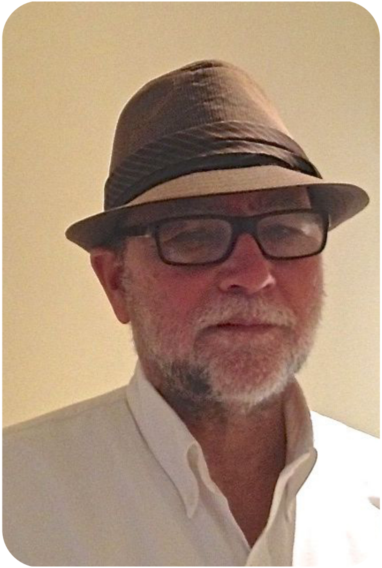
Coprime Automorphisms of Finite Groups

Cristina Acciarri

University of Modena and Reggio Emilia

22/6/22 - Ischia Group Theory 2022

Joint work with



Robert Guralnick (USC)

Pavel Shumyatsky (UnB)

Initial settings

An automorphism α of a finite group G is said to be *coprime* if

$$(|G|, |\alpha|) = 1.$$

Denote by

- $C_G(\alpha)$ the fixed-point subgroup $\{x \in G;\ x^\alpha = x\}$;
- $I_G(\alpha)$ the set of all commutators $g^{-1}g^\alpha$, where $g \in G$;
- $[G, \alpha]$ the subgroup generated by $I_G(\alpha)$.

Then $G = [G, \alpha]C_G(\alpha)$ and $|I_G(\alpha)| = [G : C_G(\alpha)]$.

Vague duality between $C_G(\alpha)$ and $I_G(\alpha)$: since $|G| = |C_G(\alpha)||I_G(\alpha)|$, if one of $C_G(\alpha), I_G(\alpha)$ is large then the other is small.

If N is any α-invariant normal subgroup of G we have:

(i) $C_{G/N}(\alpha) = C_G(\alpha)N/N$, and $I_{G/N}(\alpha) = \{gN \mid g \in I_G(\alpha)\}$;

(ii) If $N = C_N(\alpha)$, then $[G, \alpha]$ centralizes N.

Influence of $C_G(\alpha)$ on G

Theorem (Thompson, 1959)

If α has prime order and $C_G(\alpha) = 1$, then G is nilpotent.

This was generalized in several directions.

Theorem (Khukhro, 1990)

If G admits an automorphism α of prime order p with $C_G(\alpha)$ of order m, then G has a nilpotent subgroup of (m, p)-bounded index and p-bounded class.

Theorem (Khukhro, 2008)

If G admits a coprime automorphism α of prime order p with $C_G(\alpha)$ of rank r, then G has characteristic subgroups $R \leq N$ such that N/R is nilpotent of p-bounded class, while R and G/N have (p, r)-bounded ranks.

The rank of a finite group G is the least number r such that each subgroup of G can be generated by at most r elements.

Dual problem with $I_G(\alpha)$

Also properties of $I_G(\alpha)$ may strongly impact the structure of G.

If $|I_G(\alpha)| \leq m$, then the order of $[G, \alpha]$ is m-bounded.

Since $|I_G(\alpha)| \leq m$, the index of the centralizer $[G : C_G(\alpha)] \leq m$.
We can choose a normal subgroup $N \leq C_G(\alpha)$ such that $[G : N] \leq m!$
Note that $[G, \alpha]$ commutes with N and so $[[G, \alpha] : Z([G, \alpha])] \leq m!$.
The Schur theorem yields that $|[G, \alpha]'|$ is m-bounded.
We can pass to $G/[G, \alpha]'$ and assume that $[G, \alpha]$ is abelian.
Then $[G, \alpha] = I_G(\alpha)$ and so $|[G, \alpha]| \leq m$. □

A rank condition on the set $I_G(\alpha)$

The usual concept of rank does not apply to $I_G(\alpha)$.
We consider the condition that each subgroup of G generated by a subset of $I_G(\alpha)$ can be generated by at most r elements.

Theorem 1

Let G be a finite group admitting a coprime automorphism α of order e and suppose that any subgroup generated by a subset of $I_G(\alpha)$ can be generated by r elements. Then $[G, \alpha]$ has (e, r)-bounded rank.

The proof is rather technical and proceeds in several steps:

- the result for nilpotent groups: reduction to p-groups, powerful p-groups;
- for soluble groups: one key step is to show that there exists an (e, r)-bounded number f such that the fth term of the derived series of $[G, \alpha]$ is nilpotent (Zassenhaus' theorem on the derived length of any soluble subgroup of $GL_n(k)$ and Hartley-Isaacs result on representation theory).Then the Fitting height $h([G, \alpha])$ is (e, r)-bounded and $[G, \alpha]$ is generated by (e, r)-boundedly many elements from $I_G(\alpha)$;

- the general case: after a long reduction it is sufficient to prove the result in the case where G is soluble-by-semisimple-by-soluble. It depends on CFSG, on facts about conjugacy classes and characters of $PGL_2(q)$ and also on the following result (of independent interest)

Theorem 2

Let G be a finite group admitting a coprime automorphism α such that $g^{-1}g^{\alpha}$ has odd order for every $g \in G$. Then $[G, \alpha] \leq O(G)$.

Here $O(G)$ stands for the maximal normal subgroup of odd order of G. The assumption that α is coprime in Theorem 2 is really necessary.

Some conditions on solubility for $[G, \alpha]$

It is well known that if any pair of elements of a finite group generates a soluble subgroup, then the whole group is soluble (Thompson, 1968).

Theorem 3

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

More on solubility criteria

In a very recent work (arXiv:2206.03403) we get more interested on criteria for solubility and nilpotency of $[G,\alpha]$.

For technical reasons we look at a different set of elements

Let $J_G(\alpha)$ denote the set of all commutators $[x,\alpha]$, where x belongs to an α-invariant Sylow subgroup of G.

- $J_G(\alpha) \subset I_G(\alpha)$, and
- the elements of $J_G(\alpha)$ have prime power order;
- $J_G(\alpha)$ is a generating set for $[G,\alpha]$;
- If N is any α-invariant normal subgroup of G, we have $J_{G/N}(\alpha) = \{gN \mid g \in J_G(\alpha)\}$.

It turns out that properties of G are pretty much determined by those of subgroups generated by elements of *coprime orders* from $J_G(\alpha)$.

More on solubility criteria (cont.)

We extend Theorem 3 as follows

Theorem 4

Let G be a finite group admitting a coprime automorphism α. 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.

Insight of the proof

Suppose the result is false and let $G = [G, \alpha]$ be a counterexample of minimal order. Recall that by hypothesis any subgroup generated by a pair of elements of coprime orders from $J_G(\alpha)$ is soluble.

We may assume that α has prime order, say e (arguing by induction on the order of α).

Our goal: to show that there are α-invariant subgroups P and Q of coprime prime power orders such that $[x, \alpha]$ and $[y, \alpha]$ generate a nonsoluble subgroup for some $x \in P$ and $y \in Q$.

Let M be a minimal α-invariant normal subgroup of G. By induction G/M is soluble. It is enough to consider M semisimple. Then M is a direct product of isomorphic simple groups, say $M = S_1 \times \cdots \times S_k$, and α transitively permutes the simple factors. Because of minimality $G = M$.

After some work we are reduced to the case where G is simple.

$G = L(q)$ is a group of Lie type, say over the field of $q = p^s$ elements and α is a field automorphism of coprime order e. The centralizer $C_G(\alpha)$ is the group of the same Lie type (and Lie rank) defined over the subfield of $q_0 = p^{s/e}$ elements.

For any α-invariant subgroup H of G the subgroup $[H, \alpha]$ is soluble.

Note that s is a e-power. Write $s = s_1 s_2$ where s_1 is a e-power and s_2 is coprime to e. Since α nontrivially acts on the subgroup $L(p^{s_1})$, because of minimality we conclude that $q = p^{s_1}$.

We eventually can reduce to consider

- $G = \mathrm{PSL}_2(q)$ with $q = p^s$ for s odd and $s \geq 5$ or
- $G = \mathrm{Sz}(q)$ with $q = 2^s$ for odd $s > 1$.

If $G = \mathrm{PSL}_2(q)$, take U to be an α-invariant Sylow p-subgroup and note that $[U, \alpha] \neq 1$. Any element in $[U, \alpha]$ is a commutator $[u, \alpha]$ with $u \in U$.

Let 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 Zsigmondy's Theorem -1892).
Let R be an α-invariant Sylow r-subgroup. Since r does not divide the order of $C_G(\alpha)$ (and of any subfield subgroup), we have $[R, \alpha] = R$.

Let $1 \neq x \in [R, \alpha]$ and let $1 \neq y \in [U, \alpha]$. It follows that $G = \langle x, y \rangle$ since there is no proper subgroup of order divisible by pr, a contradiction.

If $G = \mathrm{Sz}(q)$, where $q = 2^s$ for odd $s > 1$. $|G| = q^2(q-1)(q^2+1)$.

The maximal subgroups of G are (up to conjugacy) a Borel subgroup of order $q^2(q-1)$, 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 α-invariant Sylow r-subgroup.
Let t be a primitive prime divisor of $q - 1 = 2^s - 1$. Then t does not divide the order of any subfield subgroup and so also t does not divide $q^2 + 1$. Let S be an α-invariant Sylow t-subgroup.

There is no proper subgroup of G whose order is divisible by rt Neither of R and S intersects $C_G(\alpha)$, whence $[R, \alpha] = R$ and $[S, \alpha] = S$. Moreover any element in R or S is a commutator with α. It follows that G is generated by $[x, \alpha]$ and $[y, \alpha]$ with $x \in R$ and $y \in S$, a contradiction. $\square$

Thank you!