p^k)\) as well.

**Proof.** If \(p^k = 3\) the claim is easily checked (it occurs as case (2) in Proposition 9). Thus, let \(p^k > 3\). Then \(G/Z(G)\) is simple, and so the kernel of the action of \(G\) on \(M\) is either \(\{1\}\) or \(Z(G)\). Let \(|M| = r^m\,\), and let \(P\) be a Sylow \(p\)-subgroup of \(G\).
Case 1. Suppose that there exists \( a \in P \setminus \{1\} \) such that \( C_M(a) \neq 1 \). Since, by the structure of \( \text{SL}(2, p^k) \), \( P \) is the only Sylow subgroup of \( G \) normalized by \( a \), it follows that \( q = p \). If \( |C_M(P)| = r^b \), then \( b|m \), and by Proposition 8(3), we have

\[
p^k + 1 = |G : N_G(P)| = \frac{r^m - 1}{r^b - 1} = r^{b(x-1)} + \cdots + r^b + 1
\]

(where \( m = bs \)). This forces \( r^b = p^k, m = 2k \), and from this it easily follows that \( M \) is the natural module for \( G \).

Assume now that \( P \) acts as a group of fixed-point free automorphisms on \( M \). Then \( r \neq p \), and, since \( P \) is elementary abelian, \( |P| = p \) (and so \( G = \text{SL}(2, p) \)).

Case 2. Suppose that \( p \) is not a Fermat prime. Then there exists an odd prime divisor \( t \) of \( p - 1 \), and a Sylow \( t \)-subgroup \( T \) of \( G \) contained in \( N_G(P) \). Now \( PT \) is a Frobenius group with kernel \( P \) acting on \( M \), and \( C_M(P) = 1 \). It follows from Lemma 2 that \( C_M(T) \neq 1 \), and so \( T \) normalizes a Sylow \( q \)-subgroup of \( G \). By the structure of the special linear group this implies that \( q \) is also an odd prime divisor of \( p - 1 \) (since \( q \neq p \)). Moreover, if \( Q \) is a Sylow \( q \)-subgroup of \( G \), then \( |N_G(Q)| = 2(p - 1) \); hence, if \( |C_M(Q)| = r^b \),

\[
\frac{r^m - 1}{r^b - 1} = |G : N_G(Q)| = \frac{p(p + 1)}{2}.
\]

By Lemma 12, since \( p \neq 2 \), we have two possibilities: either \( m \) is the order of \( r \) modulo \( p \), or \( b = 2, r = 3 \) and \( p = \frac{1}{2}(3^k - 1) \) for some \( k \geq 2 \).

Assume first that \( m \) is the order of \( r \) modulo \( p \). Then \( P \) acts irreducibly on \( M \). Let \( X = N_G(P) \); then \( |X/C_G(P)| = \frac{1}{2}(p - 1) \), and \( C_G(P) \) is abelian and irreducible on \( M \). By Lemma 4 we have \( X \leq \Gamma(M) \), and in particular \( \frac{1}{2}(p - 1) \) divides \( m \). As \( q \geq 3 \) we have \( |C_M(Q)| \leq r^m/3 \), and so it follows from (3) that

\[
\frac{p(p - 1)}{2} > \frac{r^m - 1}{r^m/3 - 1} > 2^{(2m/3)} > 2^{(p-1)/3}.
\]

As \( p \) is not a Fermat prime, this forces \( r = 2 \) and \( p = 7, 11, 13, 19, 23 \), or \( r = 3 \) and \( p = 7, 13 \). The case \( (r = 2, p = 7) \) is excluded immediately, while the case \( (r = 3, p = 13) \) is excluded because the order of 3 modulo 13 is 3. In all other cases, the order of \( r \) modulo \( p \) is \( p - 1 \), hence \( m = p - 1 \), and equation (3) cannot be satisfied.

Now let \( b = 2, r = 3, p = \frac{1}{2}(3^k - 1) \), and \( m = 2k \). Then, as 3 divides \( \frac{1}{2}(p - 1) \), there exists an element \( g \) of order 3 in \( N_G(P) \). Since \( P\langle g \rangle \) is a Frobenius group, Lemma 2 implies that 3 divides 2k. Since \( k \) is a prime, this forces \( k = 3 \), and thus \( p = 13 \). Then \( q \) must be 3, \( |C_M(Q)| = 3^2 \), and \( N_G(Q) \) has order 24. Suppose that \( Z(G) \) is the kernel of the action of \( G \) on \( M \). Since in \( \bar{G} = G/Z(G) = \text{PSL}(2, 13) \) all involutions are conjugate and there exists a Frobenius subgroup of order 26, it fol-
follows from Lemma 2 that all involutions in $\bar{G}$ centralize a submodule of order $3^3$. This implies that a Sylow 2-subgroup of $\bar{G}$ (which is elementary abelian of order 4) has non-trivial centralizer on $M$, and that is not possible. Hence $Z(G)$ acts non-trivially on $M$, and so it acts as the inversion. Then the only elements of $G$ that fix some non-trivial vectors are in the conjugates of $Q$. It follows that if $0 \neq x \in C_M(Q)$, then

$$|G : C_G(x)| = 13 \cdot 14 \cdot 4 = 36 - 1,$$

and so $G$ acts transitively on $M^* = M \setminus \{0\}$. This is case (iii) in the statement.

Case 3. Suppose now that $p = 2^n + 1$ is a Fermat prime. Then $q$ is an odd prime divisor of $p + 1 = 2(2^{n-1} + 1)$. Thus, recalling that in SL$(2, p)$ the subgroup $Q$ is contained in a cyclic group of order $p + 1$, we have

$$r^m - 1 \big/ r^b - 1 = |G : N_G(Q)| = \frac{p(p - 1)}{2} = p2^{n-1}.$$

Since $p > 3$, it follows that $r$ is odd, and $p$ is a primitive divisor of $r^m - 1$. Hence $P$ acts irreducibly on $M$, and arguing as in one of the previous cases, we find that $2^{n-1}|m$. Thus

$$(2^n + 1)2^{n-1} = p2^{n-1} = \frac{r^m - 1}{r^b - 1} > r^{m/2} \geq 2^{2^{n-2}}.$$

As $n$ is a power of 2, this forces $n = 2, 4$. For $n = 4$, easy computations show that no data afford the above formula. If $n = 2$, then $p = 5$, and we get $G = \text{SL}(2, 5)$, $r^m = 3^4$, $r^b = 3^2$. Also, $q = 3$, and we are in case (ii).

We finish by observing that cases (ii) and (iii) do occur. Case (ii) is realized by any of the two 2-dimensional representations of SL$(2, 5)$ over GF$(9)$, and case (iii) by any of the two 6-dimensional representations of SL$(2, 13)$ over GF$(3)$ (see [11] for details). □

5 The condition $c_q$

The following rather elementary observation is the key to most of our inductive arguments, and it seems to be one point at which condition $c_q$ plays a crucial role.

Lemma 14. Let $(G, M)$ satisfy $c_q$. Let $H \leq G$ with $M_H = C_M(H) \neq 1$, and $Y \leq G$ with $C_G(H) \leq Y \leq N_G(M_H)$. Then one of the following holds:

(i) $M_H \leq C_M(Q)$ for some Sylow $q$-subgroup $Q$ of $G$, and $Y \leq N_G(Q)$;

(ii) $(Y, M_H)$ satisfies $c_q$, and $q$ does not divide $|G : Y|$.
Proof. First suppose that $1 \neq M_H \leq C_M(Q)$ for some $Q \in \text{Syl}_q(G)$, and let $Y = N_G(M_H)$. Then $C_M(C_Y(M_H)) = M_H$. Since $M_H \neq 1$, we have

$$[C_Y(M_H), Q] = 1,$$

by condition $\mathcal{C}_q$. Hence $N_G(C_Y(M_H))$ contains $Q$ as a normal subgroup; in fact, if $x \in N_G(C_Y(M_H))$, then $Q^x \leq C_G(M_H)$, and so $Q^x = Q$. It follows that $Y$ normalizes $Q$.

Assume now that $M_H \not\cong C_M(Q)$ for all $Q \in \text{Syl}_q(G)$ (and $C_G(H) \leq Y \leq N_G(M_H)$). Since $M_H \neq 1$, there exists $Q \in \text{Syl}_q(G)$ such that $Q \leq C_G(H) \leq Y$, and so $q$ divides $|Y/C_Y(M_H)|$ and does not divide $|G : Y|$. Let $1 \neq v \in M_H$, and let $Q_v$ be the only Sylow $q$-subgroup of $G$ that centralizes $v$. Then $[Q_v, H] = 1$, and so $Q_v \not\leq Y$. Hence $Q_v \leq Z(C_G(v)) \cap Y \leq Z(C_Y(v))$, and therefore $(Y, M_H)$ satisfies $\mathcal{C}_q$. \qed

In the proof of the next preparatory lemma, we use Lemma 7 from Section 2.

Lemma 15. Let $q$ be an odd prime, and $G = NQ$, with $N = O^q(G)$ a $q'$-subgroup and $Q \in \text{Syl}_q(G)$ with $|Q| = q$. Let $G$ act faithfully on the elementary abelian $r$-group $M$, with $q \not\equiv r \not\equiv 1$, and assume that $(G, M)$ satisfies $\mathcal{C}_q$. Then for every prime divisor $p$ of $|N|$ and every $Q$-invariant Sylow $p$-subgroup $P$ of $N$, $[P, Q]$ is cyclic.

Proof. We proceed by induction on $|G|$.

Let $|M| = r^m$, $|C_M(Q)| = r^s$, and

$$k = |G : N_G(Q)| = |N : C_N(Q)| = (r^m - 1)/(r^s - 1).$$

We first show that $m = sq$. If $m = 2$ then $k = r + 1$, and hence $q = r$, a contradiction. Thus $m \geq 3$ and so there exists a primitive divisor $t$ of $r^m - 1$. Let $T$ be a $Q$-invariant Sylow $t$-subgroup of $N$. Then $T$ is cyclic and $Q$ acts fixed-point freely on it; hence $TQ$ is a Frobenius group acting faithfully on $M$. Since $C_M(T) = 1$, by Lemma 2 we get $m = |Q|s = qs$. It follows in particular that $k$ is odd.

Now let $p$ be a prime divisor of $|N|$, and $P$ a $Q$-invariant Sylow $p$-subgroup of $N$. If $p \nmid k$, then $P \leq N_N(Q) = C_N(Q)$ and so $[P, Q] = 1$.

Suppose that $p|k$ and $p$ does not divide $|C_N(Q)|$. Then $P$ itself is cyclic. In fact, since $p$ is odd, if $P$ is not cyclic there exists $x \in P \setminus \{1\}$ such that $C_M(x) \neq 1$, which implies by $\mathcal{C}_q$ that $x$ centralizes a conjugate of $Q$, contradicting the assumption $p \nmid |C_N(Q)|$.

Finally suppose that $p$ divides both $k$ and $|C_N(Q)|$. Then $p$ does not divide $r^s - 1$: in fact, if $p | r^s - 1$ then

$$k = r^{s(q-1)} + \cdots + r^s + 1 \equiv q \pmod{p},$$

which is absurd as $p|k$. 
Since $p \mid r^m - 1$ and since $m = sq$ from Lemma 2, this implies in particular that $q$ divides the order of $r$ modulo $p$, whence (as $q \geq 3$),

$$q \mid p - 1 \quad \text{and} \quad p \geq 5.$$ 

Let $1 \neq x \in \Omega_1(Z(P))$, and suppose that $M_x = C_M(x) \neq 1$. Then $M_x \nleq C_M(Q_1)$ for any conjugate $Q_1$ of $Q$. In fact, if $M_x \lneq C_M(Q_1)$ then, by Lemma 14,

$$P \leq N_G(\langle x \rangle) \leq N_G(Q_1) = C_G(Q_1)$$

which is a contradiction. Thus, if we set $Y = C_G(x)$ and $C = C_Y(M_x)$, then $(Y/C, M_x)$ satisfies $\mathcal{C}_q$ by Lemma 14. By possibly replacing $Q$ with a conjugate, $PQ \leq Y$ and so, by the inductive assumption, $[P, Q]C/C$ is cyclic. Since $C$ is centralized by $Q$, from this it easily follows that $[P, Q]$ is cyclic.

Thus we may assume that $C_M(x) = 1$ for every $x \in Z(P) \setminus \{1\}$. In particular $Z(P)$ is cyclic. Let $X = \Omega_1(Z(P))$.

Note that $X \in N_1^Q(P)$. For, if not, then $[X, Q] = 1$, and so $X$ acts on $C_M(Q)$, and since $C_M(x) = 1$, this would give the contradiction $p \mid r^4 - 1$.

Suppose that $|N_1^Q(P)| \geq 2$, and let $B \in N_1^Q(P)$, $B \neq X$. Then $A = \langle B, X \rangle = B \times X$ is elementary abelian of order $p^2$ and $[A, Q] = A$. Since $Q$ normalizes $B$, no conjugate of $Q$ can centralize $B$, and so $C_M(B) = 1 = C_M(X)$. By coprime action, we have

$$M = \langle C_M(U) \mid 1 \neq U \leq A \rangle.$$ 

Since $A$ has $p + 1$ non-trivial proper subgroups, and $X$ and $B$ have trivial centralizer on $M$, it follows that there exist (cyclic) subgroups of $A$ with non-trivial centralizer on $M$, and that the number of them is at most $p - 1$. Thus $A$ has a non-trivial proper subgroup $U$ such that

$$r^b \geq p^{1/\sqrt{|M|}} = r^{m/(p-1)} > r^{m/p},$$

where $M_U = C_M(U)$ and $r^b = |M_U|$. Since $X \leq C_G(U)$ is not centralized by any conjugate of $Q$ (and so it does not normalize any such conjugate), by Lemma 14, $M_U$ does not centralize any conjugate of $Q$. Thus $(Y/C, M_U)$ satisfies $\mathcal{C}_q$, where $Y = C_G(U)$ and $C = C_Y(M_U)$. In particular, if $Q_1$ is a conjugate of $Q$ contained in $Y$, then $Q_1$ centralizes $C$ and

$$|Y : N_Y(Q_1)| = \frac{r^b - 1}{p^b - q - 1}.$$ 

Note that $r^b \equiv 1 \pmod{p}$, as $X$ acts fixed-point freely on $M_U$. Suppose that $b \nmid m$, and let $t$ be a primitive divisor of $r^b - 1$; then $t \nmid r^m - 1$. But this implies that $Q_1$ centralizes a Sylow $t$-subgroup of $G$ and so it centralizes a Sylow $t$-subgroup of $Y$, which
is a contradiction. Thus $b$ divides $m$. Let $m = bt$; then

$$
\frac{r^m - 1}{r^b - 1} = r^{bt-1} + \cdots + r^b + 1 \equiv t \pmod{p}.
$$

Since $1 < t < p$, it follows that $p$ does not divide $(r^m - 1)/(r^b - 1)$. Therefore, as $p$ does not divide $r^s - 1$, the full $p$-part of $k = |N : C_N(Q)|$ divides

$$(r^b - 1)/(r^{b/q} - 1) = |Y : C_Y(Q_1)|.$$  

If $P_1$ is a $Q_1$-invariant Sylow $p$-subgroup of $N$ containing a $Q_1$-invariant Sylow $p$-subgroup $P_2$ of $Y$, we have

$$P_1 = C_{P_1}(Q_1)P_2$$

and consequently $[P_1, Q_1] = [P_2, Q_1]$, which is cyclic by the inductive assumption and an argument used before.

Hence we are left with the case $|N^{1_Q}(P)| = 1$, for which we obtain the desired conclusion by appealing to Lemma 7. □

Assuming Theorem 1 (whose proof we postpone to the next section), we now show

**Lemma 16.** Let $(G, M)$ satisfy $\mathcal{C}_q$, with $|M| = r^m$ for some prime $r \neq q$, and suppose that $G$ is $q$-nilpotent. Then $G/C_G(M)$ is a subgroup of $\Gamma(M)$.

**Proof.** We may assume that $G$ is faithful on $M$. Let $N$ be the normal $q$-complement of $G$, and $Q$ a Sylow $q$-subgroup of $N$. Let $X$ be a subgroup of order $q$ of $Q$. Then $(NX, M)$ satisfies $\mathcal{C}_q$. By Lemma 15, for every prime divisor $p$ of $|N|$ and every $X$-invariant Sylow $p$-subgroup $P$ of $N$, $[P, X]$ is cyclic. As $q \neq 2$, by Theorem 1, $[N, X]$ is cyclic. Now $[N, X]X = O^q(NX)$, which is a subgroup of $\Gamma(M)$ by the soluble case. Hence, by Lemma 11, $NX$ is a subgroup of $\Gamma(M)$. In particular, $N$ is soluble, and so, by Corollary 10, $G$ is a subgroup of $\Gamma(M)$. □

We may now prove the Main Theorem.

**Theorem 17.** Let $(G, M)$ satisfy $\mathcal{C}_q$, with $|M| = r^m$ for some prime $r \neq q$. Then $G/C_G(M)$ is a $q$-nilpotent subgroup of $\Gamma(M)$.

**Proof.** We assume, by contradiction, that the group $G$ acts on the GF($r$)-module $M$ satisfying condition $\mathcal{C}_q$, with $q \neq r$, and $|G| + |M|$ minimal such that $G/C_G(M)$ is not embedded in $\Gamma(M)$.

Clearly $G$ is faithful on $M$ and, by Proposition 8(2) we have $q \neq 2$. We set $|M| = r^m$ and, for $Q \in \text{Syl}_q(G)$, $|C_M(Q)| = r^s$. By Proposition 8(3) we have $s|m$, and we remark once again that $m \geq 3s$ (if $m = 2s$, then the equality $|G : N_G(Q)| = r^s + 1$
yields \( r = q \), contrary to one of our assumptions). By Lemma 16, we derive a contradiction if we show that \( G \) is \( q \)-nilpotent. We do this in a number of steps.

**Step 1.** \( G = O^q(G) \) is not soluble; in particular \( 2 \) divides \(|G|\).

**Proof.** This follows from Proposition 9 and Lemma 11.

**Step 2.** We may assume that \((r, |G|) = 1\), and in particular \( r \neq 2 \).

**Proof.** Suppose that \( r \) divides \(|G|\), and let \( R \) be a Sylow \( r \)-subgroup of \( G \). Then \( 1 \neq C_M(R) \neq M \). Put \( M_R = C_M(R) \). If \( M_R \leq C_M(Q) \) for some \( Q \in \text{Syl}_q(G) \), then by Lemma 14, \( R \) normalizes \( Q \), and so \( R \) acts on \([M, Q] \neq 1\). As \( q \neq r \) it follows that

\[
1 \neq C_{[M, Q]}(R) = C_M(R) \cap [M, Q] \leq C_M(Q) \cap [M, Q] = 1,
\]

a contradiction. Thus \( M_R \not\subset C_M(Q) \) for all \( Q \in \text{Syl}_q(G) \). Let \( Y = N_G(R) \); then \( Y \neq G \) since \( G \) is irreducible on \( M \). By Lemma 14, \((Y, M_R)\) satisfies \( \mathcal{C}_q \). By minimality of \((G, M)\), it follows that \( Y = Y/C_Y(M_R) \) is a \( q \)-nilpotent subgroup of \( 
G \) in particular, if \( Q \in \text{Syl}_q(Y) \),

\[
[N_Y(Q), Q] \leq Q \cap C_Y(M_R) \neq Q.
\]

On the other hand, \( C_{M_R}(Q) \neq 1 \), and so \( R \leq C_G(Q) \). By the Frattini argument we have

\[
N_G(Q) = C_G(Q)(N_G(Q) \cap N_G(R)) = C_G(Q)(N_G(Q) \cap Y) = C_G(Q)N_Y(Q).
\]

Since \( Q \) is abelian we deduce (see [1, (37.7)])

\[
Q \cap O^q(G) = [Q, N_G(Q)] = [Q, C_G(Q)N_Y(Q)] = [Q, N_Y(Q)] < Q.
\]

Therefore \( O^q(G) \neq G \). By the choice of \( G \), the subgroup \( O^q(G) \) is \( q \)-nilpotent, and so is \( G \).

**Step 3.** Let \( H \leq G \), with \(|C_M(H)| = r^b\). Then \( b|m \), or \( C_M(H) \leq C_M(Q) \) for some \( Q \in \text{Syl}_q(G) \).

**Proof.** Let \( M_H = C_M(H) \), \( Y = N_G(H) \), and suppose that \( M_H \not\subset C_M(Q) \) for all \( Q \in \text{Syl}_q(G) \). Then by Lemma 14, \((Y, M_H)\) satisfies \( \mathcal{C}_q \) and so, by choice of \( G \), \( Y/C_Y(M_H) \) is, in particular, \( q \)-nilpotent; moreover, if \( Q \) is a Sylow \( q \)-subgroup of \( G \) contained in \( Y \) (and centralizing \( C_Y(M_H) \)), we have

\[
|Y : N_Y(Q)| = \frac{r^b - 1}{r^c - 1}
\]

where \( r^c = |C_{M_H}(Q)| \).
If \( b = 2 \), then \(|Y : N_Y(Q)| = r + 1 \equiv 1 \pmod{q}\), forcing \( q = r \) against one of the assumptions. In the remaining cases, \( r^b - 1 \) admits a primitive prime divisor \( p \) (recall that \( r \neq 2 \)). Let \( P \) be a Sylow \( p \)-subgroup of \( Y \). Then \( P \) acts without fixed points on \( M_{H} \setminus \{1\} \). Suppose, by contradiction, that \( b \) does not divide \( m \). Then \( p \) does not divide \( r^m - 1 \), and so \( P \) normalizes some Sylow \( q \)-subgroup \( Q_1 \) of \( G \). In particular, \( P \) acts on \( C_M(Q_1) \). If \( C_{C_M(Q_1)}(P) \neq 1 \), then \( P \) centralizes \( Q_1 \), and this is absurd since, in \( Y \), the subgroup \( Q \) normalizes but does not centralize \( P \). Hence \( C_{C_M(Q_1)}(P) = 1 \). It follows that \( p \) divides \(|C_M(Q_1)| - 1 = r^s - 1 \). So \( b|s \); and since \( s|m \) this gives a contradiction.

**Step 4.** \( G \) is perfect and \( G/O_2(G) \) is quasi-simple.

**Proof.** Since \( G = O'^d(G) \) and \( G \) is not \( q \)-soluble, by Proposition 8(4) and the choice of \( G \) we also have \( O^q(G) = G \). So, in particular, \( G \) is perfect. Let \( K \trianglelefteq G \) be such that \( G/K \) is a non-abelian simple group; since \( G = O'^d(G) \), \( q \) divides \(|G/K|\).

Suppose that \( q \) divides \(|K|\). By Proposition 8(4), the pair \((K, M)\) also satisfies \( \mathcal{C}_q \). Let \( Q_1 = Q \cap K \) (where \( Q \in \text{Syl}_q(G) \)). If \( M_{Q_1} = C_M(Q_1) > C_M(Q) \), then \((N_G(Q_1), M_{Q_1})\) satisfies \( \mathcal{C}_q \) by Lemma 14, and, by the choice of \( G \), the quotient \( N_G(Q_1)/C_{N_G(Q_1)}(M_{Q_1}) \) is, in particular, soluble. By the Frattini argument we see that \( N_G(Q_1)/N_K(Q_1) \approx G/K \) is perfect, and so

\[
C_G(M_{Q_1})N_K(Q_1) = N_G(Q_1),
\]

yielding \( C_G(M_{Q_1})K = G \). It follows that \( C_G(M_{Q_1}) \) contains a Sylow \( q \)-subgroup of \( G \), which is a contradiction. Thus \( M_{Q_1} = C_M(Q) \), whence (since \((K, M)\) satisfies \( \mathcal{C}_q \))

\[
|G : N_G(Q)| = \frac{r^m - 1}{r^s - 1} = |K : N_K(Q_1)|.
\]

As \( N_G(Q_1) \trianglelefteq N_G(Q) \), it follows that \( N_G(Q_1) = N_G(Q) \), and by the Frattini argument this leads to the contradiction \( KQ \trianglelefteq G \). Hence \( q \) does not divide \(|K|\).

Let \( t \) be a primitive divisor of \( r^m - 1 \). Suppose that \( t \) divides \(|K|\), and let \( T_0 \in \text{Syl}_t(K) \). By the Frattini argument \( G = KN_G(T_0) \). Now \( T_0 \) is cyclic, hence \( N_G(T_0)/C_G(T_0) \) is abelian; and since \( G \) is perfect this implies \( G = KC_G(T_0) \). But in GL\((m, r)\) the centralizer of \( T_0 \) is cyclic, and this gives a contradiction. Thus \( t \) does not divide \(|K|\). Let \( T \in \text{Syl}_t(G) \), and let \( p \) be an odd prime divisor of \(|K|\), and \( P \) a \( T \)-invariant Sylow \( p \)-subgroup of \( K \). By Lemma 6, \( T \) centralizes \( P \). Hence \( |K : C_K(T)| \) is a power of 2, and thus, if \( D \) is a \( T \)-invariant Sylow 2-subgroup of \( K \), then \( K = C_K(T)D \). Therefore

\[
[K, T] = [C_K(T)D, T] = [D, T] \leq D.
\]

Since \( |K, T| \leq K \) the subgroup \( T \) centralizes \( K/O_2(K) \). Thus \( [K, T^G] \leq O_2(G) \).

Now \( G = KT^G \) and \( G/T^G \cong K/(K \cap T^G) \) is a \( q' \)-group; it follows that \( T^G = G \) and \( K/O_2(K) \) is a central factor of \( G \). Since \( G \) is perfect and \( O_2(K) = O_2(G) \), we get the conclusion.
**Step 5.** Let $D$ be a Sylow 2-subgroup of $G$. Then $D$ is not a cyclic, dihedral, or quaternion group.

**Proof.** Since $G$ is not soluble, $D$ is not cyclic. Assume that $D$ is a dihedral or quaternion group. Then $O_2(G)$ is cyclic, dihedral or quaternion; in any case its automorphism group is soluble. Since $G$ is perfect, $O_2(G) \leq Z(G)$ and thus $G$ is quasi-simple by Step 4, and the Sylow 2-subgroups of $G/Z(G)$ are dihedral. From the Gorenstein–Walters classification of groups with dihedral Sylow 2-subgroups (see e.g. [1] or [7]) it follows that $G$ is isomorphic to $\text{PSL}(2, p^k)$ or $\text{SL}(2, p^k)$ for some odd $p^k > 3$, or to a covering group of $A_7$. Since $q \neq r$, Proposition 13 rules out the linear cases. Assume that $A_7 \simeq G/Z(G)$, where $Z(G)$ is cyclic of order dividing 6. Then the Sylow 3-subgroups of $G$ are non-cyclic, and so $G$ has an element $x$ of order 3 such that $C_M(x) \neq 1$. Since the centralizer in $G$ of a non-trivial 3-element is a $\{2, 3\}$-group, condition $\mathcal{C}_q$ implies $q = 3$. But the normalizer in $G$ of a Sylow 3-subgroup has index 70, which is not of the form $(r^m - 1)/(r^i - 1)$.

**Step 6.** Let $Q \in \text{Syl}_q(G)$, and let $x$ be an involution in $N_G(Q)$. Then $x \in C_G(Q)$ or $x$ acts as the inversion on $Q$.

**Proof.** We write $B = C_Q(x)$, $Y = C_G(B)$, and $M_B = C_M(B)$. We show firstly that $M_B \leq C_M([Q, x])$. If $M_B = 1$ there is nothing to prove. So assume $M_B \neq 1$. Again, if $M_B \leq C_M(Q)$ we are immediately done. Otherwise $M_B > C_M(Q)$ and so, by Lemma 14, $(Y, M_B)$ satisfies $\mathcal{C}_q$; hence, by the minimality of $(G, M)$, the group $\overline{Y} = Y/C_Y(M_B)$ embeds as a $q$-nilpotent subgroup in $\Gamma(M_B)$. Now $\langle Q, x \rangle \leq Y$ and $x \in N_G(Q)$; thus $[Q, x] \leq C_Y(M_B)$, which means that $M_B \leq C_M([Q, x])$.

Suppose now that $x$ does not act as the inversion on $Q$. Then, since $Q$ is abelian (and $q \neq 2$), we have $Q = B \times [Q, x]$, where $B = C_Q(x) \neq 1$. Thus, by what we observed above

$$C_M(B) = C_M([Q, x]) \cap C_M(B) = C_M(Q).$$

If $[M, x] = M$ then $x$ is the inversion on $M$, and so $x \in Z(G)$. Otherwise, there exists $v \in C_M(x) \setminus \{1\}$, and $v$ is centralized by a Sylow $q$-subgroup $Q_1$ of $G$ contained in $C_G(x)$. Now $B \leq C_G(x)$, and so there exists $h \in C_G(x)$ such that $B \leq Q_1^h$. Thus $C_M(Q_1^h) \leq C_M(B) = C_M(Q)$, and it follows that $Q_1^h = Q$, whence $Q \leq C_G(x)$.

We now distinguish two cases, according to the existence or not of involutions acting as the inversion on $Q$. First suppose (up to Step 11) that all involutions normalizing $Q$ centralize it.

**Step 7.** If $x$ is an involution of $G$, then either $C_M(x) = 1$ (and so $x$ is the inversion on $M$ and $x \in Z(G)$) or $|C_M(x)| = \sqrt{|M|} = r^{m/2}$.

**Proof.** Suppose that $C_M(x) \neq 1$, and let $Y = C_G(x)$. Let $M_1 = [M, x]$, and $|M_1| = r^t$. Since $|C_M(x)| \leq r^{m/2}$ by Step 3, we have $t \geq m/2$. Let $1 \neq b \in M_1$, and let $Q$ be a Sylow $q$-subgroup of $G$ with $Q \leq C_G(b)$. Since $x$ inverts $b$ and $Q \leq C_G(b)$, we have
Let $Q \in \text{Syl}_q(G)$. Then $Q$ is cyclic and $m = s|Q|$.

Proof. Since, by Step 5, the Sylow 2-subgroups of $G$ are not cyclic or quaternion groups, $G$ has an involution $x$ which does not act as the inversion on $M$. Let $M_x = C_M(x)$ and $M_1 = [M, x]$. Then $M = M_x \times M_1$ and $|M_x| = |M_1| = r^{m/2}$ by Step 7. Let $Y = C_G(x)$. From the proof of Step 7 it follows that both $(Y, M_x)$ and $(Y, M_1)$ satisfy $\mathcal{C}_q$. Let $Q \in \text{Syl}_q(G)$ with $Q \leq Y$. Then $C_{M_1}(Q) \neq 1$, and so

$$C_Y(M_x) \cap Q = 1$$

by Step 3 (as $|M_x| = r^{m/2}$). Since, by minimality of $G$, $Y/C_Y(M_x)$ is a $q$-nilpotent subgroup of $\Gamma(M_x)$, it follows that $Q \simeq QC_Y(M_x)/C_Y(M_x)$ is cyclic and also that

$$r^{m/2} = |M_x| = r^{s_1|Q|}$$

where $r^{s_1} = |C_{M_1}(Q)|$. Now we have $|M_x| = |M_1|$, and thus condition $\mathcal{C}_q$ implies that $|C_{M_1}(Q)| = |C_{M_1}(Q)|$; therefore $s_1 = s/2$, which finally yields the desired equality

$$m = 2s_1|Q| = s|Q|.$$

Step 9. Let $Q \in \text{Syl}_q(G)$, then $|G : N_G(Q)|$ is odd.

Proof. Since $m = s|Q|$ by Step 8 and $r^s$ and $|Q|$ are odd, we have that

$$|G : N_G(Q)| = \frac{r^m - 1}{r^s - 1} = r^s(|Q|-1) + \cdots + r^s + 1$$

is odd.

Step 10. Let $Q \in \text{Syl}_q(G)$, and let $D$ be a Sylow 2-subgroup of $N_G(Q)$. Then $D \leq C_G(Q)$.

Proof. The subgroup $D$ is in fact a Sylow 2-subgroup of $G$ by Step 9. Let $z$ be a central involution of $D$.

Suppose that $M_z = C_M(z) \neq 1$ and let $Y = C_G(z)$. Observe that $DQ \leq Y$. By Step 7, $|M_z| = r^{m/2}$, and by choice of $G$, $Y/C_Y(M_z)$ is a $q$-nilpotent subgroup of $\Gamma(M_z)$. In particular $D$ centralizes $Q$ modulo $C_Y(M_z)$; that is

$$[D, Q] \leq Q \cap C_Y(M_z) < Q.$$
Suppose now that $C_M(z) = 1$. Then $z$ acts as the inversion on $M$, and $z$ is central in $G$. Now $D$ is not a cyclic or quaternion group, so it has more than one involution. In particular not all involutions of $G$ are conjugate. Since $G = O^2(G)$ (by Step 1), a classical transfer argument ensures that $D$ is not dihedral or semidihedral. Therefore $D$ has a normal elementary abelian subgroup $A = \langle x, z \rangle$ of order 4. Let $Y = C_G(x)$. Since $z$ is central in $G$ we have $Y = C_G(A)$; also, $D \leq N_G(Y)$. Let $M_x = C_M(x)$ and $C = C_Y(M_x)$. As usual, $Y/C \leq \Gamma(M_x)$ (and $Q \leq Y$). Let $t$ be a primitive divisor of $m/2 - 1$ (this exists because $m/2 = s|Q|/2 > 2$).

Suppose, by contradiction, that $t$ divides $|C|$, and let $g$ be an element of $C$ of order $t$. Then $M_x = C_M(g)$ by Step 3. On the other hand, $g$ centralizes $Q$ and so it acts on $C_M(Q)$. Since $C_M(Q) = r^s$ and $s < m/2$, it follows that $g$ centralizes $C_M(Q)$, whence $C_M(Q) \leq C_M(g) = M_x$, which contradicts $C_{[M,x]}(Q) \neq 1$ (see the proof of Step 7).

Thus $t$ does not divide $|C|$. Therefore, if $T \in \text{Syl}_t(Y)$, then $T \cong TC/C$ is a cyclic group. Possibly replacing $T$ by a conjugate, we may assume that $T$ is normalized by $Q$ (since $CT \leq Y$ and by the Frattini argument); moreover $[T, Q] = T$, since $TC/C \leq \Gamma_0(M_x)$ and $t$ is primitive. Thus $T \leq Q^Y$. But $Q$ centralizes $C$, and so we get that $T$ centralizes $C$. Hence $CT = C \times T$, and since $CT \leq Y$ we have $T \cong Y$, and consequently $T$ is characteristic in $Y$. As $D \leq N_G(Y)$, it follows that $D \leq N_G(T)$. Then $DQ$ normalizes $T$; but $T$ is cyclic and thus $\text{Aut}(T)$ is abelian; therefore

$$[D, Q] \leq Q \cap C_G(T) = C_Q(T).$$

On the other hand, $Q \not\cong C_G(T)$, and so $[D, Q] < Q$. Since $Q$ is cyclic, this forces $[D, Q] = 1$ as required.

**Step 11.** $G$ is $q$-nilpotent.

**Proof.** Let $Q \in \text{Syl}_q(G)$, $|Q| = q^k$, and $m = sq^k$. Then $Q$ is cyclic by Step 8.

Suppose that $N_G(Q) / C_G(Q) \neq 1$; let $p$ be a prime divisor of $|N_G(Q) : C_G(Q)|$ and $P$ a Sylow $p$-subgroup of $N_G(Q)$. Then $p \neq 2$ by Step 10. Now $P$ acts on $C_M(Q)$. Since $P$ does not centralize $Q$, $P$ acts without fixed points on $C_M(Q) \setminus \{1\}$, and so $p$ divides $|C_M(Q)| - 1 = r^s - 1$. Hence

$$|G : N_G(Q)| = \frac{r^m - 1}{r^s - 1} = r^s(q^k - 1) + \ldots + r^s + 1 \equiv q^k \pmod{p}.$$ 

Therefore $p$ does not divide $|G : N_G(Q)|$, and thus $P \in \text{Syl}_p(G)$. Furthermore $p \mid q - 1$ by Step 8, and $P/C_P(Q)$ is cyclic.

Let $1 \neq a \in P$ with $a^p = 1$, and assume by contradiction that $a \notin C_P(Q)$. Then we have $C_{C_M(Q)}(a) = 1$; also, $Q\langle a \rangle$ is a Frobenius group and so, by Lemma 2, $|C_M(a)| = |C_{[M,Q]}(a)| = r^m / s$. If $C_M(a) \leq C_M(Q_1)$ for some $Q_1 \in \text{Syl}_q(G)$, then

$$\frac{m - s}{p} = \frac{s(q^k - 1)}{p} \leq s,$$
hence \( q^k - 1 \leq p \), and so \( p = q - 1 \). The only possible case is \( q = 3 \), but then \( p = 2 \), against the fact that \( p \) is odd. Otherwise, \((m - s)/p = s(q^k - 1)/p\) divides \( m = sq^k \) by Step 3, and this also is impossible. Thus \( a \in C_P(Q) \) and so \( \Omega_1(P) \leq C_P(Q) \).

Now let \( 1 \neq b \in \Omega_1(Z(P)) \), and suppose that \( C_M(b) \neq C_M(Q) \). If \( Y = N_G(\langle b \rangle) \), then \( (Y, C_M(b)) \) satisfies \( \mathcal{C}_q \) by Lemma 14, and so \( Y/C_Y(C_M(b)) \) is a \( q \)-nilpotent subgroup of \( \Gamma(C_M(b)) \). Now \( P \leq Y \cap N_G(Q) \), and so it follows that

\[
[P, Q] \leq Q \cap C_Y(C_M(b)) < Q,
\]

whence \( P \leq C_G(Q) \), a contradiction. Thus \( C_M(b) \leq C_M(Q) \) for all non-trivial \( b \in \Omega_1(Z(P)) \). In particular, \( Z(P) \) is cyclic. We let \( \langle b \rangle = \Omega_1(Z(P)) \).

Suppose that \( C_M(b) \neq 1 \). Then, by what was observed above and Lemma 14, \( N_G(\langle b \rangle) \leq N_G(Q) \), and so, since \( \langle b \rangle \) is characteristic in \( P \), we have \( N_G(P) \leq N_G(Q) \). As \( Q \) is cyclic, \( N_G(Q)' \leq C_G(Q) \), and we thus get

\[
[N_G(P), P] \leq C_G(Q) \cap P = C_P(Q) < P. \tag{4}
\]

Let \( g \in G \) be such that \( P \cap P^g \neq 1 \), let \( 1 \neq h \in P \cap P^g \), and \( \langle h_1 \rangle = \Omega_1(\langle h \rangle) \). If \( \langle h_1 \rangle = \langle b \rangle \), then (as \( C_M(h_1) \neq 1 \)) \( h_1 \) centralizes just one Sylow \( q \)-subgroup of \( G \). Thus \( Q = Q^g \), i.e. \( g \in N_G(Q) \), and therefore \( P^g \in N_G(Q) \), yielding

\[
P \cap (P^g)^g \leq C_P(Q).
\]

Otherwise \( X = \langle h_1, b \rangle \) is elementary abelian of order \( p^2 \). Thus \( [M, Q] \) is generated by the centralizers of the non-trivial cyclic subgroups of \( X \). Let \( x \in X \setminus \langle b \rangle \) be such that \( C_{|M, Q|}(x) \) is as large as possible. If \( C_M(x) \leq C_M(Q_1) \) for some \( Q_1 \in \text{Syl}_q(G) \), then

\[
r^{(m-s)/p} \leq |C_M(x)| \leq |C_M(Q_1)| = r^s,
\]

and thus \( s(q^k - 1) \leq sp \leq s(q - 1) \), forcing \( q - 1 = p = 2 \), which is not the case. Therefore, by Lemma 14 and the choice of \( G \), \( (C_G(x), C_M(x)) \) satisfies \( \mathcal{C}_q \) and \( C_G(x)/C_{G(x)}((C_M(x))) \) is a \( q \)-nilpotent subgroup of \( \Gamma(C_M(x)) \). Now, as \( h \in P \) and \( b \in Z(P) \), \( h \) centralizes \( X \). In particular \( h \in C_G(x) \cap N_G(Q) \) and therefore \( [h, Q] \leq C_Q(C_M(x)) < Q \). Hence \( h \in C_P(Q) \). We have proved in particular that \( \langle C_M(b) \rangle \neq 1 \) we have \( P \cap (P^g)^g \leq C_P(Q) \) for all \( g \in G \). Together with (4) and Grün’s theorem (see [4, (3.4)]), this yields \( P \cap G' \leq C_P(Q) \), which contradicts \( G = O^q(G) \).

Thus \( C_M(b) = 1 \). Assume that \( P \) is not cyclic. Then, as \( p \neq 2 \), there exists a normal elementary abelian subgroup \( A \) of \( P \) of order \( p^2 \). Clearly \( b \in A \); fix \( a \in A \setminus \{1\} \) such that \( A = \langle a, b \rangle \), and let \( C = C_P(A) \). As \( A \cap Z(P) = \langle b \rangle \), the subgroups \( \langle ab^i \rangle \) (\( i = 0, \ldots, p - 1 \)) are conjugate in \( P \). Also

\[
M = \langle C_M(ab^i) \mid i = 0, \ldots, p - 1 \rangle = C_M(a) \times C_M(ab) \times \cdots \times C_M(ab^{p-1}).
\]

Hence \( |C_M(a)| = r^{m/p} \), and \( C_M(a) \neq C_M(Q_1) \) for all \( Q_1 \in \text{Syl}_q(G) \). We now apply the same argument as in Step 10. Let \( Y = C_G(a) \) and \( C = C_Y(C_M(a)) \). Then
$Y/C_Y(C_M(a))$ is a $q$-nilpotent subgroup of $\Gamma(C_M(a)) = \Gamma(r^{m/p})$. Let $t$ be a primitive divisor of $r^{m/p} - 1$ (it exists because $m/p \neq 2$, as $q \neq p$), and $T \in \text{Syl}_q(Y)$. Suppose that there exists an element $x$ of order $t$ in $C$; then $x$ centralizes some $Q_1 \in \text{Syl}_q(G)$ and so acts on $C_M(Q_1)$ that has order $r^t$. Since $x$ does not centralize $C_M(Q_1)$ (otherwise $C_M(Q_1) \leq C_M(x) = C_M(a)$ which is not the case), by primitivity of $t$ we have $m/p \leq s$, which yields $q^k < p$ in contrast to $p \mid q - 1$. Hence $T \cap C = 1$. Then, arguing as in Step 10, one shows that $TC = T \times C$, and $T \trianglelefteq Y$. As $C_M(b) = 1$, we have $\langle b \rangle C/C \cong Y/C$, and so $[b, T] \leq C \cap T = 1$. Hence $T$ centralizes $b$. Since $T \leq Y = C_G(a)$, we have $T \leq C_G(A) \leq Y$, and clearly $T$ is characteristic in $C_G(A)$. Now $P \leq N_G(A)$, whence $P$, as well as $Q$, normalizes $T$. Since $T$ is cyclic we derive the contradiction

$$Q = [P, Q] \leq C_T.$$  

We are left with the case in which $P$ is cyclic. Let $B = \langle b \rangle = \Omega_1(P)$. Then $[B, Q] = 1$ by what we observed before. Now, as $P \leq N_G(Q)$ and $Q$ is cyclic,

$$[N_G(P) \cap N_G(Q), P] \leq P \cap C_G(Q) < P,$$

and since $P$ is cyclic, this forces $N_G(P) \cap N_G(Q) \leq C_G(P) \leq C_G(B)$.

Let $W = N_G(B) \cap N_G(Q)$; then $P \leq C_G(B) \cap N_G(Q) \leq W$, and by the Frattini argument

$$W = (C_G(B) \cap N_G(Q))N_W(P) = (C_G(B) \cap N_G(Q))(N_G(P) \cap N_G(Q)) \leq C_G(B).$$

Therefore, since $Q \leq C_G(B)$, by applying the Frattini argument once more we have

$$N_G(B) = C_G(B)(N_G(B) \cap N_G(Q)) = C_G(B)W = C_G(B).$$

In particular, $N_G(P) \leq N_G(B) = C_G(B)$. Since $B = \Omega_1(P)$ and $P$ is cyclic, this implies $N_G(P) = C_G(P)$. It follows that $G$ is $p$-nilpotent by Burnside’s theorem, and this contradicts $O^d(G) = G$.

Therefore, $N_G(Q) = C_G(Q)$, and $G$ is $q$-nilpotent.

We now turn to the second case: suppose that $G$ has an involution $t$ that acts as the inversion on $Q \in \text{Syl}_q(G)$.

**Step 12.** $m = 3s$, and $|G : N_G(Q)|$ is odd.

**Proof.** We have $t \in N_G(Q)$ and $C_M(t) \cap C_M(Q) = 1$. Since $M = C_M(Q) \times [M, Q]$, and $t$ normalizes both factors, $C_M(t) = C_{[M, Q]}(t)$. We have $|[M, Q]| = r^{m-s}$. Now $Q \langle t \rangle$ is a Frobenius group and so, by Lemma 2,

$$|C_M(t)| = |C_{[M, Q]}(t)| = r^{(m-s)/2}.$$
By Step 3, either \((m - s)/2\) divides \(m\) or \((m - s)/2 \leq s\). Both cases imply \(m \leq 3s\). Since \(m \geq 3s\), we have \(m = 3s\). Then \(|G : N_G(Q)| = r^{2s} + r^s + 1\) is odd.

**Step 13.** Let \(x\) be an involution of \(G\). Then \(C_M(x) = C_M(Q)\) and \([x, Q] = 1\), for a unique Sylow \(q\)-subgroup \(Q\) of \(G\), and \(C_G(x) = N_G(Q)\).

**Proof.** Let \(x\) be an involution in \(G\). Then there exists a Sylow \(q\)-subgroup \(Q\) of \(G\) centralized by \(x\): if \(C_M(x) \neq 1\) this is by condition \(\mathcal{C}_q\), while if \(C_M(x) = 1\) then \(x\) is the inversion on \(M\) and \(x \in Z(G)\). By assumption there exists another involution \(t \in N_G(Q)\) that acts as the inversion on \(Q\). Now \(C_M(Q)\) is invariant for \(\langle x, y \rangle\). By condition \(\mathcal{C}_q\), \(C_{C_M(Q)}(t) = 1\) and so \(t\) acts as the inversion on \(C_M(Q)\). Suppose that \(C_M(Q) \neq C_M(x)\); then there exists \(u \in C_M(Q)\setminus\{1\}\) such that \(u^x = u^{-1} = u^t\). Thus \(u^x = u\) and by condition \(\mathcal{C}_q\), \(xt \in C_G(Q)\), a contradiction. Hence \(C_M(Q) \leq C_M(x)\). If \(C_M(Q) < C_M(x)\), then there exists another Sylow \(q\)-subgroup \(Q_1 \neq Q\) that is centralized by \(x\). By the same argument we thus have \(C_M(Q_1) \leq C_M(x)\). Therefore

\[|C_M(x)| \geq |\langle C_M(Q), C_M(Q_1)\rangle| = |C_M(Q)|^2 = r^{2s}\]

in contradiction to Step 3. Thus \(C_M(x) = C_M(Q)\). Finally, as \(Q\) is the only Sylow \(q\)-subgroup centralized by \(x\), we have \(C_G(x) \leq N_G(Q)\). If \(h \in N_G(Q)\), then \(x^h\) centralizes \(Q\), hence \(C_M(x^h) = C_M(x) = C_M(Q)\), and both \(x\) and \(x^h\) act as the inversion on \([M, Q]\); thus \([M, Q] \leq C_M(xx^h)\), and this forces \(xx^h = 1\), that is \(h \in C_G(x)\). Therefore \(C_G(x) = N_G(Q)\).

**Step 14.** Let \(D \in Syl_2(G)\). Then \(D\) has rank 2.

**Proof.** By Step 12 we have \(D \leq N_G(Q)\) for a Sylow \(q\)-subgroup \(Q\) of \(G\). Let \(C = C_D(Q)\) and let \(t \in D\) be an involution inverting \(Q\); then by Step 6, all involutions of \(D\) lie in \(\langle t\rangle C\). On the other hand, suppose that \(C\) has an elementary abelian subgroup \(A\) of order 4. Then there exists \(x \in A\) such that \(C_M(x) \cap [M, Q] \neq 1\) and so \(x\) centralizes more than a Sylow \(q\)-subgroup, in contradiction to Step 13. Thus \(C\) has only one involution, and consequently \(D\) has rank 2.

**Step 15.** Contradiction.

By Step 12, we have \(O_2(G) \leq N_G(Q)\) for any Sylow \(q\)-subgroup \(Q\). Hence \(O_2(G) \leq C_G(QG) = Z(G)\); therefore \(G\) is quasi-simple by Step 4. By Step 13, no involution of \(G\) can be central, hence \(|Z(G)|\) is odd and so, by Step 14, \(\bar{G} = G/Z(G)\) is a simple group with Sylow 2-subgroups of rank 2. By a fundamental result on finite simple groups (see [1, Theorem 48.1]), \(\bar{G}\) is isomorphic to one of the groups

\[
PSL(2, s), PSL(3, s), PSU(3, s) \text{ with } s \text{ odd, } A_7, M_{11}, PSU(3, 4).
\]

Now \(PSL(2, s)\) and \(A_7\) have dihedral Sylow 2-subgroups, and are excluded in Step 5. For the remaining cases, fix an involution \(t\) in \(G\). If \(G = PSL(3, s)\) with \(s\) odd and \(s \geq 5\), then \(C_G(x) \simeq GL(2, s)/K\) where \(|K| = 1, 3\). But, by Step 13, \(C_G(x) = N_G(Q)\)
for a Sylow $q$-subgroup $Q$ of $G$. As $s \geq 5$, this forces $Q$ to be central in $C_G(x)$ and this gives a contradiction (for instance, by Burnside’s $p$-nilpotency criterion, or because we assume that there exists an involution normalizing but not centralizing $Q$). If $G$ is $\text{PSL}(3, 3)$ or $M_{11}$, then $C_G(x) \approx \text{GL}(2, 3)$ and again, as $Q$ is not central in $C_G(x) = N_G(Q)$, we get a contradiction. The unitary cases are similar: if $s$ is odd, then $C_G(t)$ is a cyclic extension of $\text{SL}(2, s)$ and so any normal subgroup of odd order of $C_G(t) = N_G(Q)$ is central; if $q = 4$ then the Fitting subgroup of $C_G(t)$ is a 2-group, and so $C_G(x) = N_G(Q)$ cannot be satisfied with $q$ odd.

6 Proof of Theorem 1

Theorem 1 may be proved by appealing to the full classification of finite simple groups. First one reduces easily to the case in which $G$ is simple (as in the first part of the proof of Theorem 25); then the classification ensures that $G$ is a group of Lie type and $x$ a field automorphism. A case-by-case analysis (similar to that at the end of the proof of Theorem 25) would complete such a proof. However, we give a proof which does not rely on the classification (although it uses some deep results that are part of it, like Bender’s classification of groups with a strongly embedded subgroup).

Let us recall that a subgroup $H$ of a finite group $G$ is said to be strongly embedded if $H$ has even order and $H \cap H^g$ has odd order for all $g \in G \setminus H$. Groups with strongly embedded subgroups were classified by Bender (see [7]).

**Hypothesis I.** Let $G$ be a finite group and $x$ an automorphism of $G$. Suppose that

(a) $(|G|, |x|) = 1$, and 2 divides $|G|$;

(b) $[H, x]$ is cyclic for every proper $x$-invariant subgroup $H$ of $G$;

(c) $G$ does not admit any strongly embedded subgroup;

(d) $O^2(G) = G$ and $G$ does not possess any non-trivial normal abelian subgroup.

We first observe some elementary consequences of these assumptions.

**Lemma 18.** Assume Hypothesis I. Then $x$ centralizes a Sylow 2-subgroup $T$ of $G$. Also, there exists an involution $t$ of $T$ such that $C_G(t) \neq C_G(x)$.

**Proof.** By coprime action, $x$ normalizes a Sylow 2-subgroup $T$ of $G$. By assumption (d), $T \neq G$ and thus $[T, x]$ is cyclic. But a cyclic 2-group does not admit non-trivial automorphisms of odd order, and so $[T, x] = 1$, proving that $x$ centralizes $T$.

For the second part, let $H = C_G(x)$. Since $G$ does not admit any strongly embedded subgroups, there exists $g \in G \setminus H$ such that $H \cap H^g$ contains an involution $t$. As $T \leq H$ we may assume $t \in T$. Now let $Q = \langle x \rangle$. Then $t$ centralizes $Q$ and $Q^g$ (as subgroups of $GQ$). By Sylow’s theorem, there exists $x \in C_G(t)$ such that $Q^g = Q^x$, and thus $gx^{-1} \in N_G(Q) = C_G(Q) = H$. Since $g \notin H$ we have $x \in C_G(t) \setminus H$, proving that $C_G(t) \neq H$. □
Assume Hypothesis I. For every $\alpha$-invariant proper subgroup $H$ of $G$ we put

$$\theta(H) = [H, \alpha].$$

Let

$$\mathcal{L}(G) = \{ H < G \mid H^\alpha = H \text{ and } \theta(H) \neq 1 \}$$

and denote by $\mathcal{L}^*(G)$ the set of maximal elements of $\mathcal{L}(G)$. Lemma 18 and assumption (d) imply the existence of involutions $t \in G$ such that $C_G(t) \in \mathcal{L}(G)$.

**Lemma 19.** Assume Hypothesis I, and let $L \in \mathcal{L}(G)$.

(i) If $L \leq M \in \mathcal{L}^*(G)$, then $N_G(\theta(L)) = M$, and $M$ is the unique element of $\mathcal{L}^*(G)$ containing $L$; in particular, $N_G(M) = M$.

(ii) If $M \in \mathcal{L}^*(G)$ and $\theta(M) \cap L \neq 1$ then $L \leq M$.

**Proof.** (i) Observe that $\theta(L) \leq \theta(M)$, and so, since every subgroup of a cyclic group is characteristic, $M \leq N_G(\theta(L))$. Now $N_G(\theta(L)) \neq G$ by assumption (d), and so $M = N_G(\theta(L))$, by the maximality of $M$ in $\mathcal{L}(G)$. It is then clear that $M = N_G(M)$ is the unique element of $\mathcal{L}^*(G)$ containing $L$.

(ii) Let $R = \theta(M) \cap L \neq 1$. Then $R = \theta(R) \leq \theta(L)$. Hence $R \leq L$ and so, by assertion (i) we have $L \leq N_G(R) = M$. $\square$

Before we continue the study of implications of Hypothesis I, let us recall some well-known auxiliary facts; proofs are included for convenience. We recall that, for a prime $p$, the $p$-rank of a group $G$ is the largest dimension (as GF($p$)-vector space) of the elementary abelian $p$-subgroups of $G$.

**Lemma 20.** Let $T$ be a Sylow 2-subgroup of the group $G$, and $N$ a normal subgroup of $T$ such that $T/N$ is cyclic. Suppose that $T$ has an involution $t$ such that no $G$-conjugate of $t$ belongs to $N$. Then $O^2(G) \neq G$.

**Proof.** This follows easily from [1, (37.4)]. $\square$

**Lemma 21.** Let $G = O^2(G)$ be a group with 2-rank at least 3. Then every involution of $G$ lies in an elementary abelian 2-subgroup of rank 3.

**Proof.** Let $u$ be an involution of $G$, and assume by contradiction that no elementary abelian 2-subgroup of order 8 contains it. Let $S$ be a Sylow 2-subgroup of $G$ containing $u$. Since $S$ has rank at least 3, it has a normal elementary abelian subgroup $B$ of order 4 (see e.g. [4, Satz 7.6]). Let $C = C_S(B)$. By our assumption, $u$ does not centralize $B$, hence $C$ has index 2 in $S$ and $S = C \langle u \rangle$. Since $O^2(G) = G$, Lemma 20 implies that $u^g \in C$ for some $g \in G$. Thus $u^g$ centralizes $B$ and it easily follows that $u^g$ lies in an elementary abelian 2-group $A$ of rank 3; but then $u \in A^{g^{-1}}$, which is a contradiction. $\square$
Lemma 22. Let $G$ be a 2-group with $A = \Omega_1(Z(G)) \simeq C_2 \times C_2$, and $x$ an automorphism of order 2 of $G$. Suppose that $C_G(x)$ is cyclic. Then $[G, x]$ is cyclic, and $G$ has at most three generators. If, further, $G$ admits an automorphism that moves $\langle z \rangle = C_A(x)$, then $G$ is abelian of rank 2.

**Proof.** Observe that if $z$ is the unique involution in $C_G(x)$, then $z \in Z(G)$. Among all elements of type $[g, x] = g^{-1}g^x$ (with $g \in G$) choose $b$ of maximal order. Then $b_x = b^{-1}$ and $\langle b \rangle \neq G$. If $|b| = 2$, then $b = z$, hence $[G, x] = \langle z \rangle$. The map $g \mapsto [g, x]$ is a homomorphism of $G$ whose kernel is $C_G(x)$, and so $\langle z \rangle \cong G/C_G(x)$. Then $G$ has a maximal cyclic subgroup and the rest of the result follows easily.

Thus, suppose that $|b| \geq 4$. Let $b_1$ be an element of order 4 of $\langle b \rangle$; then $b_1^2 = z$. Since $A = \Omega_1(Z(G)) = \langle a \rangle \times \langle z \rangle$ is $x$-invariant and $\langle z \rangle = A \cap C_G(x)$, we have $a^x = az$. Hence $(ab_1)^x = ab_1^{-1} = ab_1$, and so $c_1 = ab_1$ is an element of order 4 in $C_G(x)$. Observe also that $c_1$ is centralized by $b$. Let $y \in G$, and suppose that $[g, x] \notin \langle b \rangle$. Then there exists an element $y \in \langle [g, x] \rangle$ such that $y \notin \langle b \rangle$ and $y^2 \in \langle b \rangle$.

By choice of $b$ there exists a power $b_0$ of $b$ such that $y^2 = b_0^{-1}$; since $z \in \langle [g, x] \rangle$, we have $|y| \geq 4$. Then

$$(yb_0^{-1})^y = y^{-1}b_0 = yy^{-2}b_0 = yb_0^{-1},$$

so $y = cb_0$ for $c = yb_0^{-1} \in C_G(x)$. Also $c^{b_0} = b_0^{-1}y = b_0b_0^{-1}y = b_0y^{-1} = c^{-1}$. But we observed above that $b_0$ centralizes an element $c_1$ of order 4 of $C_G(x)$. Since $C_G(x)$ is cyclic it follows that $|c| = 2$ and so $c \in \langle b \rangle$, which is a contradiction. Thus $\langle b \rangle = [G, x]$ is cyclic. In particular, $B = [G, x]$ is the set of all elements of the form $[g, x]$, and so it is in one-to-one correspondence with the set of (left) cosets of $G$ modulo $C_G(x)$. Thus $|B| = |G : C_G(x)|$. Since $B \cap C_G(x) = \langle z \rangle$, we have $|C_G(x)B| = |G|/2$. As both $C_G(x)$ and $B$ are cyclic, we get that $G$ is at most three-generated.

Finally, let $W = \text{Aut}(G)$ and assume that some $y \in W$ moves $z$. Then, as $A$ is characteristic in $G$, $W/C_W(A)$ is isomorphic to $S_3$, and so we may suppose that $|y|$ is a power of 3, and $y$ cyclically permutes $a, az$ and $z$. Since $y$ is faithful on $G/\phi(G)$ and $G$ is at most three-generated, we get $|y| = 3$. Then one checks that $y$ acts on $A$ as $[y, x]$ does. Since $x$ is an involution, $x$ inverts $[y, x]$, so we may also suppose that $y$ is inverted by $x$. Then $C_G(y)$ is $x$-invariant and so if $C_G(y) \neq 1$, $x$ fixes some elements of it. But $z$ is the only involution centralized by $x$, and it is moved by $y$; hence $y$ acts fixed-point freely on $G$. Then $G$ is two-generated, because $y$ acts fixed-point freely on $G/\phi(G)$ also. It follows that $G = \langle g, g^y \rangle$ for some $g \in G$, and so $G$ is abelian (of rank 2) by [7].

For a complete treatment of the situation in Lemma 22, we refer to Janko’s paper [6].

Lemma 23. Assume Hypothesis I, and let $T \in \text{Syl}_2(G)$ with $T \leq C_G(x)$. Suppose that $\text{rk}(T) \geq 3$. Then
(1) there exists a unique $M \in \mathcal{L}^*(G)$ such that $T \leq M$;

(2) if $E = \theta(M)$, and $A$ is an elementary abelian subgroup of order 8 of $T$, then $[E, A] = 1$;

(3) there exists an involution $u \in T$ such that $u$ acts as the inversion on $E$.

Proof. (1) By Lemmas 18 and 21, there exists an involution $t$, contained in an elementary abelian subgroup $A$ of order 8 of $T$, such that $C_G(t) \in \mathcal{L}'(G)$; and by Lemma 19 there exists a unique $M \in \mathcal{L}^*(G)$ with $C_G(t) \leq M$. Then $A \leq M$, and for every non-trivial $a \in A$ with $C_{\theta(M)}(a) \neq 1$ we have $C_G(a) \leq M$ by Lemma 19. Let $L \in \mathcal{L}^*(G)$ be such that $A \leq L$; then, since $A$ is elementary abelian of order 8, there exists $a \in A \setminus \{1\}$ such that $C_{\theta(M)}(a) \neq 1$ and $C_{\theta(L)}(a) \neq 1$. But then $C_{\theta(L)}(a) \leq C_G(a) \leq M$, and so, by Lemma 19, $L = M$. Thus $M$ is the unique element of $\mathcal{L}^*(G)$ containing $A$. Let $T_0 = T \cap M$. As $T$ acts by conjugation on $\mathcal{L}^*(G)$, the uniqueness of $M$ (as element of $\mathcal{L}^*(G)$ containing $T_0$) yields $N_T(T_0) \leq T \cap N_G(M) = T \cap M = T_0$, and thus $T = T_0$.

(2) Let $T$ and $M$ be as in (1), and write $E = \theta(M)$. Let $A$ be an elementary abelian subgroup of order 8 of $T$, and $u \in A$. Suppose that $[E, u] \neq 1$. Then, as $E$ is cyclic, there exists a Sylow subgroup $K$ of $E$ (of odd order) such that $K = [K, u]$. Now $T/C_T(K)$ is cyclic and $u \notin C_T(K)$. By Lemma 20 and assumption (d), there exists $g \in G$ such that $u^g \in C_T(K)$. By coprime action, we may take $g \in C_G(x)$: in fact $u \in T^{u^{-1}} \leq C_G(x^u^{-1})$, and so $\langle x \rangle$ and $\langle x \rangle^{g^{-1}}$ are conjugate in $C_G(u)$, thus $g \in C_G(u)C_G(x)$. Hence

$$K = [K, x] \leq [C_G(u^g), x] = [C_G(u), x]^g.$$  

Now $A$ acts on $[C_G(u), x]$ and so (as every subgroup of $[C_G(u), x]$ is cyclic) it acts on $K^{u^{-1}}$; on the other hand, $A \leq M$ and so $A$ acts on $K$. Since $A$ is elementary abelian of order 8, there exists $a \in A \setminus \{1\}$ such that $\langle K^{u^{-1}}, K \rangle \leq C_G(a)$. By Lemma 19 this gives $K^{u^{-1}} \leq M$; hence $K^{u^{-1}} = K$, which is a contradiction.

(3) By assumption (c) there exists an element $g \in G \setminus M$ such that 2 divides $|M \cap M^g|$; hence $M \cap M^g$ contains an involution $t$, and we may assume $t \in T$. If $t$ is not the inversion on $E$, then $C_E(t) \neq 1$, and so $C_G(t) \leq M$. Hence $C_E(t) = 1$, and $t$ acts as the inversion on $E^g$; thus $t^{g^{-1}}$ acts as the inversion on $E$, and by taking a suitable conjugate we get that $T$ has an involution $u$ acting as the inversion on $E$.

Proposition 24. Assume Hypothesis I. Then the Sylow 2-subgroups of $G$ have rank at most 2.

Proof. Let $T$ be a Sylow 2-subgroup of $G$ with $T \leq C_G(x)$ and assume, by contradiction, that $\text{rk}(T) \geq 3$. Let $M$ be the unique element of $\mathcal{L}^*(G)$ containing $T$ and $E = \theta(M) = [M, x]$. Also, write $S = C_T(E)$ and $X = \Omega_1(S)$; observe that $S$ is a Sylow 2-subgroup of $C_M(E)$, and that, by Lemma 23, there exists an involution $u \in T \setminus S$ which acts as the inversion on $E$.  

Unauthenticated
Since \( \text{rk}(T) \geq 3 \), \( T \) has a normal elementary abelian subgroup \( A \) of order 4, and \( |T : C_T(A)| \leq 2 \). Now every involution in \( C_T(A) \) lies in an elementary abelian subgroup of order 8 of \( T \), whence \( \Omega_1(C_T(A)) \leq X \) by Lemma 23; in particular, \( C_T(A) \neq T \) and so \( |T : S| = 2 \).

Recalling that \( u \) is an involution of \( T \) acting as the inversion on \( E \), we have \( T = C_T(A) \langle u \rangle \), and, by Lemma 20, there exists \( g \in G \) such that

\[
u^{g^{-1}} \in \Omega_1(C_T(A)) \leq X.
\]

Then \( g \notin M \), and we may choose \( g \in C_G(x) \) by coprime action; also \( u \) centralizes \( E^g \), and \( C_G(u) \leq M^g \). Thus

\[
C_X(u) \cap C_{M^g}(E^g) = C_G(x) \cap C_G(\langle E, E^g \rangle) = 1.
\]

Therefore, since \( M^g/C_{M^g}(E^g) \) is abelian, \( C_X(u) \) is abelian. It follows that \( C_X(u) \) is cyclic, since, by Lemma 23, \( u \) lies in no elementary abelian subgroup of order 8 of \( T \).

Let \( z \) be the only involution of \( X \) centralized by \( u \). Then clearly \( \langle z \rangle = \Omega_1(Z(T)) \).

In particular, \( A \) is generated by \( z \) and another involution \( a \), and \( a^u = az \). Suppose that there exists \( g \in G \) such that \( a^g = z \). Then \( C_G(z) = C_G(a)^g \leq M^g \) as \( a \) centralizes \( E \), and so \( M^g \leq M \) by uniqueness of \( M \), whence \( g \in M \). In particular, \( A^g \leq C_M(E) \).

Since \( S \in \text{Syl}_2(C_M(E)) \) and \( z \in A^g \), there exists \( h \in C_M(E) \cap C_M(z) \) such that \( A^g \leq S^h \). Then \( A^{gh^{-1}} \leq S \), and since \( a^{gh^{-1}} = z^{-1} = z \), we may assume that \( A^g \leq S \).

Suppose that \( A \neq A^g \). Then, since \( A \leq S \), the product \( AA^g \leq X \) is a group of order 8, and \( A \) normalizes \( A^g = \langle z, z^g \rangle \). If \( AA^g \) is dihedral, then \( (z^g)^a = zz^g \) and so

\[
a^{ugag^{-1}} = (az)^{gag^{-1}} = (zz^g)^{ag^{-1}} = z.
\]

Since \( A \) normalizes \( A^g \), \( a^{g^{-1}} = gag^{-1} \) normalizes \( A \), and so does \( u^{gag^{-1}} \). By replacing \( g \) with \( u^{gag^{-1}} \) we may therefore suppose that \( A = A^g \). If \( AA^g \) is not dihedral, then it is elementary abelian of order 8 and it is not \( u \)-invariant because \( C_X(u) \) is cyclic. Hence \( A^{gu} \neq AA^g \); that is, \( z^{gu} \neq AA^g \). Now \( K = \langle z^{gu}, z^g \rangle \) is dihedral of order at least 8 and contains \( z \), the only involution of \( X \) centralized by \( u \). Hence \( A^{gu} \) and \( A^{gu} \) are elementary abelian subgroups of order 4 of \( K \), and \( N_K(A^{gu}) \neq C_K(A^{gu}) \). It follows that there exists \( b \in N_K(A^{gu}) \) such that \( (z^{gu})^b = zz^g = (az)^g \). Since \( b \) normalizes \( A^{gu} \), \( gb^{-1}g^{-1} \) normalizes \( A \), and so \( g_1 = ugb^{-1}g^{-1} \) normalizes \( A \). As before, \( a^{g_1} = z \), and again, by replacing \( g \) with \( g_1 \), we may suppose that \( g \) normalizes \( A \). Now write \( X_0 = \Omega_1(C_T(A)) \) (then \( A \leq X_0 \leq X \)). Since \( C_T(A) \) is a Sylow 2-subgroup of \( C_M(A) \), we have, by the Frattini argument, \( g \in C_M(A)N_{M^g}(C_T(A)) \). Thus we may choose \( g \) in \( N_M(C_T(A)) \), and therefore \( g \in N_M(X_0) \). But \( X_0 \) is a 2-group with an involutionary automorphism \( u \) whose centralizer is cyclic; Lemma 22 then implies that \( X_0 = \Omega_1(C_T(A)) \) is abelian of rank 2, contradicting the fact that \( C_T(A) \) has rank at least 3. We have thus proved that

\[
z^G \cap A = \{z\}.
\]
We next show that all involutions in \( T \) that act as the inversion on \( E \) are conjugate to \( z \). In fact, it is enough to prove that \( u \) is conjugate to \( z \). By Lemma 20, there exists \( g \in G \) such that \( u^g \in C_T(A) \); note that this forces \( g \notin M \). Then \( u^g \) centralizes \( E \) and so \( C_G(u^g) \leq M \). Since \( z^g \) centralizes \( u^g \), we have \( z^g \in M \), and there exists \( y \in M \) such that \( \langle z^g, u^g \rangle \leq T^y \). Now \( z^g \notin X^y \), for otherwise \( z^g \) centralizes \( E^y = E \) and thus \( E^g = E \) and \( g \in M \). Hence \( C_{X^y}(z^g) \) contains only one involution that must be \( z^y \). On the other hand \( u^g \) centralizes both \( E \) and \( z^y \), and so \( u^g \in X^y \cap C_M(z^g) \). Therefore \( u^g = z^y \), and consequently \( u = z^{3g} \).

Now \( z^g \notin M \) for some \( g \in G \). Otherwise \( U = \langle z \rangle^G \leq M \) and \( U' \neq 1 \) by assumption (d); but \( U' \) centralizes \( E \), and so \( U' \leq Z(G) \), against (d). Consider the dihedral subgroup \( D = \langle z^g, a \rangle \) (recall that \( \langle z, a \rangle = A \)). Since \( z \) and \( a \) are not conjugate in \( G \), \( D \) contains a central involution \( t \). Since \( t \in C_G(a) \leq M \), \( t \) acts on \( E \); if \( C_E(t) \neq 1 \), then \( C_G(t) \leq M \), and we get the contradiction \( z^g \in C_G(t) \leq M \). Thus \( t \) acts as the inversion on \( E \). By what we have proved before, \( t \) is then conjugate to \( z \). Let \( t = z^y \); then, similarly, \( a \) acts as the inversion on \( E^y \) and so \( a \) is conjugate to \( z \). This contradiction finishes the proof of the proposition. \( \square \)

**Theorem 25.** Let \( \alpha \) be an automorphism of odd prime order \( q \) of the group \( G \), and \( (|G|, q) = 1 \). Assume that \( [P, \alpha] \) is cyclic for every \( \alpha \)-invariant Sylow subgroup \( P \) of \( G \) (for every prime). Then \( [G, \alpha] \) is cyclic.

**Proof.** We argue by induction on \( |G| \). The inductive assumption gives that \( [H, \alpha] \) is cyclic for every proper \( \alpha \)-invariant subgroup \( H \) of \( G \). Since, by coprime action, \( [G, \alpha, \alpha] = [G, \alpha] \), we also may suppose that \( G = [G, \alpha] \).

We show that \( G \) is non-abelian simple. Let \( M \) be a minimal normal \( \alpha \)-invariant subgroup of \( G \); then \( G/M = [G, \alpha]M/M = [G/M, \alpha] \) is cyclic by the inductive assumption. Suppose that \( M \neq G \); hence \( [M, \alpha] \) is cyclic. If \( M \leq C_G(\alpha) \), then \( G = [G, \alpha] \leq C_G(M) \), that is, \( M \leq Z(G) \). Thus \( G \) is abelian, and it immediately follows that \( [G, \alpha] \) is cyclic. Therefore, we assume \( M \neq [M, \alpha] \). Since \( [M, \alpha] \leq M \) and \( M \) is minimal normal in \( G \langle \alpha \rangle \), it follows that \( M \) is an elementary abelian \( p \)-group for a prime \( p \), and \( G \) is soluble. If \( G \) is nilpotent there is nothing to prove. Otherwise, let \( H \) be a \( \alpha \)-invariant \( p' \)-Hall subgroup of \( G \); then \( H \cong HM/M \) is cyclic and \( [H, \alpha] = H \). Thus \( H \langle \alpha \rangle \) is a Frobenius group acting on \( M \). Since \( G \) is not nilpotent \( C_M(H) \neq M \). On the other hand, \( HM \leq G \langle \alpha \rangle \) (since \( G/M \) is cyclic), and so we get \( C_M(H) = 1 \) as \( M \) is minimal normal. Therefore, by Lemma 2,

\[
rk(M) = \rk([M, \alpha]) + \rk(C_M(\alpha)) = 1 + \rk(M)/q,
\]

which contradicts \( q > 2 \). Thus we are left with the case \( M = G \). If \( M \) is a \( p \)-group then \( [G, \alpha] \) is cyclic by assumption. Otherwise \( G \) is the direct product of \( s \) copies of a non-abelian simple group, and in particular \( |G| \) is even. Since \( \alpha \) centralizes a Sylow 2-subgroup of \( G \), it follows that \( s = 1 \), and so \( G \) is non-abelian simple.

Suppose now that \( G \) admits a strongly embedded subgroup. Then, by Bender’s theorem ([7, p. 369]), \( G \) is isomorphic to one of the following groups:

- \( \text{PSL}(2, 2^n) \)
- \( \text{Sz}(2^{2n-1}) \)
- \( \text{PSU}(3, 2^n) \)
But none of these groups admits outer automorphisms of coprime order that centralize a Sylow 2-subgroup. In fact (see [2]), outer automorphisms of coprime order of groups of Lie type are field automorphisms, and so they do not centralize a Sylow 2-subgroup, which in all of these cases is a unipotent radical.

Thus the pair \((G, x)\) satisfies Hypothesis I. Then, by Proposition 24 and the classification of simple groups with Sylow 2-subgroups of rank 2, we have that \(G\) is isomorphic to one of the following groups:

\[
\text{PSL}(2, r), \text{PSL}(3, r), \text{PSU}(3, r) \text{ with } r \text{ odd; } A_7, M_{11}, \text{PSU}(3, 4).
\]

Now \(A_7, M_{11}\) and \(\text{PSU}(3, 4)\) do not admit automorphisms of coprime order. For the other cases let \(r = p^m\) with \(p\) an odd prime. Then \(x\) is induced by an automorphism of the field \(GF(p^m)\), and so \(q|m\). If \(U\) is a \(x\)-invariant Sylow \(p\)-subgroup of \(G\), then \(U\) is a unipotent radical of \(G\), and it has order \(p^m\) or \(p^{3m}\), nilpotency class at most 2, and exponent \(p\). Thus if \(|U, x|\) is cyclic, then \(|U, x| = p\). But then \(|C_U(x)| = |U|/p\) and this cannot be the case, since \(|C_U(x)|\) is equal to the order of the corresponding unipotent radical over the fixed-point field \(GF(p^m/q)\) for \(x\), and \(q > 2\).

\[\square\]

**Remarks.** (1) The conclusion of the theorem is not true for \(q = 2\). For instance, let \(p\) be a prime with \(p \equiv -1 \pmod{3}\), and let the group \(S_3\) act faithfully (and irreducibly) on an elementary abelian group \(M\) of order \(p^2\). Let \(A\) be the subgroup of order 3 in \(S_3\) and \(x\) an involution of \(S_3\). Then \(x\) acts on the odd order group \(G = MA\), fixing the Sylow subgroups \(A\) and \(M\). We have that \(A = [A, x]\) and \([M, x]\) are cyclic, while \(G = [G, x]\) is not.

(2) The theorem has been stated and proved for \(|x|\) an odd prime, but an easy induction shows that it holds for \(|x|\) odd and \(||G|, x| = 1\) (in fact this is Theorem 1).

**Acknowledgement.** The author is grateful to B. Stellmacher for suggesting an approach to the proof of Theorem 1 which is independent of the classification of finite simple groups. The author is also indebted to S. Dolfi for many conversations on the subject of this paper.

**References**


Received 25 February, 2009

Carlo Casolo, Dipartimento di Matematica “Ulisse Dini”, Università di Firenze, 50134 Firenze, Italy
E-mail: casolo@mail.math.unifi.it