Coprime Automorphisms of Finite Groups

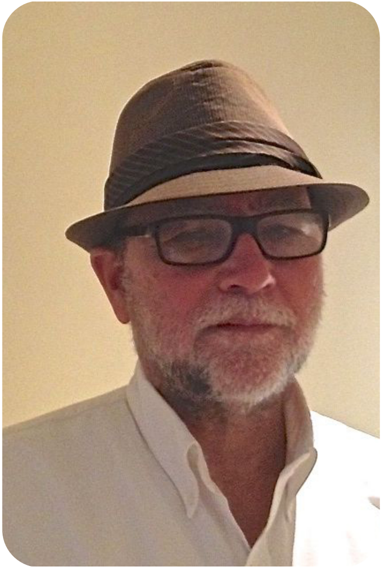
Cristina Acciarri

University of Modena and Reggio Emilia

University of Brasilia

8/6/2023 - AGTA 2023

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

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

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 $I_G(\alpha)$.

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

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.

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.

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.

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.

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.

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.

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 $[G : N] \leq m!$

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.

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 $I_G(\alpha)$.

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.

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.

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;

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).

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)

- 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 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).

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

Later we got more interested on criteria for solubility and nilpotency of $[G, \alpha]$.

More on solubility criteria

Later we got 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

More on solubility criteria

Later we got 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;

More on solubility criteria

Later we got 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 $[G, \alpha]$;

More on solubility criteria

Later we got 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 $[G, \alpha]$; this follows from

Theorem

Let G be a finite group admitting a coprime group of automorphisms A. Then $[G, A]$ is generated by all nilpotent subgrs. T such that $T = [T, A]$.

More on solubility criteria

Later we got 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 $[G, \alpha]$; this follows from

Theorem

Let G be a finite group admitting a coprime group of automorphisms A. Then $[G, A]$ is generated by all nilpotent subgrs. T such that $T = [T, A]$.

- If N is any α-invariant normal subgroup of G, we have $J_{G/N}(\alpha) = \{gN \mid g \in J_G(\alpha)\}$.

More on solubility criteria

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

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

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.

More on solubility criteria

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

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.

Observation: If $\langle \beta \rangle$ is any nontrivial subgroup of $\langle \alpha \rangle$, then the collection of β-invariant Sylow subgroups could be larger than the collection of α-invariant Sylow subgroups of G.

More on solubility criteria

To overcome this issue we will work in the following setting:

Let G be a finite group admitting a coprime group of automorphisms A, let $\alpha \in A$ and let $J_{G,A}(\alpha)$ denote the set of all commutators $[x, \alpha]$, for x in an A-invariant Sylow subgroup of G.

More on solubility criteria

To overcome this issue we will work in the following setting:

Let G be a finite group admitting a coprime group of automorphisms A, let $\alpha \in A$ and let $J_{G,A}(\alpha)$ denote the set of all commutators $[x, \alpha]$, for x in an A-invariant Sylow subgroup of G.

and we establish the following stronger result

Theorem 5

Let G be a finite group admitting a coprime group of automorphisms A and let $\alpha \in A$. 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.

More on solubility criteria

To overcome this issue we will work in the following setting:

Let G be a finite group admitting a coprime group of automorphisms A, let $\alpha \in A$ and let $J_{G,A}(\alpha)$ denote the set of all commutators $[x, \alpha]$, for x in an A-invariant Sylow subgroup of G.

and we establish the following stronger result

Theorem 5

Let G be a finite group admitting a coprime group of automorphisms A and let $\alpha \in A$. 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.

Remark: The result in the above theorem fails without the coprimeness assumption. For instance, take α a transposition in $G = S_n$, for $n \geq 5$. Then any pair of elements from $I_G(\alpha)$ generates a soluble subgroup, while $[G, \alpha]$ is insoluble.

Insight of the proof Thm 5

Our goal: 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 $y \in Q$.

Insight of the proof Thm 5

Our goal: 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 $y \in Q$.

Suppose the this is false and let $G = [G, A]$ be a counterexample of minimal order. So, any subgroup generated by a pair of elements of coprime order from $J_{G,A}(\alpha)$ is soluble but $[G, \alpha]$ is insoluble.

Insight of the proof Thm 5

Our goal: 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 $y \in Q$.

Suppose the this is false and let $G = [G, A]$ be a counterexample of minimal order. So, any subgroup generated by a pair of elements of coprime order from $J_{G,A}(\alpha)$ is soluble but $[G, \alpha]$ is insoluble.

If G contains a non-trivial characteristic soluble subgroup M, then by minimality the result holds for A acting on G/M and $[G, A]M/M$ is soluble. Hence $[G, A]$ is soluble too, a contradiction. We may assume that G contains no soluble non-trivial normal subgroups.

Insight of the proof Thm 5

Our goal: 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 $y \in Q$.

Suppose the this is false and let $G = [G, A]$ be a counterexample of minimal order. So, any subgroup generated by a pair of elements of coprime order from $J_{G,A}(\alpha)$ is soluble but $[G, \alpha]$ is insoluble.

If G contains a non-trivial characteristic soluble subgroup M, then by minimality the result holds for A acting on G/M and $[G, A]M/M$ is soluble. Hence $[G, A]$ is soluble too, a contradiction. We may assume that G contains no soluble non-trivial normal subgroups.

Then $F^*(G)$ is a direct product of non-abelian simple groups, and A acts faithfully on $F^*(G)$ (since $F^*(GA) = F^*(G)$). Choose a component S of $F^*(G)$ such that α does not centralize S.

Insight of the proof Thm 5

Our goal: 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 $y \in Q$.

Suppose the this is false and let $G = [G, A]$ be a counterexample of minimal order. So, any subgroup generated by a pair of elements of coprime order from $J_{G,A}(\alpha)$ is soluble but $[G, \alpha]$ is insoluble.

If G contains a non-trivial characteristic soluble subgroup M, then by minimality the result holds for A acting on G/M and $[G, A]M/M$ is soluble. Hence $[G, A]$ is soluble too, a contradiction. We may assume that G contains no soluble non-trivial normal subgroups.

Then $F^*(G)$ is a direct product of non-abelian simple groups, and A acts faithfully on $F^*(G)$ (since $F^*(GA) = F^*(G)$). Choose a component S of $F^*(G)$ such that α does not centralize S. Let $T = S_1 \times \cdots \times S_t$ be the A-orbit of $S = S_1$. Then $[T, \alpha]$ is insoluble and we can assume that $G = T$.

Insight of the proof of Theorem 5

$G = S_1 \times \cdots \times S_t$, $S = S_1$ and let $A_1 = N_A(S)$. Observe that $A_1/C_A(S)$ is a coprime group of automorphisms of S.

Insight of the proof of Theorem 5

$G = S_1 \times \cdots \times S_t$, $S = S_1$ and let $A_1 = N_A(S)$. Observe that $A_1/C_A(S)$ is a coprime group of automorphisms of S.

If $A_1 = 1$, then $|A| = t$ and A acts on G by permuting the coordinates of $S_1 \times \cdots \times S_t$

Theorem (Guralnick-Tiep, 2015)

Let G be a finite group. Then G is soluble if and only if $x_1 x_2 x_3 \neq 1$ for all nontrivial p_i-elements x_i of G for distinct primes p_i, $i = 1, 2, 3$

Insight of the proof of Theorem 5

$G = S_1 \times \cdots \times S_t$, $S = S_1$ and let $A_1 = N_A(S)$. Observe that $A_1/C_A(S)$ is a coprime group of automorphisms of S.

If $A_1 = 1$, then $|A| = t$ and A acts on G by permuting the coordinates of $S_1 \times \cdots \times S_t$

Theorem (Guralnick-Tiep, 2015)

Let G be a finite group. Then G is soluble if and only if $x_1x_2x_3 \neq 1$ for all nontrivial p_i-elements x_i of G for distinct primes p_i, $i = 1, 2, 3$

So there exist distinct primes p and q, a Sylow p-subgr. P_1 and a Sylow q-subgr. Q_1 of S_1, $x_1 \in P_1$ and $y_1 \in Q_1$ such that $\langle x_1, y_1 \rangle$ is insoluble.

Insight of the proof of Theorem 5

$G = S_1 \times \cdots \times S_t$, $S = S_1$ and let $A_1 = N_A(S)$. Observe that $A_1/C_A(S)$ is a coprime group of automorphisms of S.

If $A_1 = 1$, then $|A| = t$ and A acts on G by permuting the coordinates of $S_1 \times \cdots \times S_t$

Theorem (Guralnick-Tiep, 2015)

Let G be a finite group. Then G is soluble if and only if $x_1x_2x_3 \neq 1$ for all nontrivial p_i-elements x_i of G for distinct primes p_i, $i = 1, 2, 3$

So there exist distinct primes p and q, a Sylow p-subgr. P_1 and a Sylow q-subgr. Q_1 of S_1, $x_1 \in P_1$ and $y_1 \in Q_1$ such that $\langle x_1, y_1 \rangle$ is insoluble.

The direct product P of the distinct A-conjugates of P_1 is an A-invariant Sylow p-subgr. and
the direct product Q of the distinct A-conjugates of Q_1, is an A-invariant Sylow q-subgr. of G.

Insight of the proof of Theorem 5

$G = S_1 \times \cdots \times S_t$, $S = S_1$ and let $A_1 = N_A(S)$. Observe that $A_1/C_A(S)$ is a coprime group of automorphisms of S.

If $A_1 = 1$, then $|A| = t$ and A acts on G by permuting the coordinates of $S_1 \times \cdots \times S_t$

Theorem (Guralnick-Tiep, 2015)

Let G be a finite group. Then G is soluble if and only if $x_1x_2x_3 \neq 1$ for all nontrivial p_i-elements x_i of G for distinct primes p_i, $i = 1, 2, 3$

So there exist distinct primes p and q, a Sylow p-subgr. P_1 and a Sylow q-subgr. Q_1 of S_1, $x_1 \in P_1$ and $y_1 \in Q_1$ such that $\langle x_1, y_1 \rangle$ is insoluble.

The direct product P of the distinct A-conjugates of P_1 is an A-invariant Sylow p-subgr. and
the direct product Q of the distinct A-conjugates of Q_1, is an A-invariant Sylow q-subgr. of G.
Note that $[x_1, \alpha] \in [P, \alpha]$, $[y_1, \alpha] \in [Q, \alpha]$ and $\langle [x_1, \alpha], [y_1, \alpha] \rangle$ is insoluble.

Assume now that $A_1 = N_A(S) \neq 1$.

Then $S = L(q)$ is a group of Lie type, say over the field of $q = p^s$ elements and A_1 induces a cyclic group of field automorphisms.

Assume now that $A_1 = N_A(S) \neq 1$.

Then $S = L(q)$ is a group of Lie type, say over the field of $q = p^s$ elements and A_1 induces a cyclic group of field automorphisms.

Also observe that

the centralizer $C_S(A_1) = L(q_0)$ is a group of the same Lie type defined over the subfield of $q_0 = p^{s/e}$ elements, if e is the order of A_1.

Assume now that $A_1 = N_A(S) \neq 1$.

Then $S = L(q)$ is a group of Lie type, say over the field of $q = p^s$ elements and A_1 induces a cyclic group of field automorphisms.

Also observe that

the centralizer $C_S(A_1) = L(q_0)$ is a group of the same Lie type defined over the subfield of $q_0 = p^{s/e}$ elements, if e is the order of A_1.

After some work we are reduced to consider the cases:

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

Primitive prime divisors

For $q = p^s$, a power of a prime p and for any positive integer n, recall that a prime r is said to be 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

For $q = p^s$, a power of a prime p and for any positive integer n, recall that a prime r is said to be 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.

Primitive prime divisors

For $q = p^s$, a power of a prime p and for any positive integer n, recall that a prime r is said to be 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 is on the existence of primitive prime divisors.

Theorem (Zsigmondy, 1892)

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 $2^3 + 1^3$.

Let $S = \mathrm{PSL}_2(q)$ with $q = p^s$ for s odd and $s \geq 5$.
Recall that $G = S_1 \times \cdots \times S_t$, $S = S_1$ and $A_1 = N_A(S) \neq 1$.

Let $S = \mathrm{PSL}_2(q)$ with $q = p^s$ for s odd and $s \geq 5$.
Recall that $G = S_1 \times \cdots \times S_t$, $S = S_1$ and $A_1 = N_A(S) \neq 1$.

Take U to be an A_1-invariant Sylow p-subgroup of S.

Let $S = \mathrm{PSL}_2(q)$ with $q = p^s$ for s odd and $s \geq 5$.
Recall that $G = S_1 \times \cdots \times S_t$, $S = S_1$ and $A_1 = N_A(S) \neq 1$.

Take U to be an A_1-invariant Sylow p-subgroup of S.

Let r be a *primitive prime divisor* of $q + 1$, i.e. r does not divide $p^i + 1$ for $i < s$ (which exists by Zsigmondy's Theorem).

Let $S = \mathrm{PSL}_2(q)$ with $q = p^s$ for s odd and $s \geq 5$.
Recall that $G = S_1 \times \cdots \times S_t$, $S = S_1$ and $A_1 = N_A(S) \neq 1$.

Take U to be an A_1-invariant Sylow p-subgroup of S.

Let r be a *primitive prime divisor* of $q + 1$, i.e. r does not divide $p^i + 1$ for $i < s$ (which exists by Zsigmondy's Theorem). Let R be an A_1-invariant Sylow r-subgroup of S.

Let $S = \mathrm{PSL}_2(q)$ with $q = p^s$ for s odd and $s \geq 5$.
Recall that $G = S_1 \times \cdots \times S_t$, $S = S_1$ and $A_1 = N_A(S) \neq 1$.

Take U to be an A_1-invariant Sylow p-subgroup of S.

Let r be a *primitive prime divisor* of $q+1$, i.e. r does not divide $p^i + 1$ for $i < s$ (which exists by Zsigmondy's Theorem). Let R be an A_1-invariant Sylow r-subgroup of S.

Both U and R are contained in A-invariant Sylow subgroups (take the product of the distinct t conjugates under A).

Let $S = \mathrm{PSL}_2(q)$ with $q = p^s$ for s odd and $s \geq 5$.
Recall that $G = S_1 \times \cdots \times S_t$, $S = S_1$ and $A_1 = N_A(S) \neq 1$.

Take U to be an A_1-invariant Sylow p-subgroup of S.

Let r be a *primitive prime divisor* of $q + 1$, i.e. r does not divide $p^i + 1$ for $i < s$ (which exists by Zsigmondy's Theorem). Let R be an A_1-invariant Sylow r-subgroup of S.

Both U and R are contained in A-invariant Sylow subgroups (take the product of the distinct t conjugates under A).

Observe that:

- any $1 \neq x \in R$ and any $1 \neq y \in U$ generate S (insoluble);
- $[U, \alpha]$ and $[R, \alpha]$ are contained in $J_{G,A}(\alpha)$.

Let $S = \mathrm{PSL}_2(q)$ with $q = p^s$ for s odd and $s \geq 5$.
Recall that $G = S_1 \times \cdots \times S_t$, $S = S_1$ and $A_1 = N_A(S) \neq 1$.

Take U to be an A_1-invariant Sylow p-subgroup of S.

Let r be a *primitive prime divisor* of $q+1$, i.e. r does not divide $p^i + 1$ for $i < s$ (which exists by Zsigmondy's Theorem). Let R be an A_1-invariant Sylow r-subgroup of S.

Both U and R are contained in A-invariant Sylow subgroups (take the product of the distinct t conjugates under A).

Observe that:

- any $1 \neq x \in R$ and any $1 \neq y \in U$ generate S (insoluble);
- $[U, \alpha]$ and $[R, \alpha]$ are contained in $J_{G,A}(\alpha)$.

If $\alpha \in A_1$, then α induces a non-trivial automorphisms on S and $[U, \alpha] \neq 1$. Since r does not divide the order of $C_S(\alpha)$, we have $[R, \alpha] = R$. If $1 \neq x \in [U, \alpha]$ and $1 \neq y \in [R, \alpha]$, then x, y are as required.

Let $S = \mathrm{PSL}_2(q)$ with $q = p^s$ for s odd and $s \geq 5$.
Recall that $G = S_1 \times \cdots \times S_t$, $S = S_1$ and $A_1 = N_A(S) \neq 1$.

Take U to be an A_1-invariant Sylow p-subgroup of S.

Let r be a *primitive prime divisor* of $q+1$, i.e. r does not divide $p^i + 1$ for $i < s$ (which exists by Zsigmondy's Theorem). Let R be an A_1-invariant Sylow r-subgroup of S.

Both U and R are contained in A-invariant Sylow subgroups (take the product of the distinct t conjugates under A).

Observe that:

- any $1 \neq x \in R$ and any $1 \neq y \in U$ generate S (insoluble);
- $[U, \alpha]$ and $[R, \alpha]$ are contained in $J_{G,A}(\alpha)$.

If $\alpha \in A_1$, then α induces a non-trivial automorphisms on S and $[U, \alpha] \neq 1$. Since r does not divide the order of $C_S(\alpha)$, we have $[R, \alpha] = R$. If $1 \neq x \in [U, \alpha]$ and $1 \neq y \in [R, \alpha]$, then x, y are as required.

If $\alpha \notin A_1$, then α conjugates S to some other component S_i, and so the pair $[x, \alpha]$ and $[y, \alpha]$ generate an insoluble subgr.

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

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

The maximal subgroups of S 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 $(q+l+1)(q-l+1) = q^2+1$.

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

The maximal subgroups of S 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 A_1-invariant Sylow r-subgroup.

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

The maximal subgroups of S 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 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 so also u does not divide $q^2 + 1$. Let U be an A_1-invariant Sylow u-subgroup of S.

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

The maximal subgroups of S 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 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 so also u does not divide q^2+1. Let U be an A_1-invariant Sylow u-subgroup of S.

Observe that:

- There is no proper subgroup of S whose order is divisible by ru;
- Neither of R and U intersects $C_S(\alpha)$, so $[R, \alpha] = R$ and $[U, \alpha] = U$.
- Any element in R or U is a commutator with α.

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

The maximal subgroups of S 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 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 so also u does not divide q^2+1. Let U be an A_1-invariant Sylow u-subgroup of S.

Observe that:

- There is no proper subgroup of S whose order is divisible by ru;
- Neither of R and U intersects $C_S(\alpha)$, so $[R,\alpha] = R$ and $[U,\alpha] = U$.
- Any element in R or U is a commutator with α.

As before, if $\alpha \in A_1$, then $1 \neq x \in [U,\alpha]$ and $1 \neq y \in [R,\alpha]$ generate S.

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

The maximal subgroups of S 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 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 so also u does not divide q^2+1. Let U be an A_1-invariant Sylow u-subgroup of S.

Observe that:

- There is no proper subgroup of S whose order is divisible by ru;
- Neither of R and U intersects $C_S(\alpha)$, so $[R, \alpha] = R$ and $[U, \alpha] = U$.
- Any element in R or U is a commutator with α.

As before, if $\alpha \in A_1$, then $1 \neq x \in [U, \alpha]$ and $1 \neq y \in [R, \alpha]$ generate S.

If $\alpha \notin A_1$, then take $x \in R$, $y \in U$ and the pair $[x, \alpha]$ and $[y, \alpha]$ generate an insoluble group. □

Criteria for nilpotency of $[G, \alpha]$

As a consequence of the previous result we get necessary and sufficient conditions for the nilpotency of $[G, \alpha]$.

Criteria for nilpotency of $[G, \alpha]$

As a consequence of the previous result we get necessary and sufficient conditions for the nilpotency of $[G, \alpha]$.

Theorem 6

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 $\pi(xy) = \pi(x) \cup \pi(y)$.

where $\pi(x)$ denotes the set of prime divisors of the order $|x|$ of x in G.

A consequence that was a motivation

Theorem (Baumslag- Wiegold, 2014)

Let G be a finite group. Then G is nilpotent if and only if $|xy| = |x||y|$, whenever the elements x and y have coprime orders.

A consequence that was a motivation

Theorem (Baumslag- Wiegold, 2014)

Let G be a finite group. Then G is nilpotent if and only if $|xy| = |x||y|$, whenever the elements x and y have coprime orders.

Form Theorem 6 we can deduce the following variation of the Baumslag-Wiegold result.

Theorem 7

Let G be a finite group admitting a coprime automorphism α. Then $[G, \alpha]$ is nilpotent if, and only if, $|xy| = |x||y|$ whenever x and y are elements of coprime prime power orders from $I_G(\alpha)$.

Recall that $I_G(\alpha)$ is the set of all commutators $g^{-1}g^{\alpha}$, where $g \in G$.

A consequence that was a motivation

Theorem (Baumslag- Wiegold, 2014)

Let G be a finite group. Then G is nilpotent if and only if $|xy| = |x||y|$, whenever the elements x and y have coprime orders.

Form Theorem 6 we can deduce the following variation of the Baumslag-Wiegold result.

Theorem 7

Let G be a finite group admitting a coprime automorphism α. Then $[G, \alpha]$ is nilpotent if, and only if, $|xy| = |x||y|$ whenever x and y are elements of coprime prime power orders from $I_G(\alpha)$.

Recall that $I_G(\alpha)$ is the set of all commutators $g^{-1}g^{\alpha}$, where $g \in G$.

Remark: at the beginning it was unclear whether the hypothesis on the orders of elements in Theorem 7 is inherited by quotient groups. To overcome this issue we started working with elements of coprime orders from $J_G(\alpha)$ and $J_{G,A}(\alpha)$.

More details can be found in

- C.Acciarri,R.M.Guralnick,and P.Shumyatsky,Coprime automorphisms of finite groups, Trans. Amer. Math. Soc. (2022). 375:7, 4549–4565. https://doi.org/10.1090/tran/8553
- C.Acciarri,R.M.Guralnick,and P.Shumyatsky, Criteria for solubility and nilpotency of finite groups with automorphisms, Bull. London Math. Soc. 2023; 55:3, 1340–1346. https://doi.org/10.1112/blms.12794

Thank you!

acciarricristina.wixsite.com/pavel60

Finite and Residually Finite Groups

A conference celebrating Pavel Shumyatsky's 60th Birthday

20th-23rd JUNE 2023
Bilbao- Basque Country- Spain

Invited Speakers

Cristina Acciarri, University of Modena and Reggio Emilia
Rostislav Grigorchuk, Texas A&M University
Evgeny Khukhro, University of Lincoln
Benjamin Klopsch, Heinrich-Heine-Universität
Mahmut Kuzucuoğlu, Middle East Technical University
Andrea Lucchini, University of Padova
Mercede Maj, University of Salerno
Natalia Maslova, Ural Federal University
Marta Morigi, University of Bologna
Pavel Shumyatsky, University of Brasilia
Gunnar Traustason, University of Bath
Pavel Zalesski, University of Brasilia
Efim Zelmanov, SUSTech

See More at

Organizing and Scientific Committee

Cristina Acciarri (University of Modena and Reggio Emilia)
Eloisa Detomi (University of Padova)
Gustavo A. Fernández Alcober (University of the Basque Country)
Leire Legarreta Solaguren (University of the Basque Country)
Andrea Lucchini (University of Padova)

E-mail: pavel60conference@gmail.com

FOUNDATION COMPOSITIO MATHEMATICA
Università degli Studi di Padova
Eusko Jaurlaritza Gobierno Vasco
UnB
UPV EHU