Schur's exponent conjecture for p-groups of class p

Patali K.

IISER TVM

June 5, 2020

Let G be a group.

The Schur Multiplier $M(G)$ of G :

The second homology group $H_2(G, \mathbb{Z})$ of G with coefficients in integers.

Conjecture:

Does $\exp(M(G)) \mid \exp(G)$ for every group G?

Let G be a group.

The Schur Multiplier $M(G)$ of G :

The second homology group $H_2(G, \mathbb{Z})$ of G with coefficients in integers.

Conjecture:

Does $\exp(M(G)) \mid \exp(G)$ for every group G?

Theorem A (A. Antony, P. Komma, V.Z. Thomas, Commutator expansions and the Schur Multiplier 2019)

Let G be a finite p-group of class p, then the exponent of the Schur multiplier $M(G)$ of G divides the exponent of G.

Notations

Notations:

- ${}^{x}y = xyx^{-1}$ and $[x, y] = xyx^{-1}y^{-1}$.
- right normed notation for commutators:
  $[z, y, x]$ denote $[z, [y, x]]$.
- $[\,_n x, y] = [\underbrace{x, x, \ldots, x}_{n\text{-times}}, y]$.
- $\gamma_1(G) = G$, $\gamma_i(G) = [G, \gamma_{i-1}(G)]$ for $i \geq 2$.
  The nilpotency class of G is c if $\gamma_c(G) \neq \{e\}$ and $\gamma_{c+1}(G) = \{e\}$.
- A group G is n-central if $g^n \in Z(G)$ for every $g \in G$. In other words G is n-central if $\exp(\frac{G}{Z(G)}) \mid n$.

Theorem B

Definition

A covering group of G is a central extension

$$0 \to Z \to E \to G \to 1$$

of G such that $Z \subset Z(E) \cap \gamma_2(E)$ and $Z \cong M(G)$.

Theorem B

Let G be a p-group of class $p+1$. If G is p^n-central then $exp(\gamma_2(G)) \mid p^n$.

To prove Theorem A it is enough to prove Theorem B.

Theorem B

Definition

A covering group of G is a central extension

$$0 \to Z \to E \to G \to 1$$

of G such that $Z \subset Z(E) \cap \gamma_2(E)$ and $Z \cong M(G)$.

Theorem B

Let G be a p-group of class $p+1$. If G is p^n-central then $exp(\gamma_2(G)) \mid p^n$.

To prove Theorem A it is enough to prove Theorem B.

Lemma

Let G be a regular p-group or a p-group of class p. If G is p^n-central, then $exp(\gamma_2(G)) \mid p^n$.

Commutator collection formula

Let G be a group $a, b \in G$. Then
$\mathcal{A}_i(\{a, b\})$ denote all basic commutators of a, b of weight $\leq i$.
Commutator collection formula:

$$(ab)^n = \prod_{C \in \mathcal{A}_i(\{a,b\})} C^{f_C(n)} a^n b^n \mod \gamma_{i+1}(\langle a, b \rangle).$$

Commutator collection formula

Let G be a group $a, b \in G$. Then
$\mathcal{A}_i(\{a, b\})$ denote all basic commutators of a, b of weight $\leq i$.
Commutator collection formula:

$$(ab)^n = \prod_{C \in \mathcal{A}_i(\{a,b\})} C^{f_C(n)} a^n b^n \mod \gamma_{i+1}(\langle a, b \rangle).$$

For a basic commutator C of a, b

$$f_C(n) = a_1 \binom{n}{1} + \cdots + a_{r_C} \binom{n}{r_C}$$

where r_C is the largest r with $a_r \neq 0$, a_i are non negative integers depending only on the commutator C. Moreover, $r_C \leq$ weight of C in a, b.
Remark :
Let p be a prime. Then $p^n \mid \binom{p^n}{r}$ for $r < p$.

Proof of Theorem B:
We have $\text{class}(G) = p + 1$, and $G^{p^n} \subset Z(G)$.
claim: $[b, a]^{p^n} = 1$ for every $a, b \in G$.

Proof of Theorem B

Proof of Theorem B:

We have $\text{class}(G) = p + 1$, and $G^{p^n} \subset Z(G)$.

claim: $[b, a]^{p^n} = 1$ for every $a, b \in G$.

$$1 = [b, a^{p^n}] = ba^{p^n}b^{-1}a^{-p^n} = ({}^{b}a)^{p^n}a^{-p^n} = ([b, a]a)^{p^n}a^{-p^n}.$$

Applying commutator collection formula we obtain

$$1 = \prod_{C \in \mathcal{A}_p(\{[b,a],a\})} C^{f_C(p^n)}[b, a]^{p^n}.$$

Proof of Theorem B

Proof of Theorem B:

We have $\mathrm{class}(G) = p+1$, and $G^{p^n} \subset Z(G)$.

claim: $[b,a]^{p^n} = 1$ for every $a, b \in G$.

$$1 = [b, a^{p^n}] = ba^{p^n}b^{-1}a^{-p^n} = ({}^{b}a)^{p^n}a^{-p^n} = ([b,a]a)^{p^n}a^{-p^n}.$$

Applying commutator collection formula we obtain

$$1 = \prod_{C \in \mathcal{A}_p(\{[b,a],a\})} C^{f_C(p^n)}[b,a]^{p^n}.$$

- If $\mathrm{weight}(C) \leq p-1$ in $a, [b,a]$ then $p^n \mid f_C(p^n)$. As class $(\langle [b,a], a\rangle) \leq p$, $C^{p^n} = 1$.

Proof of Theorem B:
We have class$(G) = p+1$, and $G^{p^n} \subset Z(G)$.
claim: $[b,a]^{p^n} = 1$ for every $a, b \in G$.

$$1 = [b, a^{p^n}] = ba^{p^n}b^{-1}a^{-p^n} = ({}^{b}a)^{p^n}a^{-p^n} = ([b,a]a)^{p^n}a^{-p^n}.$$

Applying commutator collection formula we obtain

$$1 = \prod_{C \in \mathcal{A}_p(\{[b,a],a\})} C^{f_C(p^n)}[b,a]^{p^n}.$$

- If weight$(C) \leq p-1$ in $a, [b,a]$ then $p^n \mid f_C(p^n)$. As class $(\langle [b,a], a\rangle) \leq p$, $C^{p^n} = 1$.
- If C has weight r in $[b,a]$ and $p-r$ in a, then $C \in \gamma_{2r+p-r}(G)$. $\gamma_{p+2}(G) = 1$ gives $2r + p - r = p+1$. Thus $r = 1$ and $C = [\,_{p-1}a, [b,a]]$.

Proof of the Theorem B

- We deduce that

$$1 = [\ _{p-1}a, [b, a]]^{\binom{p^n}{p}} [b, a]^{p^n}. \tag{0.1}$$

Proof of the Theorem B

- We deduce that
$$1 = [\ _{p-1}a, [b,a]]^{\binom{p^n}{p}}[b,a]^{p^n}. \tag{0.1}$$

- By replacing a with ab in equation (0.1) we have
$$\Big(\prod_{x_i \in \{a,b\}} [x_{p-1}, x_{p-2}, \dots, x_1, [b,a]]\Big)^{\binom{p^n}{p}}[b,a]^{p^n} = 1. \tag{0.2}$$

- Let $E_r = \prod_{x_i \in \{a,b\}, x_i = b \text{ for exactly } r \ x_i's} [x_{p-1}, x_{p-2}, \dots, x_1, [b,a]]$, $0 \le r \le p - a$.

Proof of the Theorem B

- We deduce that
$$1 = [\ _{p-1}a, [b, a]]^{\binom{p^n}{p}} [b, a]^{p^n}. \qquad (0.1)$$

- By replacing a with ab in equation (0.1) we have
$$\Big(\prod_{x_i \in \{a,b\}} [x_{p-1}, x_{p-2}, \ldots, x_1, [b, a]] \Big)^{\binom{p^n}{p}} [b, a]^{p^n} = 1. \qquad (0.2)$$

- Let $E_r = \prod_{x_i \in \{a,b\}, x_i = b \text{ for exactly } r \ x_i's} [x_{p-1}, x_{p-2}, \ldots, x_1, [b, a]]$, $0 \leq r \leq p - a$.

- The above equation becomes $\big(\prod_{r=0}^{p-1} E_r \big)^{\binom{p^n}{p}} [b, a]^{p^n} = 1$. Comparing it with (0.1) gives
$$\Big(\prod_{r=1}^{p-1} E_r \Big)^{\binom{p^n}{p}} = 1. \qquad (0.3)$$

Proof of Theorem B

Definition

$\alpha_m(n) = \sum_{1 \leq i_1 < i_2 < \cdots < i_{m-1} < n} \binom{n}{i_{m-1}} \binom{i_{m-1}}{i_{m-2}} \ldots \binom{i_2}{i_1}$, where $1 < m \leq n \in \mathbb{N}$.

Proof of Theorem B

Definition

$\alpha_m(n) = \sum_{1\le i_1<i_2<\cdots<i_{m-1}<n} \binom{n}{i_{m-1}}\binom{i_{m-1}}{i_{m-2}}\dots\binom{i_2}{i_1}$, where $1 < m \le n \in \mathbb{N}$.

Example :

The values of $\alpha_m(n)$ for $2 \le m \le n \le 4$ are listed below:

$$\alpha_2(2) = \binom{2}{1} = 2,\ \ \alpha_2(3) = \binom{3}{1} + \binom{3}{2} = 6,$$

$$\alpha_2(4) = \binom{4}{1} + \binom{4}{2} + \binom{4}{3} = 14,$$

$$\alpha_3(3) = \binom{3}{2}\binom{2}{1} = 6,\ \ \alpha_3(4) = \binom{4}{2}\binom{2}{1} + \binom{4}{3}\binom{3}{1} + \binom{4}{3}\binom{3}{2} = 36,$$

$$\alpha_4(4) = \binom{4}{3}\binom{3}{2}\binom{2}{1} = 24.$$

Proof of Theorem B

Observation: Replacing a with ab in E_r gives $\prod_{s=r}^{p-1} E_s^{\binom{s}{r}}$.

Lemma 2

For $2 < m \leq n$, $\alpha_m(n) = \sum_{k=m-1}^{n-1} \binom{n}{k} \alpha_{m-1}(k)$.

Proof of Theorem B

Observation: Replacing a with ab in E_r gives $\prod_{s=r}^{p-1} E_s^{\binom{s}{r}}$.

Lemma 2

For $2 < m \leq n$, $\alpha_m(n) = \sum_{k=m-1}^{n-1} \binom{n}{k} \alpha_{m-1}(k)$.

$$\text{We prove that for } 2 \leq m \leq p-1, \prod_{k=m}^{p-1} \left({E_k}^{\alpha_m(k)}\right)^{\binom{p^n}{p}} = 1. \tag{0.4}$$

In particular, $E_{p-1}^{\alpha_{p-1}(p-1)\binom{p^n}{p}} = 1$.

Proof of Theorem B

Observation: Replacing a with ab in E_r gives $\prod_{s=r}^{p-1} E_s^{\binom{s}{r}}$.

Lemma 2

For $2 < m \leq n$, $\alpha_m(n) = \sum_{k=m-1}^{n-1} \binom{n}{k} \alpha_{m-1}(k)$.

We prove that for $2 \leq m \leq p-1$,
$$\prod_{k=m}^{p-1} \left({E_k}^{\alpha_m(k)}\right)^{\binom{p^n}{p}} = 1. \tag{0.4}$$

In particular, $E_{p-1}^{\alpha_{p-1}(p-1)\binom{p^n}{p}} = 1$.

- As $\alpha_{p-1}(p-1) = (p-1)!$, $E_{p-1}^{\binom{p^n}{p}} = 1$.

Proof of Theorem B

Observation: Replacing a with ab in E_r gives $\prod_{s=r}^{p-1} E_s^{\binom{s}{r}}$.

Lemma 2

For $2 < m \leq n$, $\alpha_m(n) = \sum_{k=m-1}^{n-1} \binom{n}{k} \alpha_{m-1}(k)$.

$$\text{We prove that for } 2 \leq m \leq p-1, \prod_{k=m}^{p-1} \left({E_k}^{\alpha_m(k)}\right)^{\binom{p^n}{p}} = 1. \tag{0.4}$$

In particular, $E_{p-1}^{\alpha_{p-1}(p-1)\binom{p^n}{p}} = 1$.

- As $\alpha_{p-1}(p-1) = (p-1)!$, $E_{p-1}^{\binom{p^n}{p}} = 1$.
- $E_{p-1} = [\,_{p-1}b, [b, a]]$, $(E_{p-1})^{-1} = [\,_{p-1}b, [a, b]]$. Thus

$$[\,_{p-1}b, [a, b]]^{\binom{p^n}{p}} = 1 \tag{0.5}$$

Interchanging a, b in (0.5) gives $[\,_{p-1}a, [b, a]]^{\binom{p^n}{p}} = 1$ as required.

Example

- Let $p = 5$, equation (0.2) gives

$$(E_1E_2E_3E_4)^{\binom{5^n}{5}} = 1. \tag{0.6}$$

- Replacement of a in (0.6) with ab gives

$$((E_1E_2^2E_3^3E_4^4)(E_2E_3^3E_4^6)(E_3E_4^4)(E_4))^{\binom{5^n}{5}} = 1. \tag{0.7}$$

Example

- Let $p = 5$, equation (0.2) gives

$$(E_1 E_2 E_3 E_4)^{\binom{5^n}{5}} = 1. \tag{0.6}$$

- Replacement of a in (0.6) with ab gives

$$\left((E_1 E_2^2 E_3^3 E_4^4)(E_2 E_3^3 E_4^6)(E_3 E_4^4)(E_4)\right)^{\binom{5^n}{5}} = 1. \tag{0.7}$$

- Comparing (0.6) and (0.7), $\left((E_2^2 E_3^3 E_4^4)(E_3^3 E_4^6)(E_4^4)\right)^{\binom{5^n}{5}} = 1.$

$$\text{Thus } \left(E_2^2 E_3^6 E_4^{14}\right)^{\binom{5^n}{5}} = 1. \tag{0.8}$$

- Again replacement of a in (0.8) with ab yields,

$$\left((E_2 E_3^3 E_4^6)^2 (E_3 E_4^4)^6 E_4^{14}\right)^{\binom{5^n}{5}} = 1. \tag{0.9}$$

Example

- Now by comparing (0.8) and (0.9) we get $\left((E_3^3 E_4^6)^2 (E_4^4)^6\right)^{\binom{5^n}{5}} = 1$. This gives

$$\left(E_3^6 E_4^{36}\right)^{\binom{5^n}{5}} = 1. \tag{0.10}$$

Example

- Now by comparing (0.8) and (0.9) we get $\left((E_3^3 E_4^6)^2 (E_4^4)^6\right)^{\binom{5^n}{5}} = 1$. This gives

$$\left(E_3^6 E_4^{36}\right)^{\binom{5^n}{5}} = 1. \quad (0.10)$$

- After replacing a in (0.10) with ab, (0.10) becomes

$$\left((E_3 E_4^4)^6 E_4^{36}\right)^{\binom{5^n}{5}} = 1. \quad (0.11)$$

Example

- Now by comparing (0.8) and (0.9) we get $\left((E_3^3 E_4^6)^2 (E_4^4)^6\right)^{\binom{5^n}{5}} = 1$. This gives

$$\left(E_3^6 E_4^{36}\right)^{\binom{5^n}{5}} = 1. \tag{0.10}$$

- After replacing a in (0.10) with ab, (0.10) becomes

$$\left((E_3 E_4^4)^6 E_4^{36}\right)^{\binom{5^n}{5}} = 1. \tag{0.11}$$

- Finally comparing (0.10) and (0.11) yields

$$\left(E_4^{24}\right)^{\binom{5^n}{5}} = 1. \tag{0.12}$$

Thank You