

A Bound for the Exponent of the Schur Multiplier of Some Finite p -Groups*

S.Kayvanfar¹ and M.A.Sanati²

Institute for studies in Theoretical Physics and Mathematics¹

and

Department of Mathematics, Mashhad University, Mashhad, Iran^{1,2}

E-mail: skayvanf@science2.um.ac.ir

Abstract

Let G be a finite p -group of exponent p^e . The paper is devoted to present a new bound for the exponent of the Schur multiplier of G , when G is of class 3, 4 or 5 and e satisfies in some conditions.

1991 Mathematics Subject Classification (Amer. Math. Soc.)

*The first author's research was partially supported by IPM.

20D15, 20F12.

Keywords: exponent, covering group, Schur multiplier, p -group.

1. Introduction and Motivation

It has been conjectured that the exponent of the Schur multiplier of a finite p -group is a divisor of the exponent of the group itself. I.D.Macdonld, J.W.Wamsley and others have constructed an example of a group of exponent 4 whereas its Schur multiplier has exponent 8, namely, the conjecture is not true in general. On the other hand M.R.Jones has shown in [3] that the conjecture is true for p -groups of class 2 and emphasized that it is true for some p -groups of class 3, but he did not characterize in which conditions it may be true. He has also proved that if G is a p -group of class $c \geq 2$ and $e(G) = p^e$, then $e(M(G)) \leq p^{e(c-1)}$ (see [3, Corollary 2.7]), in which $e(X)$ denotes the exponent of a group X . A result of G.Ellis [2, Theorem B(i)] shows that with these assumptions we have $e(M(G)) \leq p^{\lceil c/2 \rceil e}$, where $\lceil c/2 \rceil$ denotes the smallest integer n such that $n \geq c/2$. Clearly the recent bound sharpens the bound obtained by M.R.Jones.

In this paper we show that the conjecture is true for p -groups of class 4 and 5, when e is odd or $p \not\equiv -1$ modulo 3 and 4 (Theorems 2.2, 2.5 and Remark

2.8). It is also shown that for such e or p , we have; $e(M(G)) \leq p^e$ (Corollaries 2.4, 2.7 and Remark 2.8). This sharpens (under some assumptions) the above result of M.R.Jones [3] and also the results of J.Burns and G.Ellis [1] and G.Ellis [2] for $c=3, 4$ and 5 .

Notation. Let x and y be two elements of a group G , then $[x, y]$, the *commutator* of x and y , and x^y denote the elements $x^{-1}y^{-1}xy$ and $y^{-1}xy$, respectively. The commutator of higher weight is defined inductively as follows; $[x_1, x_2, \dots, x_{n-1}, x_n] = [[x_1, x_2, \dots, x_{n-1}], x_n]$ ($n > 2$). The *lower central series* of a group G is denoted by $\gamma_1(G) = G \supseteq \gamma_2(G) = G' \supseteq \gamma_3(G) \supseteq \dots \supseteq \gamma_n(G) \supseteq \gamma_{n+1}(G) \supseteq \dots$, in which $\gamma_n(G) = [G, \gamma_{n-1}(G)] = [G, G, \dots, G]$, (G is repeated n times), ($n \geq 2$), Finally the minimum number of generators of a group X is denoted by $d(X)$. Other notations, where not explained, will be standard.

Theorem 1.1. (Schur 1907) Let G be a finite group and $1 \rightarrow R \rightarrow F \rightarrow G \rightarrow 1$ be a free presentation for G . Then $M(G) \cong (R \cap F')/[R, F]$.

Definition 1.2. Let G be a group. An exact sequence $1 \rightarrow A \rightarrow G^* \rightarrow G \rightarrow 1$ (*), where $A \subseteq Z(G^*) \cap G^{*'}$ is called a *stem-extension* of G . If furthermore $A \cong M(G)$, then (*) is called a *stem-cover* of G and in this case G^* is said to be a *covering group* of G .

It is known that such a G^* always exists although need not be unique.

2. The Bound Obtained

In order to establish our main result, we need the following technical lemma.

Lemma 2.1. Let X be a group and $x, y \in X$. Then for every positive integer n , we have the following identity modulo $\gamma_7(X)$;

$$[x, y^n] = \prod_{r=1}^5 [x, {}_r y] \binom{n}{r} \prod_{s=0}^1 [x, y, [y, [x, y]], {}_s y] \binom{n}{s+2} ,$$

in which $[a, {}_k b]$ is $[a, b, b, \dots, b]$ (b is repeated k times).

Proof. The proof can be done using induction on n . \square

Theorem 2.2. Let G be a finite p -group ($p > 3$) of class 4 and $e(G) = p^e$ in which e is an odd number. If G^* is a covering group of G , then

$$e(G^*) \mid e(G) .$$

Proof. Suppose that $G = \langle g_1, g_2, \dots, g_{d(G)} \rangle$ and $f : G^* \rightarrow G$ is the epimorphism satisfied in the definition of the covering group. Let $u_i \in G^*$

be such that $f(u_i) = g_i$ for $1 \leq i \leq d(G)$. Since $\ker f \subseteq \Phi(G^*)$, then $G^* = \langle u_1, u_2, \dots, u_{d(G)} \rangle$.

For each $x_1 \in G^*$ we have $[u_i, u_j, x_1]^{p^e} \in Z(G^*)$, ($1 \leq i, j \leq d(G)$), therefore $[[u_i, u_j, x_1]^{p^e}, x_2] = 1$, for all $x_2 \in G^*$. Now using Lemma 2.1, one can easily check that

$$[u_i, u_j, x_1, x_2]^{p^e} = 1 ; \quad \forall x_1, x_2 \in G^*. \quad (1)$$

A similar argument shows that:

$$[u_i, u_j, x_1, x_2, x_3]^{p^e} = 1 ; \quad \forall x_1, x_2, x_3 \in G^*. \quad (2)$$

On the other hand for all $x \in G^*$; $[u_i, u_j, x]^{p^e} = 1$, ($1 \leq i, j \leq d(G)$). By applying Lemma 2.1, it is concluded that

$$[u_i, u_j, x]^{p^e} [u_i, u_j, x, x]^{p^e(p^e-1)/2} [u_i, u_j, x, x, x]^{p^e(p^e-1)(p^e-2)/6} = 1 . \quad (3)$$

Clearly $(p^e - 1)/2 \in \mathbf{Z}$, hence $[u_i, u_j, x, x]^{p^e(p^e-1)/2} = 1$, by (1). Also if $p \equiv 1 \pmod{3}$, then $3|p^e - 1$ and so $6|p^e - 1$, and if $p \equiv -1 \pmod{3}$, then $3|p^e - 2$ (since e is odd) and hence $6|(p^e - 1)(p^e - 2)$. Therefore in any case we have $[u_i, u_j, x, x, x]^{p^e(p^e-1)(p^e-2)/6} = 1$, by (2). Now (3) follows that

$$[u_i, u_j, x]^{p^e} = 1 , \quad \forall x \in G^*. \quad (4)$$

In the following we intend to prove that $[u_i, u_j]^{p^e} = 1$.

The property of covering group implies that $u_j^{p^e} \in Z(G^*)$ and so $[u_i, u_j^{p^e}] = 1$. Therefore by Lemma 2.1 and the above comments it is enough to show that

$$[u_i, {}_4u_j]^{p^e(p^e-1)(p^e-2)(p^e-3)/24} = 1,$$

and by (2), we must illustrate that $24|(p^e - 1)(p^e - 2)(p^e - 3)$.

(Note that :

$$[u_i, u_j, [u_j, [u_i, u_j]]]^{p^e} = 1 ,$$

$$[u_i, u_j, [u_j, [u_i, u_j]], u_j] = 1 .)$$

We consider two cases :

Case 1. $p \equiv 1 \pmod{4}$. If $p \equiv 1 \pmod{3}$, then $12|p^e - 1$ and since $p^e - 3$ is even, hence $24|(p^e - 1)(p^e - 3)$. If $p \equiv -1 \pmod{3}$, then $3|p^e - 2$. But $4|p^e - 1$ and $2|p^e - 3$. Whence we are done.

Case 2. $p \equiv -1 \pmod{4}$. It follows that $4|p^e - 3$. If $p \equiv 1 \pmod{3}$, then $6|p^e - 1$ and so $24|(p^e - 1)(p^e - 3)$. Let $p \equiv -1 \pmod{3}$, then $3|p^e - 2$ and also $2|p^e - 1$, $4|p^e - 3$. They therefore follow that $24|(p^e - 1)(p^e - 2)(p^e - 3)$, as required.

(Recall that p is odd and so $p \not\equiv 2 \pmod{4}$). \square

The argument which is done in the proof of Theorem 2.2, shows that in some cases, it can be omitted the extra condition to be odd for e . In other words we have;

Corollary 2.3. Let G be a finite p -group ($p > 3$) of class 4 and $p \not\equiv -1$ modulo 3 and 4. Suppose also that G^* is a covering group of G , then $e(G^*) \mid e(G)$. \square

As it is mentioned in the introduction, the following corollary sharpens the bound of M.R.Jones [3, Corollary 2.7] and J.Burns and G.Ellis [1, Theorem 6] and G.Ellis [2, Theorem B (i)] on the exponent of the Schur multiplier of some prime-power groups.

Corollary 2.4. Let G be a finite p -group ($p > 3$) of class 4 and $e(G) = p^e$. Then

$$e(M(G)) \leq p^e ,$$

when one of the following conditions hold:

- (i) e is an odd number.
- (ii) $p \not\equiv -1$ modulo 3 and 4.

(Note that \leq can be taken to mean “divides”).

In the next theorem we show that our above results can be extended to p -groups of one class more.

Theorem 2.5. Let $p > 5$ be a prime and G be a finite p -group of class 5 with $e(G) = p^e$, in which e is odd. If G^* is a covering group of G , then $e(G^*) \mid e(G)$.

Proof. We keep all the notations used in the proof of Theorem 2.2. By a similar argument which is applied in the proof of Theorem 2.2 and repeated use of Lemma 2.1, one can prove that;

$$[u_i, {}_t u_j]^{p^e} = 1 \quad (2 \leq t \leq 5), \quad (5)$$

$$[u_i, u_j, [u_j, [u_i, u_j]]]^{p^e} = 1, \quad (6)$$

$$[u_i, u_j, [u_j, [u_i, u_j]], u_j]^{p^e} = 1. \quad (7)$$

(Note that in Theorem 2.2, $\gamma_6(G^*) = 1$ whereas our recent assumption implies that $\gamma_7(G^*) = 1$.)

On the other hand, since $[u_i, u_j^{p^e}] = 1$, ($1 \leq i, j \leq d(G)$), then by Lemma 2.1 we deduce that;

$$\prod_{r=1}^5 [u_i, {}_r u_j]^{p^e} \prod_{s=0}^1 [u_i, u_j, [u_j, [u_i, u_j]], {}_s u_j]^{p^e} = 1 \quad (8)$$

Since $\binom{p^e}{s+2}/p^e \in \mathbf{Z}$, ($s = 0, 1$), it is immediately follows, from the relations (6) and (7) that both terms of the second product is identity. We have also shown in Theorem 2.2 that $\binom{p^e}{r}/p^e \in \mathbf{Z}$ for $r = 2, 3$ and 4. Whence by (5) it is concluded that:

$$[u_i, {}_r u_j]^{p^e} = 1 \quad (2 \leq r \leq 4).$$

We claim that $\binom{p^e}{5}/p^e \in \mathbf{Z}$.

Case 1. $p \equiv 1 \pmod{5}$. Hence $5|p^e - 1$. We know from the previous that $24|(p^e - 1)(p^e - 2)(p^e - 3)$. Consequently $120|(p^e - 1)(p^e - 2)(p^e - 3)(p^e - 4)$.

Case 2. $p \equiv 2 \pmod{5}$. If $e \equiv 1 \pmod{4}$, then we can write $e = 4k + 1$, for some $k \in \mathbf{Z}$. Hence by Fermat theorem $p^e \equiv p \pmod{5}$ and therefore $5|p^e - 2$. Now similar to case 1 we deduce that $\binom{p^e}{5}/p^e \in \mathbf{Z}$. But if $e \equiv 3 \pmod{4}$, then similar previous, it is concluded that $5|p^e - 3$ and so again similar to case 1, the required assertion follows.

Case 3. $p \equiv 3 \pmod{5}$. Similar to case 2, $e \equiv 1 \pmod{4}$ implies that $5|p^e - 3$, and $e \equiv 3 \pmod{4}$ implies that $5|p^e - 2$. In each case we are in a position like case 1.

Case 4. $p \equiv 4 \pmod{5}$. Then $5|p^e - 4$ and the assertion follows immediately.

Now clearly we have $[u_i, {}_5u_j]^{(p^e)} = 1$, by (5). It therefore follows from (8) that $[u_i, u_j]^{p^e} = 1$, as required. \square

The above process shows that the condition of being odd for e can be replaced with the other condition, as follows:

Corollary 2.6. Suppose that G is a finite p -group ($p > 5$) of class 5 and $p \not\equiv -1$ modulo 3 and 4. Then for every covering group G^* of G , we have

$e(G^*) \mid e(G)$.

Proof. Let p^e be the exponent of G . By the assumption $24 \mid (p^e - 1)(p^e - 2)(p^e - 3)$. Now if in addition to cases considered in the proof of the Theorem 2.5, we pay attention to the two cases $e \equiv 0$ or 2 modulo 4 (when e is even), then with a similar argument to Theorem 2.5, the required assertion follows. \square

We are at last in a position to attain our other main objective, which is similar to Corollry 2.4.

Corollary 2.7. If G is a finite p -group ($p > 5$) of class 5 and exponent p^e . Then

$$e(M(G)) \leq p^e ,$$

when one of the following conditions hold:

- (i) e is an odd number.
- (ii) $p \not\equiv -1$ modulo 3 and 4. \square

Corollary 2.7 shows that the bounds p^{4e} and p^{3e} which are obtained for the exponent of the Schur multiplier of p -groups of class 5 in [3] and [2] respectively, can be reduced to p^e for some p -groups.

Remark 2.8. As we mentioned in the introduction, M.R.Jones has stated in [3] that the bound p^e can be obtained for the exponent of the Schur multiplier of some p -groups of class 3. But it has not been exactly determined for which groups it is true. By repeating the argument stated in the proof of Theorem 2.2, one can easily check that $e(M(G)) \leq p^e$, for every p -group ($p > 3$) of class 3, when e is an odd number.

References

- [1] J.Burns and G.Ellis, “Inequalities for Baer invariants of finite groups”, *Canad. Math. Bull.*, to appear (1999).
- [2] G.Ellis, “On the relation between upper central quotients and lower central series of a group”, Max-Planck-Institute preprint, January 1999.
- [3] M.R.Jones, “Some inequalities for the multiplier of a finite group.II”, *Proc. Amer. Math. Soc.* **45** (1974), 167-172.