ISRAEL JOURNAL OF MATHEMATICS **126** (2001), 345–362

DERIVED SUBGROUPS OF FIXED POINTS

BY

ROBERT GURALNICK*

Department of Mathematics, University of Southern California
Los Angeles, CA 90089-1113, USA
e-mail: guralnic@math.usc.edu

AND

PAVEL SHUMYATSKY**

Department of Mathematics, University of Brasilia
Brasilia-DF, 70910-900 Brazil
e-mail: pavel@ipe.mat.unb.br

ABSTRACT

Let A be an elementary abelian q-group acting on a finite q'-group G. We show that if A has rank at least 3, then properties of $C_G(a)', 1 \neq a \in A$ restrict the structure of G'. In particular, we consider exponent, order, rank and number of generators.

1. Introduction

Let q be a prime, and A be an elementary abelian q-group acting on a finite q'-group G. It has been known for some time that if $C_G(a)$ satisfies certain "smallness" conditions for each $a \in A^{\#}$ then the whole group G has a similar property. To exemplify this we cite the following results.

The first result is a celebrated theorem of Thompson [19].

1. If A is cyclic and $C_G(A) = 1$, then G is nilpotent.

---

* This author was supported by the NSF.

** This author was supported by CNPq-Brazil.

Received April 6, 2000

The next result is an easy consequence of the classification of finite simple groups [20]. There is a somewhat more precise version of the result, but note that it is not true that if A is cyclic and $C_G(A)$ is solvable, then G is solvable (consider $L_2(2^q)$).

2. If B is a group of automorphisms of G whose order is coprime to that of G and $C_G(B)$ is nilpotent or has odd order, then G is solvable.

For the rest of the paper, we assume that A is noncyclic.

Let m be a positive integer.

3. If $C_G(a)$ has order at most m for each $a \in A^{\#}$ then the order of G is at most m^{q+1}.

This follows from the well-known facts that A normalizes some Sylow p-subgroup of G for any $p \in \pi(G)$ and if G is a p-group then $G = \prod_{a\in A^{\#}} C_G(a)$ ([6, Theorem 6.2.2, Theorem 5.3.16]). We also use that if A is of rank 2 then it has exactly $q+1$ cyclic subgroups.

Recall that the rank of a finite group is the maximum number of generators required for any subgroup.

4. If $C_G(a)$ has rank at most m for each $a \in A^{\#}$ then the rank of G is $\{m, q\}$-bounded.

This can be shown as follows. Let P be any A-invariant Sylow p-subgroup of G and H any A-invariant subgroup of P. Since $H = \prod_{a\in A^{\#}} C_H(a)$, we conclude that H is generated by at most $d = m(q+1)$ elements. Let V be the intersection of kernels of all homomorphisms of P into $\mathrm{GL}_d(F)$, where F is the field with p elements. Set $W = V$ if p is odd and $W = V^2$ if $p = 2$. Then any characteristic d-generated subgroup of P contained in W is powerful [3, Proposition 2.12]. Since the Sylow p-subgroups of $\mathrm{GL}_d(F)$ are nilpotent of class $d-1$, it follows that $\gamma_d(P) \leq V$. We know that $\gamma_d(P)$ is d-generated so the image of $\gamma_d(P)$ in P/W has order at most 2^d. Therefore P/W is nilpotent of class at most $2d-1$ whence $\gamma_{2d}(P) \leq W$. Since $\gamma_{2d}(P)$ has at most d generators, it becomes clear that $\gamma_{2d}(P)$ is powerful. Thus we conclude that $\gamma_{2d}(P)$ has rank at most d [3, Theorem 2.9]. Since P has at most d generators, the rank of $P/\gamma_{2d}(P)$ is d-bounded. Then so is the rank of P. Let r be the maximum of ranks of Sylow p-subgroups of G, where p ranges through $\pi(G)$. Since A normalizes some Sylow p-subgroup of G for any $p \in \pi(G)$, it follows that r is $\{m, q\}$-bounded. But the rank of G is at most $r+1$ [10, 7, 14] and we are done.

5. If $C_G(a)$ has exponent at most m for each $a \in A^{\#}$ then the exponent of G is $\{m, q\}$-bounded.

This was proved in [9].

In this paper we impose conditions on the derived groups of $C_G(a)$ and investigate the effect on the structure of G'.

THEOREM 1.1: *Let m be an integer, q a prime. Let G be a finite q'-group acted on by an elementary abelian group A of order q^3. Assume that $C_G(a)$ has derived group of order at most m for each $a \in A^\#$. Then the order of G' is $\{m, q\}$-bounded.*

THEOREM 1.2: *Let m be an integer, q a prime. Let G be a finite q'-group acted on by an elementary abelian group A of order q^3. Assume that $C_G(a)$ has derived group of rank at most m for each $a \in A^\#$. Then the rank of G' is $\{m, q\}$-bounded.*

THEOREM 1.3: *Let m be an integer, q a prime. Let G be a finite q'-group acted on by an elementary abelian group A of order q^3. Assume that $C_G(a)$ has derived group of exponent dividing m for each $a \in A^\#$. Then the exponent of G' is $\{m, q\}$-bounded.*

Each of the above theorems fails if $|A| = q^2$. Indeed, let G be a finite q'-group admitting a non-cyclic automorphism group A of order q^2 such that $C_G(a)$ is abelian for each $a \in A^\#$. Ward showed that G is necessarily solvable [23]. The second author proved that if G has derived length k then G' is nilpotent of class bounded by some function of q and k [17]. However the derived length k can be arbitrarily large. For instance, for any odd prime p Khukhro constructed a p-group G of derived length bigger than $\log_2(p-1)$ acted on by a four-group A such that $C_G(a)$ is abelian for each $a \in A^\#$ [8, pp. 149–150]. Thus Theorems 1.1 and 1.3 fail in the case $|A| = q^2$. Direct products of such groups show that in this case G' can have arbitrarily large rank. So the assumption that $|A| = q^3$ is essential in each of the above theorems. This seems to be a part of a more general phenomenon: if a certain property of $C_G(a)$ for all $a \in A^\#$ implies a similar property for the whole group G then the property of $C_G(a)'$ for all $a \in A^\#$ implies a similar property for G' provided that the rank of A increases by 1. To illustrate this we mention the following results of Ward: if $|A| = q^3$ and $C_G(a)$ is nilpotent for each $a \in A^\#$ then G is likewise nilpotent [21]; if $|A| = q^4$ and $C_G(a)'$ is nilpotent for each $a \in A^\#$ then G' is nilpotent [22]. Both of these results have been extended in [16] to the case where G is allowed to be periodic solvable.

It is also worth noting that proofs of the results 3–5 mentioned above reduce very easily to the case of p-groups. This is no longer true for the results in this paper. We need to prove the following result of independent interest:

THEOREM 1.4: *Let q be a prime. Let G be a finite q'-group acted on by an elementary abelian group A of order q^3. Let P be an A-invariant Sylow subgroup of G. Then $P \cap G' = \langle P \cap C_G(a)' | a \in A^{\#} \rangle$.*

Our proof of this result involves the classification of finite simple groups. The fact we use is that any group of coprime automorphisms of a finite simple group is cyclic. Once Theorem 1.4 is proved we deal with the case of p-groups using Lie methods. The techniques developed by Zelmanov in his solution of the Restricted Burnside Problem are particularly helpful.

2. Preliminaries

The first two lemmas are well-known (see for example [6, 6.2.2, 6.2.4]).

LEMMA 2.1: *Let A be a group of automorphisms of the finite group G with $(|A|, |G|) = 1$.*

1. *If N is any A-invariant normal subgroup of G we have $C_{G/N}(A) = C_G(A)N/N$;*
2. *If H is an A-invariant p-subgroup of G, then H is contained in an A-invariant Sylow p-subgroup of G;*
3. *$C_G(A)$ is transitive on the set of A-invariant Sylow p-subgroups of G;*
4. *If P is an A-invariant Sylow p-subgroup of G, then $C_P(A)$ is a Sylow p-subgroup of $C_G(A)$.*

LEMMA 2.2: *Let q be a prime, G a finite q'-group acted on by an elementary abelian q-group A of rank at least 2. Let $A_1, \ldots, A_s$ be the maximal subgroups of A. If H is an A-invariant subgroup of G we have $H = \langle C_H(A_1), \ldots, C_H(A_s) \rangle$.*

LEMMA 2.3: *Let q be a prime, G a finite q'-group acted on by an elementary abelian q-group A of rank at least 3. If N is any A-invariant normal subgroup of G then $[N, G] = \langle [C_N(a), C_G(a)] | a \in A^{\#} \rangle$. If $[N, G]$ is nilpotent then $[N, G] = \prod [C_N(a), C_G(a)]$, where the product is taken over all $a \in A^{\#}$.*

Proof: Let $A_1, \ldots, A_s$ be the maximal subgroups of A. By Lemma 2.2, $G = \langle C_G(A_1), \ldots, C_G(A_s) \rangle$ and $N = \langle C_N(A_1), \ldots, C_N(A_s) \rangle$. Consider the subgroup $R = \langle [C_N(A_i), C_G(A_j)] | 1 \leq i, j \leq s \rangle$. Obviously R is A-invariant so $R = \langle C_R(A_1), \ldots, C_R(A_s) \rangle$. To show that R is normal it is sufficient to establish that $y^x \in R$ for any $y \in C_R(A_i)$ and $x \in C_G(A_j)$. We have $y^x = y^x y^{-1} y$ and obviously both $y^x y^{-1}$ and y belong to R. Hence $y^x \in R$ and R is normal. Using that $G = \langle C_G(A_1), \ldots, C_G(A_s) \rangle$ and $N = \langle C_N(A_1), \ldots, C_N(A_s) \rangle$ it is now easy to see that the image of N in G/R is central whence $R = [N, G]$. Since the intersection $A_i \cap A_j$ cannot be trivial (the rank of A is at least 3), it follows that any subgroup of the form $[C_N(A_i), C_G(A_j)]$ is contained in $[C_N(a), C_G(a)]$ for some $a \in A^\#$ so that $[N, G] = \langle [C_N(a), C_G(a)] | a \in A^\# \rangle$.

Assume now that $[N, G]$ is nilpotent of class c. If $[N, G]$ is abelian then the factorization $[N, G] = \prod [C_N(a), C_G(a)]$ is immediate so we assume that $c \geq 2$ and use induction on c. Set

$$M = \underbrace{[[N, G], \ldots, [N, G]]}_{c-1}.$$

Then $[M, [N, G]]$ is central in $[N, G]$. Let $\bar{H}$ denote the image of any subgroup H of G in $G/[M, [N, G]]$. By the inductive hypothesis $[\bar{N}, \bar{G}] = \prod [C_{\bar{N}}(a), C_{\bar{G}}(a)]$. Since $[M, [N, G]]$ is abelian, it is clear that

$$[M, [N, G]] = \prod [C_M(a), [C_N(a), C_G(a)]].$$

Using that each subgroup $[C_M(a), [C_N(a), C_G(a)]]$ is central in $[N, G]$, the result follows. ∎

COROLLARY 2.4: *Assume the hypothesis of the previous lemma. If G' is nilpotent then $G' = \prod C_G(a)'$, where the product is taken over all $a \in A^\#$.*

LEMMA 2.5: *Let G be a finite group and N a normal perfect subgroup. Let P be a Sylow p-subgroup of G. Let $R = P \cap N$ and $H = N_G(R)$. Then $P \cap G' = R(P \cap H')$.*

Proof: By the Frattini argument, $G = HN$ and so $G' = H'N$. Thus, $H \cap G' = H'(H \cap N)$. Hence $H'R$ contains a Sylow p-subgroup of $H \cap G'$. Since $H'R$ is normal in $H \cap G'$, this implies it contains every Sylow p-subgroup of $H \cap G'$. In particular, $P \cap G' = P \cap H'R = (P \cap H')R$. ∎

Let $d(H)$ denote the minimal size of a generating set for H. Let the rank of H be the maximum of $d(K)$ as K ranges over all subgroups K.

The following result is an immediate consequence of a result obtained independently by the first author [7] and Lucchini [14]. It depends on the classification of finite simple groups. The result for solvable groups was obtained by Kovács [10].

THEOREM 2.6: *Let G be a finite group.*

(a) $d(G) \leq 1 + \max_p\{d(P)|\ P$ *a Sylow p-subgroup of* $G\}$.

(b) $\mathrm{rank}(G) \leq 1 + \max_p\{\mathrm{rank}(P)|\ P$ *a Sylow p-subgroup of* $G\}$.

Proof: The theorem cited above is precisely (a). Applying this to every subgroup proves (b). ∎

We need one further result that is dependent upon the classification of finite simple groups.

LEMMA 2.7: *Let S be a finite simple group and T a group of automorphisms of S with $(|T|, |S|) = 1$. Then T is cyclic.*

Proof: If S is alternating or sporadic, then $\mathrm{Out}(S)$ has order dividing 4, and $|S|$ has even order.

If S is a Chevalley group, then $\mathrm{Out}(S)$ has a normal series $N_1 < N_2 < \mathrm{Out}(S)$ with N_1 consisting of diagonal automorphisms, N_2/N_1 cyclic (corresponding to field automorphisms) and with the final quotient being the group of graph automorphisms. Only, N_2/N_1 can be divisible by primes not dividing $|S|$. Thus, T embeds in N_2/N_1 and is cyclic. ∎

We point out some easy consequences of the previous result. See [20]. We will not be using these results in the remainder of the article.

COROLLARY 2.8: *Let A be a group of automorphisms of the finite group G with $(|G|, |A|) = 1$.*

1. *If $C_G(A)$ is solvable and has no section isomorphic to S_3, A_4 or* $\mathrm{Sz}(2)$, *then G is solvable;*
2. *If A is not cyclic of prime power order and $C_G(a)$ is solvable for all $a \in A^{\#}$, then G is solvable.*

Proof: The first statement follows by an elementary standard reduction argument. Taking G to be minimal, we may assume that G is a direct product of simple groups and that A acts transitively on the simple direct factors. If B is the normalizer of one of the factors L, then $C_G(A) \cong C_L(B)$ and so we are reduced to the case that G is simple. It follows that A is a cyclic group of field automorphisms. The only cases where $C_A(G)$ is solvable is when $G = L_2(r^e)$ with $r = 2$ or 3, $U_3(2^e)$ or $\mathrm{Sz}(2^e)$ and A is the full group of field automorphisms. Inspection of these cases yields the result.

We now prove the second statement. Let G be a minimal counterexample. Let N be a minimal normal A-invariant subgroup of G. If N is solvable, we may pass to G/N. So N is a direct product of simple groups and A permutes the simple direct factors transitively. Thus, $G = N$.

Let L be one of the factors. Suppose that $a \in A$ has prime order q and does not normalize L. Then $L \cong \{xx^a \cdots x^{a^{q-1}} \mid x \in L\} \leq C_G(a)$ is not solvable. So every element of prime order fixes L (and each A-conjugate of L). By the simple case, we see that $N_A(L)$ must be cyclic of prime order q (because for any proper subgroup of $N_A(L)$, the centralizer would not be solvable). It follows that A is a q-group and is either cyclic (q odd) or generalized quaternion (if $q = 2$). Since we are assuming that A is not cyclic of prime power order and has order relatively prime to $|L|$, we have a contradiction. ∎

The second part of the previous result can be proved without the classification if A is abelian of rank 3 by results on solvable signalizer functors. See [4], [5], [2].

3. A generation result

Throughout this section, let G be a finite group and A an elementary abelian q-group of order q^e, q a prime not dividing the order of G.

Our goal is to prove Theorem 1.4 which we restate for convenience.

THEOREM 3.1: *Assume $e \geq 3$. Let P be an A-invariant Sylow subgroup of G; then $P \cap G' = \langle C_G(a)' \cap P \mid a \in A^\# \rangle$.*

Before we prove Theorem 1.4, we note some easy consequences including the proof of Theorem 1.1.

COROLLARY 3.2: *Assume $e \geq 3$. Let P be an A-invariant Sylow subgroup of G; then $P \cap G' = \langle [x, y] \in P \mid x \in C_P(a), y \in C_G(a), a \in A^\# \rangle$.*

Proof: This follows from the theorem and the Focal Subgroup Theorem [6] which describes $P \cap C_G(a)'$. ∎

COROLLARY 3.3: *Assume $e \geq 3$. Then $\pi(G') = \bigcup_{a \in A^\#} \pi(C(a)')$.*

COROLLARY 3.4: *If $e \geq 3$, then $G' = \langle C_G(a)' \mid a \in A^\# \rangle$.*

Since a rank 3 elementary abelian q-group has $q^2 + q + 1$ nontrivial cyclic subgroups, the next result follows immediately.

COROLLARY 3.5: *If $e \geq 3$ and $C_G(a)'$ can be generated by at most m elements for each nontrivial $a \in A$, then G' can be generated $m(q^2 + q + 1)$ elements.*

We can now prove a somewhat more precise version of Theorem 1.1. Note that there is an analogous result for the order of a Sylow p-subgroup of G' in terms of the maximal order of a Sylow p-subgroup of $C_G(a)'$.

THEOREM 3.6: *Let m be an integer, q a prime. Let G be a finite q'-group acted on by an elementary abelian group A of order q^3. Assume that $C_G(a)$ has derived group of order at most m for each $a \in A^{\#}$. Then $|G'| \le m^{2(q^2+q+1)}$.*

Proof: Let P be an A-invariant Sylow p-subgroup of G. Let Δ denote the set of nontrivial cyclic subgroups of A. For each $B \in \Delta$, let $m_B = |C_G(B)'|$ and $m_B(p)$ be the order of the Sylow p-subgroup of $C_G(B)'$. By Lemma 2.1, $m_B(p) = |P \cap C_G(B)'|$.

By Lemma 2.3, $|P'| \le \prod_{B\in\Delta} m_B(p)$. By Theorem 3.1,

$$|P \cap G'| \le |P'| \prod_{B\in\Delta} m_B(p) \le \prod_{B\in\Delta} m_B(p)^2.$$

Thus,

$$|G'| \le \prod_{p,B\in\Delta} m_B(p)^2 \le \prod_B m_B^2 \le m^{2(q^2+q+1)}. \qquad \blacksquare$$

In order to prove the other main theorems, we will need to consider the p-group case more closely.

We now prove the theorem. We first handle the case of direct products of simple groups. Let H^∞ denote the final term in the derived series for H.

LEMMA 3.7: *Assume that G is a direct product of nonabelian simple groups. Let P be an A-invariant Sylow p-subgroup of G. If $e > 2$, then*

$$P = \langle C_G(a)^\infty \cap P | \, a \in A^{\#} \rangle.$$

Proof: We may assume that A is transitive on the direct factors of G. Consider the stabilizer of one these factors L. If this stabilizer has order at least q^2, then as the Sylow q-subgroup of $\mathrm{Aut}(L)$ is cyclic by Lemma 2.7, it follows that there is a nontrivial subgroup A_0 of A which centralizes L. Since A is abelian, A_0 centralizes L^a for all $a \in A$. Since A is transitive on the direct factors of G, this implies that A_0 centralizes G, whence the result is clear.

So there exists a subgroup B of A of order q^2 which fixes no direct factor $L^a, a \in A$. Let H be the direct product of these q^2 factors. We will show that $P \cap H = \langle P \cap C(a)^\infty | \, a \in B^{\#} \rangle$ which implies the result.

Identifying the various direct factors by the action of B, we may assume that B acts by permuting the coordinates of the q^2 copies of L. Then we see that for

$1 \neq a \in B$, $C_H(a)$ is just q copies of L (one copy for each a-orbit). In particular, $C_H(a)$ is perfect.

By Lemma 2.2, we know that

$$P \cap H = \langle P \cap C(a) | \, a \in B^{\#} \rangle = \langle P \cap C(a)^{\infty} | a \in B^{\#} \rangle. \qquad \blacksquare$$

We now complete the proof of Theorem 3.1.

Proof of Theorem 3.1: Set $B = \langle C_G(a)' \cap P | \, a \in A^{\#} \rangle$. Clearly, $P \cap G' \geq B$. So we only need the opposite inclusion.

Let G be a counterexample of minimal order.

If $G' = 1$, there is nothing to prove. Let N be a normal subgroup of G which is A-invariant and which is minimal with respect to these properties. So N is characteristically simple.

By Lemma 2.1, $C_{G/N}(a)' = C(a)'N/N$. Thus, by minimality $PN \cap G' = \langle C(a)'N \cap PN | \, a \in A^{\#} \rangle$. Since a has order prime to $|G|$, it follows that $C(a)'N \cap P \leq C_P(a)N$. It also follows that $C_P(a)$ is a Sylow p-subgroup of $C(a)$ and so $P \cap C(a)'$ is a Sylow p-subgroup of $C(a)'$.

First suppose that N is a p'-group. Thus, $P \cap C(a)'$ is a Sylow p-subgroup of $C(a)'N$ and so $PN \cap C(a)'N = (P \cap C(a)')N$. So

$$PN \cap G' = \langle (C(a)' \cap P)N | \, a \in A^{\#} \rangle = BN,$$

whence $P \cap G' = B$.

Next suppose that N is perfect and $R := P \cap N$ is nontrivial. Let $H = N_G(R)$. Then H is a proper subgroup of G and is A-invariant. So by minimality, $P \cap H' \leq B$. By Lemma 2.5, $P \cap G' = (P \cap H')R$. By the previous result, $R \leq B$ and so $P \cap G' \leq B$ as required.

So we may assume that N is a p-group and so is contained in P. Indeed, it follows that every minimal normal subgroup is a p-group. Moreover, we may assume that N is contained in G' (otherwise $G' = 1$ and there is nothing to prove).

Thus, $PN \cap C(a)'N = (P \cap C(a)')N$ and $(P \cap G') \leq B(P \cap N)$. So it suffices to prove that $N \leq B$.

If N is not central in G, then by Lemma 2.3,

$$N = [N, G] = \langle [C_N(a), C_G(a)] | \, a \in A^{\#} \rangle \leq B$$

and the result holds.

If G is not perfect and $G'' \neq 1$, then we may choose $N \leq G''$. By minimality, $N \leq B$ and the result follows.

If $G'' = 1$, then G' is an abelian p-group. Then Lemma 2.3 implies that $P \cap G' = G' = \prod_a [C_G(a), C_G(a)] \leq B$.

So we are reduced to the case that G is perfect.

If $N \leq \Phi(P)$, the Frattini subgroup of P, then $P = P \cap G' = B\Phi(P) = B$ as required.

If N is not disjoint from $\Phi(P)$, then we can choose an A-invariant complement to $N \cap \Phi(P)$ in N, contradicting the minimality of N.

Now choose $Z \leq N$ of order p. Since Z is not contained in the Frattini subgroup of P, it follows that $P = Z \times M$ for some maximal subgroup M of P; i.e. the sequence

$$1 \to Z \to P \to P/Z \to 1$$

splits.

Consider the sequence

$$1 \to Z \to G \to G/Z \to 1.$$

This corresponds to an element $\beta \in H^2(G/Z, Z)$. The fact that the sequence above splits indicates that $\beta = 0$ in $H^2(P/Z, Z)$. Since P/Z is a Sylow p-subgroup of G/Z, the restriction mapping from $H^2(G/Z, Z)$ to $H^2(P/Z, Z)$ is injective and so $\beta = 0$ in $H^2(G/Z, Z)$, whence Z is complemented in G. This implies that Z is not contained in G', a contradiction, since $Z \leq N \leq G'$. ∎

4. Some Lie-theoretic machinery

Let L be a Lie algebra over a field $\mathfrak{k}$. Let k, n be positive integers and let $x_1, x_2, \ldots, x_k, x, y$ be elements of L. We define inductively

$$[x_1] = x_1; \quad [x_1, x_2, \ldots, x_k] = [[x_1, x_2, \ldots, x_{k-1}], x_k]$$

and

$$[x, {}_0 y] = x; \quad [x, {}_n y] = [[x, {}_{n-1} y], y].$$

An element $a \in L$ is called ad-nilpotent if there exists a positive integer n such that $[x, {}_n a] = 0$ for all $x \in L$. If n is the least integer with the above property then we say that a is ad-nilpotent of index n. Let $X \subseteq L$ be any subset of L. By a commutator in elements of X we mean any element of L that can be obtained as a Lie product of elements of X with some system of brackets. Denote by F the free Lie algebra over $\mathfrak{k}$ on countably many free generators $x_1, x_2, \ldots$. Let $f = f(x_1, x_2, \ldots, x_n)$ be a non-zero element of F. The algebra L is said to satisfy the identity $f \equiv 0$ if $f(a_1, a_2, \ldots, a_n) = 0$ for any $a_1, a_2, \ldots, a_n \in L$. In this case we say that L is PI. A deep result of Zelmanov says that if a Lie algebra L is PI and is generated by finitely many elements all commutators in which are ad-nilpotent, then L is nilpotent [25, III(0.4)]. Using this and some routine universal arguments, the next theorem can be deduced (see [9]).

THEOREM 4.1: *Let L be a Lie algebra over a field $\mathfrak{k}$ generated by $a_1, a_2, \ldots, a_m$. Assume that L satisfies an identity $f \equiv 0$ and that each commutator in the generators $a_1, a_2, \ldots, a_m$ is ad-nilpotent of index at most n. Then L is nilpotent of $\{f, n, m, \mathfrak{k}\}$-bounded class.*

An important criterion for a Lie algebra to be PI is the following

THEOREM 4.2 (Bahturin–Linchenko–Zaicev): *Let L be a Lie algebra over a field $\mathfrak{k}$. Assume that a finite group A acts on L by automorphisms in such a manner that $C_L(A)$, the subalgebra formed by fixed elements, is PI. Assume further that the characteristic of $\mathfrak{k}$ is either 0 or prime to the order of A. Then L is PI.*

This theorem was proved by Bahturin and Zaicev for solvable groups A [1] and extended by Linchenko to the general case [12].

COROLLARY 4.3 ([18]): *Let F the free Lie algebra of countable rank over $\mathfrak{k}$. Denote by F^* the set of non-zero elements of F. For any finite group A there exists a mapping*

$$\phi\colon F^* \to F^*$$

such that if L and A are as in Theorem 4.2, and if $C_L(A)$ satisfies an identity $f \equiv 0$, then L satisfies the identity $\phi(f) \equiv 0$.

The following lemma is quite helpful.

LEMMA 4.4 ([9]): *Suppose that L is a Lie algebra, K a subalgebra of L generated by r elements $h_1, \ldots, h_r$ such that all commutators in the h_i are ad-nilpotent in L of index t. If K is nilpotent of class c, then for some $\{r, t, c\}$-bounded number u we have*

$$[L, \underbrace{K, \ldots, K}_{u}] = 0.$$

We now turn to groups. Throughout the rest of the section p will denote an arbitrary but fixed prime. Let G be any group. A series of subgroups

$$(*) \qquad G = G_1 \geq G_2 \geq \cdots$$

is called an N_p-series if $[G_i, G_j] \le G_{i+j}$ and $G_i^p \le G_{pi}$ for all i, j. To any N_p-series $(*)$ of a group G one can associate a Lie algebra $L^*(G)$ over $\mathbb{F}_p$, the field with p elements. Let us briefly describe the construction.

Given an N_p-series $(*)$, let us view the quotients $L_i^* = G_i/G_{i+1}$ as linear spaces over $\mathbb{F}_p$, and let $L^*(G)$ be the direct sum of these spaces. Commutation in G induces a binary operation $[,]$ in L. For homogeneous elements $xG_{i+1} \in L_i^*, yG_{j+1} \in L_j^*$ the operation is defined by

$$[xG_{i+1}, yG_{j+1}] = [x, y]G_{i+j+1} \in L_{i+j}^*$$

and extended to arbitrary elements of $L^*(G)$ by linearity. It is easy to check that the operation is well-defined and that $L^*(G)$ with the operations $+$ and $[,]$ is a Lie algebra over $\mathbb{F}_p$.

We are now concerned with the relationship between G and $L^*(G)$. For any $x \in G_i \setminus G_{i+1}$ let x^* denote the element xG_{i+1} of $L^*(G)$.

PROPOSITION 4.5 (Lazard, [11]): *For any $x \in G$ we have $(ad\, x^*)^p = ad\,(x^p)^*$. Consequently, if x is of finite order p^t then x^* is ad-nilpotent of index at most p^t.*

Let Fr denote the free group on free generators $x_1, x_2, \ldots$, and choose a non-trivial element $w = w(x_1, x_2, \ldots, x_s) \in Fr$. We say that a group G satisfies the identity $w \equiv 1$ if $w(g_1, g_2, \ldots, g_s) = 1$ for any $g_1, g_2, \ldots, g_s \in G$. The following proposition can be deduced from the proof of Theorem 1 in the paper of Wilson and Zelmanov [24]

PROPOSITION 4.6: *Let G be a group satisfying an identity $w \equiv 1$. Then there exists a non-zero multilinear Lie polynomial f over $\mathbb{F}_p$ depending only on p and w such that for any N_p-series $(*)$ of G the algebra $L^*(G)$ satisfies the identity $f \equiv 0$.*

In fact Wilson and Zelmanov describe in [24] an effective algorithm allowing one to write f explicitly for any p and w, but we do not require this.

In general a group G has many N_p-series. The series described below is particularly important. To simplify the notation we write γ_i for $\gamma_i(G)$. Set $D_i = D_i(G) = \prod_{jp^k \ge i} \gamma_j^{p^k}$. The subgroups D_i form an N_p-series $G = D_1 \ge D_2 \ge \cdots$ in the group G. This is known as the Jennings–Lazard–Zassenhaus series.

Let $DL(G) = \bigoplus L_i$ be the Lie algebra over $\mathbb{F}_p$ corresponding to the Jennings–Lazard–Zassenhaus series of G. Here $L_i = D_i/D_{i+1}$. Let $L_p(G) = \langle L_1 \rangle$ be the subalgebra of $DL(G)$ generated by L_1. The proof of the following lemma can be found in [9].

LEMMA 4.7: *Suppose that X is a d-generator finite p-group such that the Lie algebra $L_p(X)$ is nilpotent of class c. Then X has a powerful characteristic subgroup of $\{p,c,d\}$-bounded index.*

Recall that powerful p-groups were introduced by Lubotzky and Mann in [13]: a finite p-group G is powerful if and only if $G^p \geq [G,G]$ for $p \neq 2$ (or $G^4 \geq [G,G]$ for $p = 2$). These groups have many nice properties, so that often a problem becomes much easier once it is reduced to the case of powerful p-groups. The above lemma is quite useful as it allows us to perform such a reduction.

Given a subgroup H of the group G, we denote by $L(G,H)$ the linear span in $DL(G)$ of all homogeneous elements of the form hD_{j+1} where $h \in D_j \cap H$. Clearly, $L(G,H)$ is always a subalgebra of $DL(G)$. Moreover, it is isomorphic with the Lie algebra associated with H using the N_p-series of H formed by $H_j = D_j \cap H$. We also set $L_p(G,H) = L_p(G) \cap L(G,H)$. Let α be any automorphism of the group G. Then α acts naturally on every quotient of the Jennings–Lazard–Zassenhaus series of G. This action induces an automorphism of the Lie algebra $DL(G)$. So when convenient we will consider α as an automorphism of $DL(G)$ (or of $L_p(G)$). Lemma 2.1 implies that if G is finite and $(|G|,|\alpha|) = 1$ then $L_p(G, C_G(\alpha)) = C_{L_p(G)}(\alpha)$.

LEMMA 4.8: *Suppose that any Lie commutator in homogeneous elements $x_1,\ldots,x_r$ of $DL(G)$ is ad-nilpotent of index at most t. Let $K = \langle x_1,\ldots,x_r\rangle$ and assume that $K \leq L(G,H)$ for some subgroup H of G satisfying a group identity $w \equiv 1$. Then for some $\{r,t,w,p\}$-bounded number u we have*

$$[DL(G), \underbrace{K,\ldots,K}_{u}] = 0.$$

Proof: In view of Lemma 4.4 it is sufficient to show that K has $\{r,t,w,p\}$-bounded nilpotency class. We know from Proposition 4.6 that K satisfies certain multilinear polynomial identity depending only on w. Thus Theorem 4.1 shows that K has $\{r,t,w,p\}$-bounded nilpotency class. ∎

5. Proofs of main results

Proof of Theorem 1.2: Suppose that we have proved the result for p-groups. Choose an A-invariant Sylow p-subgroup P of G. Then P' has bounded rank. Since $P \cap G'$ has a bounded number of generators by Theorem 1.4 (in terms of q and m), it follows that $P \cap G'$ has rank bounded in terms of m and q. Then, by Theorem 2.6, the result holds for all groups (with the bound increased by 1).

So we assume that G is a p-group. By Lemma 2.3, if N is any normal A-invariant subgroup of G we have $[N,G] = \prod[C_N(a), C_G(a)]$. Therefore $[N,G]$ has at most $d = m(q^2+q+1)$ generators. In particular we conclude that any term of the lower central series of G (except possibly G) has at most d generators. Let V be the intersection of kernels of all homomorphisms of G into $\mathrm{GL}_d(F)$, where F is the field with p elements. Set $W = V$ if p is odd and $W = V^2$ if $p = 2$. Then any characteristic d-generated subgroup of G contained in W is powerful [3, Proposition 2.12]. Since the Sylow p-subgroups of $\mathrm{GL}_d(F)$ are nilpotent of class $d-1$, it follows that $\gamma_d(G) \leq V$. We know that $\gamma_d(G)$ is d-generated so the image of $\gamma_d(G)$ in G/W has order at most 2^d. Therefore G/W is nilpotent of class at most $2d-1$ whence $\gamma_{2d}(G) \leq W$. Since $\gamma_{2d}(G)$ has at most d generators, it becomes clear that $\gamma_{2d}(G)$ is powerful. Thus we conclude that $\gamma_{2d}(G)$ has rank at most d [3, Theorem 2.9]. Since G' has at most d generators, it is easy to see that r, the rank of $G'/\gamma_{2d}(G)$, is d-bounded. But then the rank of G' is at most $r+d$. ∎

To prove Theorem 1.3 some more preparatory work is required. First note that it suffices to prove that there is a bound on the exponent of $P \cap G'$ for a Sylow p-subgroup for each prime p (with a bound depending only on m and q). By Theorem 1.4, the exponent of $(P \cap G')/P'$ is bounded by m. Thus, the exponent of $P \cap G'$ is bounded by mm' where m' is the bound for p-groups. Note also that if $p > m$, $P \cap G' = 1$ and so p does not divide $|G|'$. So in what follows we assume the hypothesis of Theorem 1.3 with G being a p-group.

LEMMA 5.1: *Theorem 1.3 is valid if G is powerful.*

Proof: If G is powerful so is G' [3, Exercise 2.1]. Since G' is generated by elements of order dividing m (Lemma 2.3), it follows that the exponent of G' divides m [3, Lemma 2.5]. ∎

LEMMA 5.2: *Assume G has a characteristic powerful subgroup H of index t. Then the exponent of G' is $\{m,q,t\}$-bounded.*

Proof: We know from the previous lemma that the exponent of H' is $\{m,q\}$-bounded. Factoring out H' we can assume that H is abelian. Then, by Lemma 2.3, $[H,G]$ has exponent dividing m. Passing to the quotient $G/[H,G]$ we can assume that H is central. But then G' has t-bounded order by the Schur Theorem (see [15, Part 1, Theorem 4.12]).

Proof of Theorem 1.3: Let x be any element of G'. By Lemma 2.3, x can be written as a product $x = x_1 \cdots x_s$, where each x_l belongs to some $C_G(a)'$ for a suitable $a \in A^{\#}$. So $s \leq q^2 + q + 1$. Let Y be the subgroup of G generated by the orbits x_l^A, $l = 1, 2, \dots, s$. Each such orbit contains at most q^2 elements so it follows that Y has at most $q^2 s$ generators, each of order dividing m. Since $x \in Y$ and our goal is to bound the order of x, it is sufficient to show that the exponent of Y is $\{m, q\}$-bounded.

Let $L = L_p(Y)$, $M = Y/\Phi(Y)$. Then M is a subspace of L such that $\langle M \rangle = L$. Of course the dimension of M is at most $q^2 s$. For any $a \in A^{\#}$ we let M_a denote the image of $C_G(a)' \cap Y$ in M. Since Y is generated by x_l^A, it is clear that $M = \sum M_a$, where the summation is taken over all $a \in A^{\#}$. Any Lie commutator in elements of M_a (for a fixed $a \in A^{\#}$) corresponds to a group commutator in elements of $C_G(a)'$. Since $C_G(a)'$ has exponent dividing m, Proposition 4.5 shows that any Lie commutator in elements of M_a is ad-nilpotent of index at most m. We know that the dimension of M_a is at most $q^2 s$ and $C_G(a)'$ satisfies the law $y^m = 1$. Thus, by Lemma 4.8, there exists an $\{m, q\}$-bounded number u such that

$$[L, \underbrace{M_a, \dots, M_a}_{u}] = 0. \tag{5.3}$$

Let ω be a primitive qth root of unity, and let $\overline{L} = L \otimes \mathbb{F}_p[\omega]$. We will view $\overline{L}$ as a Lie algebra over $\mathbb{F}_p[\omega]$ and L as a subset of $\overline{L}$. For any $\mathbb{F}_p$-subspace S of L we write $\overline{S}$ for $S \otimes \mathbb{F}_p[\omega]$. An element of $\overline{L}$ will be called homogeneous if it belongs to $\overline{S}$ for some homogeneous subspace S of L. The group A acts naturally on L and this action extends uniquely to $\overline{L}$. It is easy to see that $C_{\overline{L}}(a) = \overline{C_L(a)}$ for any $a \in A$. Also recall that $C_L(a) = L_p(Y, C_Y(a))$. The field $\mathbb{F}_p[\omega]$ contains all eigenvalues for any $a \in A$ regarded as a linear transformation of $\overline{L}$. It follows that any A-invariant subspace of $\overline{L}$ decomposes as a direct sum of 1-dimensional A-invariant subspaces. Applying this remark to the subspaces $\overline{M_a}$ (for all $a \in A^{\#}$) and using that the algebra $\overline{L}$ is generated by $\overline{M}$ and that the $\mathbb{F}_p[\omega]$-dimension of $\overline{M}$ is at most $q^2 s$, we can choose vectors $v_1, \dots, v_d$ with $d \leq q^2 s$ such that $\overline{M}$ is spanned by $v_1, \dots, v_d$ and each of them is a common eigenvector for all $a \in A^{\#}$ lying in $\overline{M_a}$ for some $a \in A^{\#}$. Obviously (5.3) implies that

$$[\overline{L}, \underbrace{\overline{M_a}, \dots, \overline{M_a}}_{u}] = 0$$

so that, in particular, it follows that

(5.4) each of the vectors $v_1, \dots, v_d$ is ad-nilpotent of index at most u.

We will now show that

(5.5) there exists an $\{m,q\}$-number u_1 such that if $l_1, l_2 \in \overline{L}$ are common eigenvectors for all $a \in A$, and if they are homogeneous, then $[l_1, l_2]$ is ad-nilpotent of index at most u_1.

Really, since l_1, l_2 are common eigenvectors for all $a \in A$, it follows that there exist two maximal subgroups A_1 and A_2 of A such that $l_1 \in C_{\overline{L}}(A_1)$, $l_2 \in C_{\overline{L}}(A_2)$. Let a be a non-identity element in $A_i \cap A_j$. Since $C_G(a)$ has derived group of exponent m, and since $C_L(a) = L_p(Y, C_Y(a))$, Proposition 4.5 shows that any homogeneous element of $[C_L(a), C_L(a)]$ is ad-nilpotent of index at most m. The commutator $[l_1, l_2]$, being a homogeneous element of $\overline{L}$, can be written as $[l_1, l_2] = y_0 \otimes 1 + y_1 \otimes \omega + \cdots + y_{q-2} \otimes \omega^{q-2}$ for suitable homogeneous elements $y_0, y_1, \ldots, y_{q-1}$ of $[C_L(a), C_L(a)]$. The elements $y_0, y_1, \ldots, y_{q-1}$ correspond to some $g_0, g_1, \ldots, g_{q-1}$ that belong to the derived group of $C_Y(a)$. Set $K = \langle y_0, y_1, \ldots, y_{q-1} \rangle$ and $H = \langle g_0, g_1, \ldots, g_{q-1} \rangle$. Since H has exponent m and $K \leq L(Y, H)$, Lemma 4.8 shows that there exists an $\{m,q\}$-number u_1 such that

$$[L, \underbrace{K, \ldots, K}_{u_1}] = 0.$$

Clearly, this gives us

$$[\overline{L}, \underbrace{\overline{K}, \ldots, \overline{K}}_{u_1}] = 0.$$

Since $[l_1, l_2] \in \overline{K}$, (5.5) follows.

Using Proposition 4.6 and the fact that $C_L(a) = L_p(Y, C_Y(a))$, we conclude that $C_L(a)$ satisfies a certain $\{m,q\}$-bounded multilinear polynomial identity. This also holds in $C_{\overline{L}}(a) = \overline{C_L(a)}$. Therefore Corollary 4.3 implies that $\overline{L}$ satisfies a certain $\{m,q\}$-bounded polynomial identity. Combined with (5.4) and with (5.5) this places us in a situation where Theorem 4.1 can be used. Thus we conclude that $\overline{L}$ is nilpotent of $\{m,q\}$-bounded class. Now Lemma 4.7 yields that Y has a characteristic powerful subgroup of $\{m,q\}$-bounded index. By Lemma 5.2 we conclude that Y' has $\{m,q\}$-bounded exponent. Since Y is generated by elements of order dividing m, it follows that the exponent of Y is $\{m,q\}$-bounded, as required. ∎

References

[1] Yu. A. Bahturin and M. V. Zaicev, *Identities of graded algebras,* Journal of Algebra **205** (1998), 1-12.

[2] H. Bender, *Goldschmidt's* 2-*signalizer functor theorem,* Israel Journal of Mathematics **22** (1975), 208-213.

[3] J. D. Dixon, M. P. F. du Sautoy, A. Mann and D. Segal, *Analytic pro-p groups,* London Mathematical Society Lecture Note Series **157**, Cambridge University Press, 1991.

[4] G. Glauberman, *On solvable signalizer functors in finite groups,* Proceedings of the London Mathematical Society **33** (1976), 1-27.

[5] D. M. Goldschmidt, 2-*signalizer functors on finite groups,* Journal of Algebra **21** (1972), 321-340.

[6] D. Gorenstein, *Finite Groups,* Harper and Row, New York, 1968.

[7] R. Guralnick, *On the number of generators of a finite group,* Archiv der Mathematik **53** (1989), 521-523.

[8] E. I. Khukhro, *Nilpotent Groups and their Automorphisms,* de Gruyter-Verlag, Berlin, 1993.

[9] E. I. Khukhro and P. V. Shumyatsky, *Bounding the exponent of a finite group with automorphisms,* Journal of Algebra **212** (1999), 363-374.

[10] L. Kovács, *On finite soluble groups,* Mathematische Zeitschrift **103** (1968), 37-39.

[11] M. Lazard, *Sur les groupes nilpotents et les anneaux de Lie,* Annales Scientifiques de l'École Normale Supérieure **71** (1954), 101-190.

[12] V. Linchenko, *Identities of Lie algebras with actions of Hopf algebras,* Communications in Algebra **25** (1997), 3179-3187.

[13] A. Lubotzky and A. Mann, *Powerful p-groups. I: finite groups,* Journal of Algebra **105** (1987), 484-505; *II: p-adic analytic groups,* Journal of Algebra **105** (1987), 506-515.

[14] A. Lucchini, *A bound on the number of generators of a finite group,* Archiv der Mathematik **53** (1989), 313-317.

[15] D. J. S. Robinson, *Finiteness Conditions and Generalized Soluble Groups,* Springer, Berlin, 1972.

[16] P. Shumyatsky, *On periodic soluble groups and the fixed-point groups of operators,* Communications in Algebra **20** (1992), 2815-2820.

[17] P. Shumyatsky, *On periodic solvable groups having automorphisms with nilpotent fixed point groups,* Israel Journal of Mathematics **87** (1994), 111-116.

[18] P. Shumyatsky, *Exponent of finite groups admitting an involutory automorphism,* Journal of Group Theory **2** (1999), 367-372.

[19] J. G. Thompson, *Finite groups with fixed-point-free automorphisms of prime order*, Proceedings of the National Academy of Sciences of the United States of America **45** (1959), 578–581.

[20] Y. M. Wang and Z. M. Chen, *Solubility of finite groups admitting a coprime order operator group*, Unione Matematica Italiana. Bollettino **7** (1993), 325–331.

[21] J. N. Ward, *On finite groups admitting automorphisms with nilpotent fixed-point group*, Bulletin of the Australian Mathematical Society **5** (1971), 281–282.

[22] J. N. Ward, *On finite soluble groups and the fixed-point groups of automorphisms*, Bulletin of the Australian Mathematical Society **5** (1971), 375–378.

[23] J. N. Ward, *On groups admitting a noncyclic abelian automorphism group*, Bulletin of the Australian Mathematical Society **9** (1973), 363–366.

[24] J. S. Wilson and E. Zelmanov, *Identities for Lie algebras of pro-p groups*, Journal of Pure and Applied Algebra **81** (1992), 103–109.

[25] E. Zelmanov, *Nil Rings and Periodic Groups*, The Korean Mathematical Society Lecture Notes in Mathematics, Seoul, 1992.