Criteria for solubility and nilpotency of finite groups with automorphisms

Cristina Acciarri, Robert M. Guralnick, and Pavel Shumyatsky

Abstract. Let $G$ be a finite group admitting a coprime automorphism $\alpha$. Let $J_G(\alpha)$ denote the set of all commutators $[x, \alpha]$, where $x$ belongs to an $\alpha$-invariant Sylow subgroup of $G$. We show that $[G, \alpha]$ is soluble or nilpotent if and only if any subgroup generated by a pair of elements of coprime orders from the set $J_G(\alpha)$ is soluble or nilpotent, respectively.

1. Introduction

In [4] Baumslag and Wiegold established the following sufficient condition for the nilpotency of a finite group $G$.

Theorem 1.1. Let $G$ be a finite group in which $|ab| = |a|\cdot |b|$, whenever the elements $a, b$ have coprime orders. Then $G$ is nilpotent.

Here the symbol $|x|$ stands for the order of an element $x$ in a group $G$. Obviously the condition above is also necessary for the nilpotency of $G$. We mention that there are several recent results related to the theorem of Baumslag and Wiegold (see for example [2, 3, 10, 12, 6]).

An automorphism $\alpha$ of a finite group $G$ is said to be coprime if $(|G|, |\alpha|) = 1$. Following [1] denote by $I_G(\alpha)$ the set of commutators $g^{-1}g^\alpha$, where $g \in G$. Let $[G, \alpha]$ be the subgroup generated by $I_G(\alpha)$. In [1] the authors studied the impact of $I_G(\alpha)$ on the structure of $[G, \alpha]$.

Here we establish the following variation of the result of Baumslag and Wiegold.

\begin{itemize}
  \item 2010 Mathematics Subject Classification. 20D45.
  \item Key words and phrases. Finite groups, automorphisms.
\end{itemize}

The authors thank the reviewer for pointing out an error in an earlier version of the paper. The second author was partially supported by the NSF grant DMS-1901595 and a Simons Foundation Fellowship 609771. The third author was supported by CNPq and FAPDF, Brazil.
Theorem 1.2. Let $G$ be a finite group admitting a coprime automorphism $\alpha$. Then $[G, \alpha]$ is nilpotent if, and only if, $|xy| = |x||y|$ whenever $x$ and $y$ are elements of coprime prime power orders from $I_G(\alpha)$.

At the start of this project, we did not know whether the hypothesis on the orders of elements in Theorem 1.2 is inherited by quotient groups. In order to overcome this issue we work instead with a somewhat different condition that behaves well with respect to forming quotients. Let $J_G(\alpha)$ denote the set of all commutators $[x, \alpha]$, where $x$ belongs to an $\alpha$-invariant Sylow subgroup of $G$. Observe that $J_G(\alpha)$ is a subset of $I_G(\alpha)$ and the elements of $J_G(\alpha)$ have prime power order. Moreover note that $J_G(\alpha)$ is a generating set for $[G, \alpha]$. Indeed this easily follows from $[13, \text{Lemma 2.4}]$. It turns out that properties of $G$ are pretty much determined by those of subgroups generated by elements of coprime orders from $J_G(\alpha)$.

It is well known that if any pair of elements of a finite group generates a soluble (respectively nilpotent) subgroup, then the whole group is soluble (respectively nilpotent). One of the theorems established in $[1]$ provides a variation of this for groups with automorphisms.

Let $G$ be a finite group admitting a coprime automorphism $\alpha$. If any pair of elements from $I_G(\alpha)$ generates a soluble subgroup, then $[G, \alpha]$ is soluble. If any pair of elements from $I_G(\alpha)$ generates a nilpotent subgroup, then $[G, \alpha]$ is nilpotent.

Here this will be extended as follows.

Let $G$ be a finite group admitting a coprime automorphism $\alpha$. Then $[G, \alpha]$ is soluble if and only if any subgroup generated by a pair of elements of coprime orders from $J_G(\alpha)$ is soluble.

In fact, we will establish a stronger result. Assume that a finite group $G$ admits an automorphism group $A$. If $\alpha \in A$, let $J_{G,A}(\alpha)$ be the set of commutators $[x, \alpha]$ for $x$ in an $A$-invariant Sylow subgroup of $G$.

Theorem 1.3. Let $G$ be a finite group admitting a coprime group of automorphisms $A$. If $\alpha \in A$, then $[G, \alpha]$ is soluble if and only if any subgroup generated by a pair of elements of coprime orders from $J_{G,A}(\alpha)$ is soluble.

Note that this fails if the coprimeness assumption is omitted. For example if $\alpha$ is a transposition in the symmetric group $G = S_n$, any
pair of elements from \( I_G(\alpha) \) generates a soluble subgroup while \([G, \alpha]\) is insoluble for \( n \geq 5 \).

Theorem 1.3 is used to establish the following related necessary and sufficient conditions for the nilpotency of \([G, \alpha]\).

**Theorem 1.4.** Let \( G \) be a finite group admitting a coprime group of automorphisms \( A \), and let \( \alpha \in A \). Then the following statements are equivalent.

(i) The subgroup \([G, \alpha]\) is nilpotent;
(ii) Any subgroup generated by a pair of elements of coprime orders from \( J_{G,A}(\alpha) \) is nilpotent;
(iii) Any subgroup generated by a pair of elements of coprime orders from \( J_{G,A}(\alpha) \) is abelian;
(iv) If \( x \) and \( y \) are elements of coprime orders from \( J_{G,A}(\alpha) \), then \(|xy| = |x||y|\);
(v) If \( x \) and \( y \) are elements of coprime orders from \( J_{G,A}(\alpha) \), then \( \pi(xy) = \pi(x) \cup \pi(y) \).

Here, \( \pi(g) \) denotes the set of prime divisors of the order of \( g \in G \).

Note that Theorem 1.2 easily follows from Theorem 1.4.

2. A condition for solubility of \([G, \alpha]\)

All groups considered in this paper are finite. We start with a collection of well-known facts about coprime automorphisms of finite groups (see for example [8]).

**Lemma 2.1.** Let a group \( G \) admit a coprime group of automorphisms \( A \). The following conditions hold:

(i) \( G = [G, A]C_G(A) \);
(ii) If \( N \) is any \( A \)-invariant normal subgroup of \( G \), we have \( C_{G/N}(A) = C_G(A)N/N \);
(iii) If \( \alpha \in A \) and \( N \) is an \( A \)-invariant normal subgroup of \( G \), we have \( J_{G/N,A}(\alpha) = \{ gN \ | \ g \in J_{G,A}(\alpha) \} \);
(iv) If \( N \) is any \( A \)-invariant normal subgroup of \( G \) such that \( N = C_N(A) \), then \([G, A]\) centralizes \( N \);
(v) Any \( A \)-invariant \( p \)-subgroup of \( G \) is contained in an \( A \)-invariant Sylow \( p \)-subgroup.

The purpose in this section is to establish conditions that lead to the solubility of \([G, \alpha]\). Throughout, by a simple group we mean a nonabelian simple group. If a simple group \( G \) admits a coprime automorphism \( \alpha \) of order \( e \), then \( G = L(q) \) is a group of Lie type and \( \alpha \) is a field automorphism. Furthermore, \( C_G(\alpha) = L(q_0) \) is a group of the
same Lie type (and rank) defined over the subfield such that \( q = q_0^e \) (see [9]).

In what follows, \( q = p^s \) is a power of a prime \( p \). For any positive integer \( n \), we say that a prime \( r \) is a primitive prime divisor of \( q^n - 1 \) if \( r \) divides \( q^n - 1 \) and \( r \) does not divide \( q^k - 1 \) for any positive integer \( k < n \). Primitive prime divisors of \( q^n + 1 \) are defined in a similar way. The following result of Zsigmondy ([18]) on the existence of primitive prime divisors will be used in the sequel.

**Theorem 2.2 ([18]).** Let \( a > b > 0 \), \( \gcd(a, b) = 1 \) and \( n > 1 \) be positive integers. Then

(i) \( a^n - b^n \) has a prime divisor that does not divide \( a^k - b^k \) for all positive integers \( k < n \), unless \( a = 2, b = 1 \) and \( n = 6 \); or \( a + b \) is a power of 2 and \( n = 2 \).

(ii) \( a^n + b^n \) has a prime divisor that does not divide \( a^k + b^k \) for all positive integers \( k < n \), with exception \( 2^3 + 1^3 \).

Throughout, the term “semisimple group” means direct product of simple groups. We are now ready to deal with the proof of Theorem 1.3.

**Proof of Theorem 1.3.** If \([G, \alpha]\) is soluble, the result is clear. Let us prove the converse. We wish to show that there are \( A \)-invariant subgroups \( P \) and \( Q \) of coprime prime power orders such that \([x, \alpha] \) and \([y, \alpha] \) generate an insoluble subgroup for some \( x \in P \) and \( y \in Q \). Note that any \( A \)-invariant \( p \)-subgroup \( P \) of \( G \) is contained in an \( A \)-invariant Sylow \( p \)-subgroup.

Suppose that this is false and let \( G = [G, A] \) be a counterexample of minimal order. So any pair of elements of coprime order in \( J_{G, A}(\alpha) \) generate a soluble group but \([G, \alpha] \) is insoluble. Suppose that \( G \) contains a nontrivial characteristic soluble subgroup \( M \). Then, by minimality, the result holds for \( A \) acting on \( G/M \) and so \([G, \alpha]M/M \) and \([G, \alpha] \) are both soluble, a contradiction.

So we may assume that \( G \) contains no soluble nontrivial normal subgroups. Then \( F^*(G) \) is a direct product of nonabelian simple groups and \( A \) acts faithfully on \( F^*(G) \) (since \( F^*(GA) = F^*(G) \)). Choose a component \( S \) of \( F^*(G) \) so that \( \alpha \) does not centralize \( S \). Let \( T = S_1 \times \ldots \times S_t \) be the \( A \)-orbit of \( S = S_1 \). Then \([T, \alpha] \) is insoluble and so it suffices to assume that \( G = T \).

Let \( A_1 = N_A(S) \). Then \( A_1/C_A(S) \) is a coprime group of automorphisms of the simple group \( S \). If \( A_1 \) is trivial, then \( |A| = t \) and \( A \) acts on \( G \) by permuting the coordinates of \( S_1 \times \ldots \times S_t \). By [11, Theorem 1.2] (or [7]), there exist distinct primes \( p \) and \( q \), a Sylow \( p \)-subgroup \( P_1 \)
of $S = S_1$ and a Sylow $q$-subgroup $Q_1$ of $S$ so that $\langle x_1, y_1 \rangle$ is insoluble, with $x_1 \in P_1$ and $y_1 \in Q_1$. Then the (direct) product $P$ of the distinct $A$-conjugates of $P_1$ is an $A$-invariant Sylow $p$-subgroup of $G$. Similarly the direct product $Q$ of the $A$-conjugates of $Q_1$ is an $A$-invariant Sylow $q$-subgroup of $G$. Note that $[x_1, \alpha] \in [P, \alpha]$ and $[y_1, \alpha] \in [Q, \alpha]$ generate an insoluble group.

So we may assume that $A_1 \neq 1$. It follows that $S = L(q)$ is a group of Lie type over the field of $q = p^s$ and $A_1$ induces a cyclic group of field automorphisms (see [9]).

First assume that $S$ has rank at least 2. Note that $A_1$ normalizes a Borel subgroup $B$ and, by the structure of field automorphisms, $A_1$ normalizes each parabolic subgroup containing $B$ and indeed $A_1$ acts faithfully on a Levi subgroup $L_1$ of $S$. Since $q \geq 8$, $L_1$ is insoluble. It follows that $A$ acts faithfully on the (direct) product $H$ of the $A$-conjugates of $L_1$ and $[H, \alpha]$ is a nontrivial normal subgroup of $H$. Thus $[H, \alpha]$ is insoluble and the result follows by induction.

So assume that $S$ has (twisted) Lie rank 1. If $S = PSU_3(q)$ or $^2G_2(q)$, we observe that there is an $A_1$-invariant subgroup isomorphic to $PSL_2(q)$ which is not centralized by $A_1$ and so we can reduce to the case $S = PSL_2(q)$. Thus, we only need to consider $S = PSL_2(q)$ with $q = p^s$ for $s$ odd and $s \geq 5$ or $S = Sz(q)$ with $q = 2^s$ for odd $s > 1$.

If $S = PSL_2(q)$, take $U$ to be an $A_1$-invariant Sylow $p$-subgroup of $S$. Let now $r$ be a primitive prime divisor of $q+1$, i.e. $r$ does not divide $p^i + 1$ for $i < s$ (that always exists by Theorem 2.2), and let $R$ be an $A_1$-invariant Sylow $r$-subgroup of $S$. Then $U$ and $R$ are contained in $A$-invariant Sylow subgroups (by taking the product of the distinct $t$ conjugates under $A$).

Note that any nontrivial element $x$ of $R$ and any nontrivial element $y$ of $U$ generate $S$ by [15, Theorem 6.25 in Chap. 3] (and in particular generate an insoluble subgroup). Moreover $[U, \alpha]$ and $[R, \alpha]$ are both contained in $J_G(\alpha)$. If $\alpha$ is contained in $A_1$, then it induces a nontrivial automorphism on $S$ and $[U, \alpha] \neq 1$. Further, since $r$ does not divide the order of $C_S(\alpha)$ we have $[R, \alpha] = R$. If $x \in [U, \alpha]$ and $y \in [R, \alpha]$, then the pair $x, y$ is as required. If $\alpha \notin A_1$, then the pair $[x, \alpha]$ and $[y, \alpha]$ is as required, since $\alpha$ conjugates $S$ to some other component $S_i$.

It remains to consider the case $S = Sz(q)$, where $q = 2^s$ for odd $s > 1$. See [14] for properties of Suzuki groups. Essentially the same argument applies. The order of $S$ is $q^2(q - 1)(q^2 + 1)$. Observe that the maximal subgroups of $S$ are (up to conjugacy) a Borel subgroup of order $q(q - 1)$, a dihedral subgroup of order $2(q - 1)$, subfield subgroups, and two subgroups of the form $T.4$, where $T$ is cyclic of order $q \pm l + 1$.
with \( l^2 = 2q \), i.e. of order \( 2^s \pm 2^{(s+1)/2} + 1 \). Note that \((q+l+1)(q-l+1) = q^2 + 1\).

Let \( r \) be a primitive prime divisor of \( q^2 + 1 = 2^{2s} + 1 \). Let \( R \) be an \( A_1 \)-invariant Sylow \( r \)-subgroup. Let \( u \) be a primitive prime divisor of \( q - 1 = 2^s - 1 \). Then \( u \) does not divide the order of any subfield subgroup and also \( u \) does not divide \( q^2 + 1 \). By \([14, Theorem 9]\), there is no proper subgroup of \( S \) whose order is divisible by \( ru \). Let \( U \) be an \( A_1 \)-invariant Sylow \( u \)-subgroup of \( S \). Neither of \( R \) and \( U \) intersects \( C_S(\alpha) \), whence \([R, \alpha] = R \) and \([U, \alpha] = U \). Moreover any element in \( R \) or \( U \) is a commutator with \( \alpha \). It follows that \( S \) is generated by nontrivial \([x, \alpha] \) and \([y, \alpha] \) with \( x \in R \) and \( y \in U \). This gives the result if \( \alpha \in A_1 \). If \( \alpha \) does not normalize \( S \), then, as in the previous case, take elements \( x \in R \) and \( y \in U \). The commutators \([x, \alpha] \) and \([y, \alpha] \) generate an insoluble group. This completes the proof. \( \square \)

As a by-product of the proof of Theorem 1.3 we obtain the following proposition.

**Proposition 2.3.** Let \( G \) be a finite group admitting a coprime group of automorphisms \( A \). Let \( \alpha \in A \), and assume that \( \pi(xy) = \pi(x) \cup \pi(y) \) whenever \( x \) and \( y \) are elements of coprime orders from \( J_{G,A}(\alpha) \). Then \([G, \alpha] \) is soluble.

The proof will be omitted since it is just an obvious modification of the argument used in Theorem 1.3. The proposition will be used in the proof of Theorem 1.4, which in particular shows that under the hypotheses of the proposition the subgroup \([G, \alpha] \) is nilpotent.

### 3. Criteria for nilpotency of \([G, \alpha]\)

In this section we aim to establish Theorem 1.4 that gives necessary and sufficient conditions for the nilpotency of \([G, \alpha]\). For the reader’s convenience we restate it here.

**Let \( G \) be a finite group admitting a coprime group of automorphisms \( A \), and let \( \alpha \in A \). Then the following statements are equivalent.**

(i) The subgroup \([G, \alpha] \) is nilpotent;

(ii) Any subgroup generated by a pair of elements of coprime orders from \( J_{G,A}(\alpha) \) is nilpotent;

(iii) Any subgroup generated by a pair of elements of coprime orders from \( J_{G,A}(\alpha) \) is abelian;

(iv) If \( x \) and \( y \) are elements of coprime orders from \( J_{G,A}(\alpha) \), then \(|xy| = |x||y|\);
(v) If \( x \) and \( y \) are elements of coprime orders from \( J_{G,A}(\alpha) \), then 
\[ \pi(xy) = \pi(x) \cup \pi(y). \]

**Proof of Theorem 1.4.** Note that obviously (i) implies (ii). Now if \( x \) and \( y \) are elements of coprime prime power orders from \( J_{G,A}(\alpha) \) generating a nilpotent subgroup, then \( x \) and \( y \) commute with each other and so (ii) implies (iii). If \( x \) and \( y \) are elements of coprime prime power orders from \( J_{G,A}(\alpha) \) generating an abelian subgroup, then \( |xy| = |x||y| \), and so (iii) implies (iv). Moreover it is immediate to see that (iv) implies (v).

We now prove the implication (v) \( \Rightarrow \) (i). Assume (v). In view of Proposition 2.3, the subgroup \([G,\alpha]\) is soluble. Suppose that the result is false and let \( G \) be a counterexample of minimal order. Note that \( G = [G,\alpha]^A \), that is, there are no proper \( A \)-invariant subgroups containing \([G,\alpha]\). Let \( M \) be a minimal \( A \)-invariant normal subgroup of \( G \). Hence, \( M \) is an elementary abelian \( p \)-group, for some prime \( p \), because \( G \) is soluble. Since \( G/M \) satisfies the hypothesis, by induction \([G,\alpha]M/M\) is nilpotent. Taking into account that \( G = [G,\alpha]^A \) we deduce that \( G/M \) is nilpotent.

It follows that \( G = MQ \), where \( Q \) is an \( A \)-invariant Sylow \( q \)-subgroup of \( G \) satisfying \( Q = [Q,\alpha]^A \). Remark that by definitions of \( J_{G,A}(\alpha) \) and \( J_G(\alpha) \) we have \( J_{M,A}(\alpha) = J_M(\alpha) \) and \( J_{Q,A}(\alpha) = J_Q(\alpha) \).

By hypothesis, for any \( x \in J_Q(\alpha) \) and \( y \in J_M(\alpha) \), the order of \( xy \) is divisible by both \( p \) and \( q \). Note that the element \( y \) is of the form \([m,\alpha]\), for suitable element \( m \in M \) and \( y \in [M,\alpha] \). If \( y \in [M,x] \), then \( xy \) is a \( q \)-element, contradicting the hypothesis. Hence we have \([M,x] \cap [M,\alpha] = 1 \), whenever \( x \in J_Q(\alpha) \).

Suppose that for a nontrivial element \( u \) there is \( x \in J_Q(\alpha) \) such that \( u \in C_M(x\alpha^{-1}) \) while \( u \notin C_M(\alpha) \). Then the element \([u,\alpha]\) is nontrivial and belongs to the intersection \([M,\alpha] \cap [M,x] \). This leads to a contradiction with the above assumption that \([M,x] \cap [M,\alpha] = 1 \), whenever \( x \in J_Q(\alpha) \).

Therefore
\[
C_M(x\alpha^{-1}) \leq C_M(\alpha) \quad \text{whenever} \quad x \in J_Q(\alpha).
\]

(1)

Now, let \( g \) be an arbitrary element of \( Q \) and apply (1) with \( x = [g,\alpha] \). Then \( x\alpha^{-1} = \alpha^{-g} \) and we obtain that \( C_M(\alpha)^g = C_M(\alpha) \). Since this holds for any \( g \in Q \), we conclude that \( C_M(\alpha) \) is normal in \( G \). Lemma 2.1 (iv) now shows that \( C_M(\alpha) \) commutes with \([Q,\alpha] \). Since \( G \) is a counterexample of minimal order, we deduce that \( C_M(\alpha) = 1 \). Thus, we have \( M = [M,\alpha] \). Recall that \([M,x] \cap [M,\alpha] = 1 \). It follows that \([M,x] = 1 \) for any \( x \in J_Q(\alpha) \) and, taking into account that \( Q = [Q,\alpha]^A \),
we obtain that $M \leq Z(G)$, a contradiction. This proves that (v) implies (i) and thus the theorem is established. □
