SCHUR MULTIPLIERS AND POWER ENDOMORPHISMS OF GROUPS

PRIMOŽ MORAVEC

Abstract. We obtain new bounds for the exponent of the Schur multiplier of a given $p$-group. We prove that the exponent of the Schur multiplier can be bounded by a function depending only on the exponent of a given group. As a consequence we show that the exponent of the Schur multiplier of any group of exponent four divides eight, and that this bound is best possible. The notion of the exponential rank of a $p$-group is introduced. We show that powerful $p$-groups have exponential rank either zero or one.

1. Introduction

A group $G$ is said to be $n$-abelian if the map $x \mapsto x^n$ is an endomorphism of $G$. The study of $n$-abelian groups was initiated by Levi in [19], and has been a topic of several other papers, see, e.g., [2, 7, 11, 15, 23]. $n$-abelian groups are closely related to $n$-central groups; here a group $G$ is said to be $n$-central if $G/Z(G)$ has exponent dividing $n$. For instance, it is not difficult to prove that every $n$-abelian group is $n(n-1)$-central. On the other hand, Adjan [1] constructed examples of $n$-central groups which are not $m$-abelian for any $m \neq 0, 1$. Nevertheless, some favorable results in this direction are known. Gupta and Rhemtulla [11] proved that every 2-central group is 4-abelian, every 3-central group is 9-abelian, and every 4-central groups is 32-abelian. This has been further improved in [23] where it has been shown that for $n \in \{2, 3, 4, 6\}$, every $n$-central group is $n^2$-abelian. Other questions related to these classes groups and some generalisations have been considered in [7].

The purpose of this paper is to apply the theory of $n$-central groups in studying Schur multipliers of groups. It turns out that $n$-central groups provide a natural setting in which Schur multipliers can be studied. Namely, if $G$ is a finite group of exponent $n$, then its covering group is $n$-central. Thus several properties of the Schur multiplier $M(G)$ of $G$ can be deduced from the structure of $n$-central groups. We focus here on determining bounds for the exponent of $M(G)$. For instance, it follows from our previous work [7, 23] that if $G$ is a locally finite group of finite exponent, then the exponent of $M(G)$ can be bounded in terms of $\exp G$ only. Since our proof is based on the solution of the Restricted Burnside Problem, it does not provide any reasonable bound of $\exp M(G)$. On the other hand, there is a known result of Jones [14] saying that if $G$ is finite $p$-group and $c$ its nilpotency class ($c \geq 2$), then $\exp M(G)$ divides $(\exp G)^{c-1}$. This has been improved by Ellis [9] who showed that $\exp M(G)$ divides $(\exp G)^{\lceil c/2 \rceil}$. We show here that $\lceil c/2 \rceil$ can be replaced by $2 \lceil \log_2 c \rceil$, which is an improvement if $c \geq 11$. Beside that, we give an explicit bound for the exponent of $M(G)$ for a metabelian $p$-group $G$ in terms of

Date: 6th June 2006.

2000 Mathematics Subject Classification. 20D15.

Key words and phrases. Schur multiplier, $p$-group, power endomorphism.

The author was supported by the Ministry of Higher Education, Science and Technology of Slovenia. A part of this work was done during a visit to the University of Bath. The author wishes to thank the Department of Mathematical Sciences in Bath for its fine hospitality. He also wishes to thank the referee for valuable suggestions.
exp $G$ only. As a consequence we prove that if $G$ is a metabelian group of exponent $p$, then exp $M(G)$ divides $p$.

We also apply our techniques to calculate exp $M(G)$ in the case when $G$ is a group of exponent 4. Note that if $G$ is an infinite group of exponent 4, then $G$ may not be nilpotent. Thus the above mentioned results of Jones and Ellis do not guarantee that exp $M(G)$ is finite. This is however ensured by the above mentioned use of the solution of the Restricted Burnside Problem. Using information on the structure of 4-central groups obtained in [23, Theorem 1.1], we prove that exp $M(G)$ divides 8. We also show by an example that this result is best possible.

Another aspect of this paper is consideration of exponent semigroups of finite $p$-groups. Given a group $G$, define $E(G) = \{n \in \mathbb{Z} : (xy)^n = x^n y^n \text{ for all } x, y \in G\}$ to be the exponent semigroup of $G$. F. W. Levi [20] obtained an arithmetic characterisation of exponent semigroups of groups, and L.-C. Kappe [15] provided further information on these sets. Based on her results we prove that if $G$ is a finite $p$-group and exp$(G/Z(G)) = p^r$, then there exists $r \geq 0$ such that $E(G) = p^{r+rZ}\cup(p^{r+rZ}+1)$. Since $r$ is uniquely determined by $G$, we define $r$ to be the exponential rank of $G$. Clearly abelian $p$-groups have exponential rank zero, and the same is true for regular $p$-groups. From our results it also follows that the exponential rank of a given $p$-group does not exceed log$_p$ exp$(G/Z(G))$. Additionally we show that the exponential rank is an invariant of powerful $p$-groups. More precisely, we prove that if $G$ is a powerful $p$-group, then its exponential rank is either 0 or 1, depending on whether $p$ is odd or not. This result therefore provides the complete picture of exponent semigroups of powerful $p$-groups.

Finally we mention as a curiosity that the methods of this paper provide a rather short proof of the fact that every 6-central group is 36-abelian. This has already been proved in [23, Theorem 1.2] with the help of computer calculations. Our present proof requires only some elementary theory of Schur multipliers.

2. BOUNDS FOR THE EXPONENT OF THE SCHUR MULTIPLIER

Although this section is primarily devoted to estimating the exponent of the Schur multiplier of a given group, our first result can be proved in a more general setting. Let $G$ be a group and $n$ an integer. For $x, y \in G$ we define the $n$-commutator of $x$ and $y$ by $[x, y]_n = (xy)^n y^{-n} x^{-n}$.

Furthermore, let $[G, G]_n$ be the subgroup of $G$ generated by all $n$-commutators $[x, y]_n$, where $x, y \in G$. We say that a group $G$ is $n$-nilpotent of class $c$ if $c$ is the smallest integer for which

$$\underbrace{[\ldots, [G, G], G, G, \ldots, G]}_{c+1 \text{ copies of } G} = 1.$$

It is now clear that a group is $n$-nilpotent of class 1 if and only if it is $n$-abelian. Additionally, it is not difficult to see that our definition agrees with the definition of $n$-nilpotent groups given by Baer [3].

Our first aim is to show that $n$-nilpotent groups are closely related to the notion of the nilpotent multiplier of a group. Let $G$ be a group presented as the quotient of a free group $F$ by a normal subgroup $R$. Let $c$ be a positive integer. Define a series of groups $\gamma_c(R, F)$ as $\gamma_1(R, F) = R$ and $\gamma_{c+1}(R, F) = [\gamma_c(R, F), F]$ for $c \geq 1$.

The abelian group $M^{(c)}(G) = (R \cap \gamma_{c+1}(F))/\gamma_{c+1}(R, F)$ is said to be the $c$-nilpotent multiplier of $G$. The groups $M^{(c)}(G)$ are known to be invariants of $G$ (for a more general notion of a multiplier associated to a given variety of groups see a paper of Leedham-Green and McKay [18]). The group $M(G) = M^{(1)}(G)$ is more known as the Schur multiplier of $G$. When $G$ is finite, $M(G)$ is isomorphic to the second cohomology group $H^2(G, \mathbb{Z}^*)$. For an excellent account on the Schur multipliers see a book of Karpilovsky [16].
Proposition 2.1. Let
\[ 1 \to R \to F \to G \to 1 \]
be a free presentation of the group G. Suppose that \( \exp G = e \) and \( \exp M^{(c)}(G) = f \).
Then the group \( F/\gamma_{c+1}(R,F) \) is \((ef)\)-nilpotent of class \( \leq c \).

Proof. Let \( x_1, x_2, \ldots, x_{c+1} \in F \) and put \( y = [\ldots [[x_1, x_2]], x_{c+1}] \). Then we have (see, e.g., the proof of Proposition 7.2 of [23])
\[
[y, x_{c+1}] = [y, x_{c+1}] \cdot y^e, x_{c+1}^e \cdot [y, x_{c+1}] \cdot y^e \cdot (y, x_{c+1}) \cdot y^e.
\]
Since \( y \in \gamma_c(F) \cap R \), we have \( [y, x_{c+1}] \in \gamma_{c+1}(F) \cap R \). As \( \exp M^{(c)}(G) = f \), it follows that \( (y, x_{c+1}) \in \gamma_{c+1}(R,F) \). Consider now the \( f \)-commutator \( [y, x_{c+1}] \cdot y^e \). The assumption \( F^e \leq R \) implies \( [x_1, x_2] \in R \), whence \( y \in \gamma_{c-1}(R,F) \). This shows that \( [y, x_{c+1}] \in \gamma_c(R,F) \), hence \( [y, x_{c+1}] \cdot y^e \in \gamma_{c+1}(R,F) \).

It remains to consider \( [y, x_{c+1}] \cdot y^e, x_{c+1}^e \). Note that \( x_{c+1}^e \in R \) and \( [y, x_{c+1}] \cdot y^e \in \gamma_c(F) \), hence \( [y, x_{c+1}] \cdot y^e, x_{c+1}^e \in R, \gamma_c(F) \). We shall prove by induction on \( c \) that \( \gamma_c(F), R \leq \gamma_{c+1}(R,F) \) for every group \( F \) and \( R \leq F \). For \( c = 1 \) this is clear. Assume that this inclusion holds for some \( c \) and all \( F \) and \( R \). Consider the groups \( F, R, \gamma_c(F) \) and \( [R, \gamma_c(F), F] \). By the induction assumption, \( [R, \gamma_c(F), F] \leq \gamma_{c+1}(R,F) \) and \( [F, R, \gamma_c(F)] \leq \gamma_{c+1}(R,F) \). By the Three Subgroup Lemma we have \( \gamma_{c+1}(F), R \leq \gamma_{c+2}(R,F), \gamma_{c+2}(R,F) \), as required. Thus we have proved that \( [y, x_{c+1}] \in \gamma_{c+1}(R,F) \). This shows that \( F/\gamma_{c+1}(R,F) \) is \((ef)\)-nilpotent of class \( \leq c \).

We can also interpret Proposition 2.1 in the following way. Suppose that \( G \) is a \((c,n)\)-central group [23], that is, \( G/Z_n(G) \) has exponent dividing \( n \). Let \( G/Z_n(G) \) have a free presentation
\[ 1 \to R \to F \xrightarrow{\phi} G/Z_n(G) \to 1 \]
and suppose that \( M^{(c)}(G/Z_n(G)) \) has exponent \( f \). By Proposition 2.1, \( F/\gamma_{c+1}(R,F) \) is \((ef)\)-nilpotent of class \( \leq c \). We claim that \( G \) is also \((ef)\)-nilpotent of class \( \leq c \). Since \( F \) is free, there exists a homomorphism \( \psi : F \to G \) such that \( \psi \circ \iota = \phi \), where \( \iota \) is the canonical homomorphism \( G \to G/Z_n(G) \). Clearly \( \psi \) is surjective. We have that \( R^e \leq Z_n(G) \), hence \( R \leq \ker \psi \), and hence \( \psi \) induces a homomorphism \( \theta : F/\gamma_{c+1}(R,F) \to G \) such that \( \psi \circ \theta = \psi \). Here \( \kappa \) is the canonical homomorphism \( F \to F/\gamma_{c+1}(R,F) \). If it follows that \( G \) is a homomorphic image of \( F/\gamma_{c+1}(R,F) \), hence it is \((ef)\)-nilpotent of class \( \leq c \). Note that this can be compared with [23, Proposition 7.2].

As an application we reprove Theorem 1.2 of [23] which was proved there with the help of extensive computer calculations. Our proof here is computer-free, moreover, it does not require any profound commutator calculus.

Corollary 2.2 (cf. [23], Theorem 1.2). Every 6-central group is 36-abelian.

Proof. Clearly it suffices to prove this for 2-generator groups. Since every 2-generator 6-central group is a homomorphic image of \( F/[F^6, F] \), where \( F \) is the free group of rank two, it is enough to show that \( F/[F^5, F] \) is 36-abelian. Let \( G = F/[F^6, F] \). By Proposition 2.1 this will follow at once, when we have proved that \( \exp M(G) \) divides 6. First note that \( G \) is a finite \((2,3)\)-group by the solution of the Burnside Problem for exponent six (see, for instance, [25]). Let \( P \) be a Sylow 2-subgroup of \( G \) and \( Q \) a Sylow 3-subgroup of \( G \). For a prime \( p \), denote by \( M_G(p) \) the \( p \)-th component of \( M(G) \). Clearly, if \( p \notin \{2,3\} \), then \( M_G(p) \) is trivial. By [16, Theorem 2.1.2], \( M(G)_2 \) is isomorphic to a subgroup of \( M(P) \). As \( P \) is elementary abelian 2-group, we have that \( \exp M(P) = 2 \), thus \( M(G)_2 \) has exponent dividing 2. Similarly, \( M(G)_3 \) embeds into \( M(Q) \). As \( Q \) has exponent 3, it is 2-Engel [24, Theorem 7.14]. Thus the proof of Lemma 2.5 of [14] shows that \( \exp M(Q) \) divides 3. We conclude that \( \exp M(G) \) divides 6, hence the proof is finished. □
In the case \( c = 1 \) we can prove a partial converse of Proposition 2.1. More precisely, we have the following.

**Proposition 2.3.** Let \( G \cong F/R \) be a free presentation of the group \( G \). Let \( G \) have exponent \( c \) and suppose that the group \( F/[R, F] \) is \((ef)-ablian. Then the exponent of \( M(G) \) divides \( ef \).

**Proof.** As \( F/[R, F] \) is \((ef)-ablian, we have \((x_1 \cdots x_k)^{ef} \equiv x_1^{ef} \cdots x_k^{ef} \mod [R, F] \) for all \( x_1, \ldots, x_k \in F \), \( k \geq 1 \). Let \( z \in R \cap F' \). Then we can write \( z = \prod_i [x_i, y_i] \), where \( x_i, y_i \in F \). We obtain

\[
z^{ef} \equiv \prod_i [x_i, y_i]^{ef} \mod [R, F] \\
\equiv \prod_i (x_i^{-1} x_i^{y_i})^{ef} \mod [R, F] \\
\equiv \prod_i x_i^{ef} (x_i^{ef})^{y_i} \mod [R, F] \\
\equiv \prod_i [x_i^{ef}, y_i] \mod [R, F].
\]

Since \( x_i^{ef} \in R \), we get \( z^{ef} \in [R, F] \), thus \( M(G) \) has exponent dividing \( ef \). \( \square \)

A well-known result of Schur [16, Theorem 2.1.5] says that if \( G \) is a finite group and \( e \) is the exponent of \( M(G) \), then \( e^2 \) divides the order of \( G \). Suppose that \( n \) is the exponent of \( G \) and \( d \) the minimal number of generators of \( G \). Then the solution of the Restricted Burnside Problem [25] shows that \( e \) can be bounded by a function depending only on \( d \) and \( n \). Our first application of Proposition 2.3 shows that we can eliminate \( d \) from this bound.

**Proposition 2.4.** Let \( G \) be a locally finite group of exponent \( n \). Then the exponent of \( M(G) \) is bounded by a function \( f(n) \), depending on \( n \) only.

**Proof.** Let \( G \) be a locally finite group of exponent \( n \). Suppose that \( G \) is presented as a quotient of a free group \( F \) by a normal subgroup \( R \). Then the group \( H = F/[F, R] \) is a central extension of a locally finite group. Furthermore, since \( F^n \leq R \), we have that \( [F^n, F] \leq [R, F] \), hence it follows that \( H \) is \( n \)-central. By a remark from [23] (see also [7]) there exists an integer \( m > 1 \) such that \( H \) is \( m \)-abelian. The argument from [23] also shows that \( m \) depends only on \( n \) (here the solution of the Restricted Burnside Problem is used), furthermore, it can be chosen to be divisible by \( n \). By Proposition 2.3 the exponent of \( M(G) \) divides \( m \). This concludes the proof. \( \square \)

For instance, if \( G \) is any group of exponent 4, then it is locally finite [25]. Thus Proposition 2.4 implies that the exponent of \( M(G) \) is bounded by a fixed constant. Using [23], it is rather straightforward to obtain an estimate for \( \exp M(G) \). Namely, if \( G \cong F/R \) is a group of exponent 4, then \( F/[F, R] \) is 4-central. By [23, Theorem 1.1], \( F/[F, R] \) is 16-abelian, hence Proposition 2.3 shows that \( \exp M(G) \) divides 16. Yet this bound is not best possible. We are going to prove the following.

**Theorem 2.5.** Let \( G \) be a group of exponent 4. Then \( \exp M(G) \) divides 8.

Before embarking on the proof, recall that a group \( H \) is said to be a covering group of a group \( G \) if there exists \( M \leq H \) isomorphic to \( M(G) \) such that \( M \leq H' \cap Z(H) \) and \( H/M \cong G \). Schur (1904) proved that covering groups of finite groups always exist, although they need not be unique (see, e.g., [16, Theorem 2.1.4]). Covering groups play a crucial role in studying the Schur multipliers of finite groups. Theorem 2.5 will follow from the following more general result.

**Theorem 2.6.** Let \( G \) be a finite group of exponent 4 and let \( H \) be its covering group. Then \( H' \) has exponent dividing 8.
Lemma 2.7. Let $G$ be a group, $x, y \in G$. Suppose $p$ is a prime and $k$ a positive integer. Then

(a) $(xy)^p \equiv x^p y^p \prod_{i=1}^{p^k-1} [y, x]^{(p^k)} \mod C_{p,k}(x, y)$.

(b) $(xy)^p \equiv x^p y^p \mod \gamma_2((x, y))^p \prod_{i=1}^{k} \gamma_{p^i}((x, y))^{p^k-i}$.

(c) $[x^p y] \equiv \prod_{i=0}^{p-1} [x, y, x]^{(p^k)} \mod C_{p,k}(x, [x, y])$.

(d) $[x^p y] \equiv \prod_{i=0}^{p-1} [x, y]^{(p^k)} \mod \gamma_2((x, [x, y]))^p \prod_{i=1}^{k} \gamma_{p^i}((x, [x, y]))^{p^k-i}$.

Here $C_{p,k}(a, b)$, where $a, b \in \langle x, y \rangle$, is defined to be the normal closure in $\langle x, y \rangle$ of the set of all basic commutators in $\{a, b\}$ of weight $\geq p^k$ and of weight $\geq 2$ in $b$, together with the set of $p^{k-j+1}$-th powers of all basic commutators in $\{a, b\}$ of weight $< p^j$ and of weight $\geq 2$ in $b$, $j = 1, \ldots, k$.

We will also use the following result on groups of exponent 4. It can be proved by referring to power-commutator presentation of the group $B(3,4)$, the free Burnside group of exponent 4 and rank 3. For details see [25].

Lemma 2.8. Let $G$ be a group of exponent 4 and $a, b, c \in G$. Then we have:

(a) $[a, b]^2 = [a, b, b, b][a, b, a, b][a, b, a, a][a, b, b, b]$.

(b) $[a, b, c]^2 = [a, b, a, b]^2 = [a, b, a, a]^2 = 1$.

(c) $[a, b, c, c, c] = [c, a, b, c, c]$.

Proof of Theorem 2.6. Since $G$ has exponent 4, $H$ is a 4-central group. From the proof of [23, Theorem 1.1] it follows that $H$ satisfies the law $[a, b]^8 = 1$. For $z \in H'$ and $x, y \in H$ we therefore obtain

$$
(1) \quad (z[x, y])^8 \equiv z^8[x, y, z]^{(z)}[x, y, z, z]^{(z)} \mod C_{2,3}(z, [x, y])
$$

by Lemma 2.7. Now let $a, b, c$ be arbitrary elements of $H$. From the proof of [23, Theorem 1.1] we get $\gamma_2((a, b))^2 = \gamma_2((a, b)) = 1$ and $\gamma_2((a, b, c)) = 1$. This, together with Lemma 2.8 (a), implies

$$
(2) \quad [[a, b]^2, c] = [a, b, b, c][a, b, a, c][a, b, b, c] = [a, b, a, a][a, b, b, c].
$$

As $[a, b]^2 = [c, [a, b]^2][a, b, [a, b]]$, we get

$$
[[a, b]^2, c] = [a, b, [c, [a, b]]][a, b, c],
$$

hence

$$
(3) \quad [a, b, c] = [c, [a, b][a, b][a, b, b, c][a, b, a, c][a, b, a, c][a, b, b, c].
$$

Lifting the identities of Lemma 2.8 (b) to the group $H$ and using the class restriction, we get

$$
[a, b, b, c]^2 = [a, b, a, c]^2 = [a, b, b, c]^2 = 1,
$$

whence also

$$
||[a, b]^2, c||^2 = 1.
$$

Now let $x_i \in \{a, b, c\}$, $i = 1, \ldots, 5$. Since $(a, b, c)$ is nilpotent of class $\leq 8$, the equation (3) implies

$$
[x_1, x_2, x_3, x_4, x_5]^2 = [x_1, x_2, x_3, x_4, x_5][x_1, x_2, x_3, x_4, x_5][x_1, x_2, x_3, x_4, x_5].
$$

Lifting the identities of Lemma 2.8 (c) to $H$, we observe that $\gamma_3((a, b, c))^2 = 1$. This, together with (3), shows that $[a, b, c]^4 = 1$. By definition we also get $C_{2,3}(z, [x, y]) = 1$, hence we can rewrite (1) as $(z[x, y])^8 = z^8$. From here we conclude that $\exp H'$ divides 8.

Proof of Theorem 2.5. If $G$ is finite, then the conclusion follows from Theorem 2.6. Otherwise, let $\{G_i : i \in I\}$ be the family of all finitely generated subgroups of $G$. We need a technical lemma which can be proved using the Hall-Petrescu formula [12, pp. 65–66].
Since each $G_i$ has exponent 4, it is finite [25]. By the direct limit argument [5] we get
\[ M(G) = M(\text{lim} G_i) \cong \text{lim} M(G_i), \]
hence $\exp M(G)$ divides 8 by Theorem 2.6. \qed

Note that Theorem 2.5 provides best possible bound for the exponent of the Schur multiplier of a group of exponent 4. Macdonald and Wamsley (see [4]) constructed a group $G$ of order $2^{21}$ which has exponent 4 and multiplier of exponent 8. It is not very difficult to find a similar example of order 2048. This is the smallest example of a group $G$ of exponent 4 with $\exp M(G) = 8$ we have been able to find, perhaps one can find some even smaller examples using computational tools such as GAP [10]. A brief search through the GAP library of groups of small size reveals that the order of such a group has to be at least 256.

Example 2.9. Let $D = A \times \langle c_1 \rangle$, where $A = \langle c_2 \rangle \times \langle c_3 \rangle \times \langle c_4 \rangle \times \langle c_5 \rangle \cong C_4 \times C_4 \times C_4$ and $c_1$ is an automorphism of order 2 of $A$ acting in the following way.
\[ [c_2, c_1] = c_2, \quad [c_3, c_1] = c_3^2, \quad [c_4, c_1] = c_4^3, \quad [c_5, c_1] = 1. \]
There exists an automorphism $a$ of $D$ of order 4 acting on $D$ as follows.
\[ [c_1, a] = c_3, \quad [c_2, a] = c_2^2c_3^2c_4, \quad [c_3, a] = c_5, \quad [c_4, a] = c_2^2, \quad [c_5, a] = c_3^2. \]
Form $H = D \times \langle a \rangle$ and put $G = H \times \langle b \rangle$, where $b^2 = 1$ and
\[ [c_1, b] = c_2, \quad [c_2, b] = c_2^2c_3^3c_5, \quad [c_3, b] = c_4, \quad [c_4, b] = c_3c_4^2, \quad [c_5, b] = c_2c_3^2c_4, \quad [a, b] = c_1. \]
The group $G$ is nilpotent of class 6, its order is 2048. Using techniques from [16, Section 2.2], we get $M(G) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_8$.

Since the proof of Proposition 2.4 is based on the solution of the Restricted Burnside Problem, it becomes evident that it provides only a very crude bound of $f(n)$. In some cases, better bounds of $\exp M(G)$ can be achieved by allowing some other invariants of $G$ to appear in the estimate. In connection with this we mention a result of Ellis [9]. For a real number $\alpha$, let $[\alpha]$ be the smallest integer not less than $\alpha$. The result goes as follows.

Proposition 2.10. [9, Theorem B1] Let $G$ be a finite $p$-group of nilpotency class $c \geq 2$. Then $\exp M(G)$ divides $(\exp G)^{[c/2]}$.

Our aim is to improve this result for large nilpotency classes. First we deal with metabelian groups.

Theorem 2.11. Let $p$ be a prime and let $G$ be a metabelian group of exponent $p^e$. Denote $q = (p - 1)p^{e-1}$. Then the exponent of $M(G)$ divides $p^k$, where
\[ k = \lceil \max\{\log_p(1 + eq), e + \log_p(q/\log p) + 1/q - 1/\log p\} \rceil, \]
if $p$ is odd, and $k = \lceil \log_2(1 + e \cdot 2^{e-1}) \rceil + 1$ if $p = 2$.

Proof. We prove our theorem only for $p$ odd; if $p = 2$, then the proof follows the lines of the odd case, thus we leave out the details. As in the proof of Theorem 2.5 we may assume that $G$ is finitely generated and therefore finite (in the infinite case we can use the direct limit argument, since the exponents of finitely generated subgroups are uniformly bounded by a constant). Let $H$ be a covering group of $G$. Then $H$ is centre-by-metabelian and $p^e$-central. Let $x, y \in H$ and let $\overline{x}, \overline{y}$ be their images in $H/Z(H)$. Put $N = \langle x, y \rangle$ and $\overline{N} = \langle \overline{x}, \overline{y} \rangle$. By a result of Dark and Newell [6] we have $(\gamma_{(e-i)q+1}(N))^{\overline{N}} = 1$ for $0 \leq i < e$, where $q = (p - 1)p^{e-1}$. Taking preimages in $H$, we conclude that $(\gamma_{(e-i)q+1}(N))^{\overline{N}} \leq Z(H)$. For $w \in \gamma_{(e-i)q+1}(N)$ and $h \in H$
we get $1 = [w^p, h] = [w, h]^{w^{i-1} + \ldots + w^i}$. Since we have $[w, h]^{w^i} = [w, h][w, h, w]^{i}$ and $[w, h, w^j] \in Z(H)$, this can be rewritten as

$$
1 = [w, h]^{p^i} \cdot \prod_{j=1}^{p^i} [w, h, w^{p^i-j}]
$$

$$
= [w, h]^{p^i} [w, h, \prod_{j=1}^{p^i} w^{p^i-j}]
$$

$$
= [w, h]^{p^i} [w, h, (w^{p^i})],
$$

hence $[w, h]^{p^i} [w, h, w] \in H$ for all $h \in H$ and $w \in \gamma(e-i+1)(N)$. Replacing $h$ by some commutator $[h_1, h_2] \in H'$, we get $[w, [h_1, h_2]]^{p^i} = 1$. Using linear expansion of commutators in $H$, we conclude that $\gamma(e-i+1)(N), H')^{p^i} = 1$. In particular, we get $[w, h, w] = 1$. As $p$ is odd, this gives $[w, h]^{p^i} = 1$ for all $w \in \gamma(e-i+1)(N)$ and $h \in H$. We claim that $(\gamma(e-i+1)(N))^{p^i} = 1$. Let $c$ be a commutator of length $(e-i+1)(N) = 2$ in $N$ and $d \in \gamma(e-i+1)(N)$. Then Lemma 2.7 (a), together with the fact that $H$ is centre-by-metabelian, implies

$$(dc)^{p^i} = d^{p^i} e^{p^i} [c, d] = d^{p^i},$$

whence $(\gamma(e-i+1)(N))^{p^i} = 1$ for $0 \leq i < e$. For a positive integer $k$ we get

$$[x^{p^k}, y] \equiv [x, y]^{p^k} \mod \gamma_2(M)^{p^k} \prod_{i=1}^{k} \gamma_i(M)^{p^{k-i}},$$

where $M = (x, [x, y])$, by Lemma 2.7. Note that $\gamma_j(M) \leq \gamma_{j+1}(N)$ for $j \geq 2$, hence we can rewrite the above equation as

$$(4) \quad [x^{p^k}, y] \equiv [x, y]^{p^k} \mod \gamma_3(N)^{p^k} \prod_{i=1}^{k} \gamma_{p^i+1}(N)^{p^{k-i}}.$$}

Let $k = \max\{\log_p(1+q), e + \log_p(q/\log p) + 1/q - 1/\log p\}$. First expand $1 = [[x, y]^{p^k}, z]$ in a similar way as above. We obtain

$$1 = [x, y, z]^{p^k} \cdot \prod_{i=1}^{p^k} [x, y, z, [x, y]^{p^{k-i}}]
$$

$$= [x, y, z]^{p^k} [x, y, z, \prod_{i=1}^{p^k} [x, y]^{p^{k-i}}]
$$

$$= [x, y, z]^{p^k} [x, y, z, [x, y]^{(p^k)}],$$

hence

$$(5) \quad [x, y, z]^{p^k} [x, y, z, [x, y]^{(p^k)}] = 1.$$
because of the nilpotency class restriction. Hence the equation (4) implies \( [x, y]^{p^k} = 1 \) for all \( x, y \in H \). Since \( H \) is centre-by-metabelian, \( H' \) is nilpotent of class \( \leq 2 \).

Let \( c \in H' \) and \( x, y \in H \). Then \( (c[x, y])^{p^k x^k y^k} = c^{p^k} |x, y|^{p^k} [x, y, c]^{\binom{p}{2}} = c^{p^k} \), since \( p \) is odd. This shows that \( (H')^{p^k} = 1 \), which concludes the proof.

Close inspection of the bound for the exponent of the Schur multiplier in Theorem 2.11 shows that \( k \leq 2e \); if \( p \) is large enough, then we actually get \( k = 2e \), so the bound is probably not best possible. For instance, our theorem implies that if \( G \) is a metabelian group of exponent \( p (p \text{ odd}) \), then \( \exp(M(G)) \) divides \( p^2 \). However, this can be improved.

**Proposition 2.12.** Let \( G \) be a metabelian group of exponent \( p \). Then \( M(G) \) is an elementary abelian \( p \)-group.

**Proof.** We can evidently assume that \( p \) is odd and that \( G \) is finite. Our claim follows then directly from equation (4) and from the fact that every two-generator metabelian group of exponent \( p \) is nilpotent of class \( \leq p - 1 \), see e.g. [6].

With the help of Theorem 2.11 we can improve the bound given by Proposition 2.10. Here we use the notation \( \lfloor \alpha \rfloor \) for the greatest integer less than or equal to \( \alpha \in \mathbb{R} \).

**Theorem 2.13.** Let \( G \) be a finite \( p \)-group and let \( c \) be its nilpotency class. Suppose \( c \geq 2 \) and let \( H \) be a covering group of \( G \). If \( \exp(G) = p^e \), then the exponent of \( H' \) (and hence also \( \exp(M(G)) \)) divides \( p^{\lfloor \log_2 c \rfloor} \), where \( k \) is as in Theorem 2.11.

**Proof.** Let \( d \) be the derived length of \( G \) and \( \exp(G) = p^e \). Suppose \( k \) is as in Theorem 2.11. Let \( H \) be any covering group of \( G \). Then \( H \) is \( p^e \)-central and centre-by-(solvable with derived length \( \leq d \)). We claim that for every such group \( H \), \( \exp(H') \) divides \( p^{\lfloor d-1 \rfloor} \), and prove this by induction on \( d \). For \( d = 2 \) this follows from the proof of Theorem 2.11. Assume that \( d > 2 \). Then \( H^{d-2} \) is \( p^e \)-central and centre-by-metabelian, thus it follows from the proof of Theorem 2.11 that \( \exp(H^{(d-1)}) \) divides \( p^{d-1} \). The factor group \( H/H^{(d-1)} \) is \( p^e \)-central and solvable of derived length \( \leq d-1 \), whence the induction assumption implies that the group \( (H/H^{(d-1)})' = H'/H^{(d-1)} \) has exponent dividing \( p^{d-2} \). From here we get that the exponent of \( H' \) divides \( p^{d-1} \), as required. To conclude the proof, note that \( d \leq \lfloor \log_2 c \rfloor + 1 \), which gives the result.

Note that \( p^{\lfloor \log_2 c \rfloor} \leq p^{2e} \lfloor \log_2 c \rfloor \) and that \( 2 \lfloor \log_2 c \rfloor \leq \lfloor c/2 \rfloor \) for \( c \geq 11 \), so this result definitely improves a related result of Ellis ([9], see also Proposition 2.10) for \( p \)-groups having nilpotency class at least 11. It also improves the bound given by Jones [14] for \( c \geq 5 \). At the other end of the scale, if \( c \leq 2 \), then \( \exp(M(G)) \) divides \( \exp(G) \) by [14]. From the same paper it follows that a similar conclusion holds for \( p \)-groups of class 3 when \( p \neq 3 \). Results of this kind have also been proved by Kayvanfar and Sanati [17] for \( c = 4, 5 \).

3. **Exponent Semigroups of Finite \( p \)-Groups**

Given a group \( G \), define
\[
\mathcal{E}(G) = \{ n \in \mathbb{Z} : (xy)^n = x^ny^n \text{ for all } x, y \in G \}.
\]
It is clear that \( \mathcal{E}(G) \) is always a multiplicative subsemigroup of \( \mathbb{Z} \) containing 0 and 1. Following [15], we say that \( \mathcal{E}(G) \) is the exponent semigroup of \( G \). One of the main results of [15] is a number-theoretic characterisation of \( \mathcal{E}(G) \) for an arbitrary group \( G \). More precisely, let \( q_1, q_2, \ldots, q_t \) be integers, \( q_i > 1 \) and \( \gcd(q_i, q_j) = 1 \) for \( i \neq j \). Let \( B(q_1, q_2, \ldots, q_t) \) be the set of integers which is the union of \( 2^t \) residue
classes modulo $q_i$ satisfying each a system of congruences $m \equiv \delta_i \mod q_i$, where $i = 1, \ldots, t$ and $\delta_i \in \{0, 1\}$. Then we can summarize relevant results of [15] as follows.

**Proposition 3.1** (cf. Theorem 1 and Corollary 1 in [15]). Let $W$ be a nonempty set of integers. Then $W = \mathcal{E}(G)$ for some group $G$ if and only if either $W = \{0, 1\}$, $\mathbb{Z}$ or $B(q_1, \ldots, q_t)$ with $q_i > 2$ for all $i$. Furthermore, there exists a non-negative integer $\epsilon = \epsilon(G)$ such that $\epsilon \in \mathcal{E}(G)$ and $n^2 \equiv n \mod \epsilon$ for all $n \in \mathcal{E}(G)$. If $\mathcal{E}(G) = \{0, 1\}$, then $\epsilon = 0$. Otherwise $\epsilon$ is positive and $\epsilon = \min\{n \in \mathcal{E}(G) : n > 0, \exp(G/Z(G)) \mid n\}$.

Let $G$ be a finite $p$-group and suppose $G$ is $n$-abelian for some $n \neq 0, 1$. Proposition 3.1 implies that $G$ is $(1-n)$-abelian, hence it is also $n(1-n)$-abelian. Thus $[x^{n(1-n)}, y] = [x, y]^{n(1-n)} = [x^n, y^{1-n}] = x^{-n}y^{-1}y^n x^n y^{-n}y = x^{-n}y^{-1}(yxy^{-1})^n y = x^{-n}y^{-1}(x^n)^{-1} y = 1$ for all $x, y \in G$, hence $G$ is $n(n-1)$-central. Write $n(n-1) = p^k q$ where $q$ is not divisible by $p$. Since $G$ is a $p$-group, it follows that $G$ is also $p^k$-central. Let $\mathcal{E}_0(G) = \{n \in \mathcal{E}(G) : n > 0, \exp(G/Z(G)) \mid n\}$. By Proposition 3.1, $\mathcal{E}_0(G)$ is an ideal in $\mathcal{E}(G)$. Since $n(1-n) \in \mathcal{E}_0(G)$, we conclude that $p^k \in \mathcal{E}_0(G)$, hence $\mathcal{E}_0(G)$ is generated by some $p^t$, where $t$ is a nonnegative integer not exceeding $k$. By Proposition 3.1 we now obtain the following result.

**Proposition 3.2.** Let $G$ be a finite $p$-group and let $\exp(G/Z(G)) = p^r$. Then there exists a nonnegative integer $r$ such that $\mathcal{E}(G) = B(p^{r+t}) = p^{r+t} \mathbb{Z} \cup (p^{r+t} \mathbb{Z} + 1)$.

Note that $r$ in Proposition 3.2 is uniquely determined. This leads to the following definition:

**Definition.** Let $G$ be a finite $p$-group and let $r$ be as in Proposition 3.2. Then we say that $r$ is the exponential rank of $G$. We use the notation $r = \exp r(G)$.

If $G$ is a finite $p$-group, then Proposition 2.1 implies that $0 \leq \exp r(G) \leq \log_p \exp M(G/Z(G))$. In general, these bounds are best possible, as the following example shows.

**Example 3.3.** Let $p$ be a prime. A finite $p$-group $G$ is said to be generalised extraspecial if $Z(G)$ is cyclic and $G'$ has order $p$. In this case, $G/Z(G)$ is elementary abelian $p$-group and $\exp M(G/Z(G)) = p$. $G$ is clearly nilpotent of class two, hence $(xy)^p = x^p y^p [y, x]^{p(p-1)/2}$ for all $x, y \in G$. Thus $\exp r(G) = 0$ in case $p$ is odd, and $\exp r(G) = 1$ for $p = 2$.

The definition of the exponential rank indicates that the $p$-groups which are in a certain sense close to being abelian, have a small exponential rank. Let us illustrate this by an example. For a finite $p$-group $G$ and a positive integer $k$ define $\mathcal{U}_k(G) = G^{p^k}$. A $p$-group $G$ is said to be regular [13] if for all $x, y \in G$ we have that $(xy)^p \equiv x^p y^p \mod \mathcal{U}_k(\gamma_2(x, y))$. If $G$ is a regular $p$-group and $\exp G/Z(G) = p^r$, then Satz 10.8 in [13] implies that $\exp \gamma_2(G) = p^r$. From here we conclude that $G$ is $p^r$-abelian, hence $\exp r(G) = 0$. In fact, almost the same phenomenon occurs with powerful $p$-groups. Here a finite $p$-group $G$ is said to be powerful [21] if $p$ is odd and $G' \leq \mathcal{U}_1(G)$, or $p = 2$ and $G' \leq \mathcal{U}_2(G)$. More generally, a normal subgroup $N$ of a finite $p$-group $G$ is said to be powerfully embedded in $G$ if $p$ is odd and $[N, G] \leq \mathcal{U}_1(N)$, or $p = 2$ and $[N, G] \leq \mathcal{U}_2(N)$. Note that every quotient of a powerful $p$-group is again powerful. On the other hand, subgroups of powerful $p$-groups need not be powerful. For other basic properties of powerful $p$-groups we refer to [8] or [21].

In connection with exponent semigroups we mention here two known results. The first one is a theorem due to Lubotzky and Mann [21] stating that if $G$ is a powerful $p$-group then $\exp M(G)$ divides $\exp G$. A direct consequence of this result is that if $G$ is a powerful $p$-group, then $\exp r(G) \leq \log_p \exp(G/Z(G))$. The other one
Proposition 3.4 (cf. [8], p. 45). Let $G$ be a powerful $p$-group and let $\exp G = p^\ell$. Then $G$ is $p^{\ell-1}$-abelian.

Theorem 3.5. Let $G$ be a powerful $p$-group.

(a) If $p$ is odd, then $\exp \rank(G) = 0$.

(b) If $p = 2$ and $G$ is not abelian, then $\exp \rank(G) = 1$.

Proof. Let $c$ be the nilpotency class of $G$. We may assume that $c > 1$. First we want to prove that

$$\exp \gamma_k(G) = \exp(G/Z_{k-1}(G))$$

for each $k \in \{1, \ldots, c+1\}$. To this end, we need the following auxiliary result.

Claim. Let $N$ be powerfully embedded in $G$. Then $\mathcal{U}_1([N,G]) = [\mathcal{U}_1(N),G]$.

Proof of Claim. For the simplicity assume that $p$ is odd; the proof for $p = 2$ is similar. We prove our claim by induction on $i$. First we deal with the case $i = 1$. By [21, Corollary 1.2], $[N,G]$ is powerfully embedded in $G$. Thus $[N,G,G] \subseteq [N,G,G] \leq \mathcal{U}_1([N,G])$. Similarly, $[N,G,G] \leq [\mathcal{U}_1(N),G]$.

Factoring with $[N,G,G]$, we may assume that $N \leq Z_2(G)$. But in this case we clearly obtain $\mathcal{U}_1([N,G]) = [\mathcal{U}_1(N),G]$, as the elements of $[N,G,G]$ commute with those from $N$. Suppose now that $\mathcal{U}_1([N,G]) = [\mathcal{U}_1(N),G]$ holds true for some $i \geq 1$ and for every $N$ powerfully embedded in $G$. Since the groups $N$, $[N,G]$ and $[\mathcal{U}_1(N),G]$ are powerfully embedded in $G$ (see [21]), we get $\mathcal{U}_{i+1}([N,G]) = \mathcal{U}_1(\mathcal{U}_1([N,G])) = \mathcal{U}_1([\mathcal{U}_1(N),G]) = [\mathcal{U}_1(\mathcal{U}_1(N)),G] = [\mathcal{U}_{i+1}(N),G]$.

To prove (6), observe that $\gamma_j(G)$ is powerfully embedded in $G$ for each $j \in \mathbb{N}$; see [21]. Using the above Claim and induction on $j$, we get $\mathcal{U}_1(\gamma_j(G)) = \gamma_j(\mathcal{U}_1(G))$ for all $i,j \in \mathbb{N}$. From here (6) readily follows.

Denote $\exp(G/Z_k(G)) = p^{e_k}$. By [21, Proposition 2.5] we have that $c - k \leq e_k$, hence $e_k > 1$ for $k = 0, \ldots, c - 2$. Since $G$ is $p^{e_0-1}$-abelian by Proposition 3.4, we infer from Proposition 3.2 that $e_1 < e_0$. Since $G/Z(G)$ is also powerful, a similar conclusion yields $e_2 < e_1$. Continuing with this process, we obtain a chain

$$e_0 > e_1 > e_2 > \cdots > e_{c-1} > e_c = 0.$$

This shows that if $0 \leq i \leq j < c$, then $e_i \geq e_j + j - i$. Now assume that $p$ is odd. Let $x, y \in G$. Then Lemma 2.7 gives

$$(xy)^{p^e_i} \equiv x^{p^{e_i} y^{p^{e_i}}} \mod \mathcal{U}_{e_1}(\gamma_{2i}(\langle x,y \rangle)) \prod_{i=1}^{c_1} \mathcal{U}_{e_1-i}(\gamma_{p^i}(\langle x,y \rangle)).$$

We have $\mathcal{U}_{e_1}(\gamma_{2i}(\langle x,y \rangle)) = 1$. Besides, if $p^i \geq c + 1$, then $\gamma_{p^i}(\langle x,y \rangle) = 1$. For $p^i < c + 1$ we have $e_{p^i-1} > 0$. Furthermore, $e_1 \geq e_{p^i-1} + p^i - 2 \geq e_{p^i-1} + i$, since $p^i \geq i + 2$. From here it follows that $\mathcal{U}_{e_1-i}(\gamma_{p^i}(\langle x,y \rangle)) \leq \mathcal{U}_{e_1-i}(\gamma_{p^i}(\langle x,y \rangle)) = 1$, hence $G$ is $p^{e_i}$-abelian.

For the rest of the proof assume $p = 2$. Then a similar approach as above yields that $G$ is $2^{c+1}$-abelian, hence $\exp \rank(G) \leq 1$. Suppose there exists a nonabelian powerful 2-group $G$ with $\exp \rank(G) = 0$. If $G$ is nilpotent of class two, then $(xy)^{2^i} = x^{2^{i+1}} y^{2^i} \cdot [x,y]^{2^i-1}$ for any $x, y \in G$. Since $G$ is $2^{e_1}$-abelian, this implies that $\exp G'$ divides $2^{c+1}$, which is a contradiction. Thus $c > 2$. As $2^i \geq i + 2$ for $i \geq 2$, we obtain $\mathcal{U}_{e_1-i}(\gamma_{2i}(\langle x,y \rangle)) = 1$ for $2 \leq i \leq e_1$, hence

$$(xy)^{2^i} \equiv x^{2^{i+1}} y^{2^i} \mod \mathcal{U}_{e_1-i}(\gamma_{2i}(\langle x,y \rangle)).$$
The corresponding terms in $\mathcal{U}_{e_1-1}(\gamma_2((x,y)))$ can be computed using the commutator collection process described in [12, pp. 65–66]. We obtain

$$(xy)^{2e_1} = x^{2e_1}y^{2e_1}[y,x](x_{1}^{2e_1})[y,x,x](x_{3}^{2e_1})[y,x,y](x_{5}^{2e_1}) + 2(x_{7}^{2e_1}),$$

hence $G$ satisfies the law

$$[y,x](x_{1}^{2e_1})[y,x,x](x_{3}^{2e_1})[y,x,y](x_{5}^{2e_1}) + 2(x_{7}^{2e_1}) = 1.$$  

Since $\exp G' = 2e_1$, this gives

$$(7) \quad [y,x](x_{1}^{2e_1})[y,x,x](x_{3}^{2e_1})[y,x,y](x_{5}^{2e_1}) = 1.$$  

Note that $e_1 - 1 \geq e_2$, whence $[y,x][y,x]^{2e_1-1} \in Z_2(G)$. Thus $[y,x][y,x]^{2e_1-1}$ commutes with $[y,x][y,x]^{2e_1-1}$, hence we can rewrite (7) as $([y,x][y,x]^{2e_1-1})[y,x,y][y,x,y]^{2e_1-1} = 1$. Since $G$ is a 2-group, we obtain $[y,x][y,x]^{2e_1-1} = 1$. This gives

$$[y,x,y][y,x,y]^{2e_1-1} = [y,x,y][y,x,y]^{2e_1-1}.$$  

Replacing $y$ by $[x,y]$ in this equation, we get $[[x,y],x,[x,y]]^{2} = [x,y][x,y]^{2} = [x,y][x,y]^{2} = [[x,x,x],[y,x,y],[y,x,y]]^{2}$. Further replacement of $x$ by $[x,y]$ yields $[x,y]^{2} = [[x,x],[y,x,y],[y,x,y]]^{2}$. Since $G$ is nilpotent, repeated use of this process shows that $G$ satisfies the law $[x,y]^{2} = 1$. By a result of Macdonald [22], $G$ is centre-by-nilpotent and $\exp G'$ divides 4. Since $G'$ is powerful, we get $\exp G' \leq (G')^{4} = 1$, hence $G'$ is abelian. We conclude that $\exp G' = 2$, but this immediately implies that the nilpotency class of $G$ does not exceed 2. This gives the final contradiction.  

REFERENCES


Primož Moravec, Oddelok za matematiko, Inštitut za matematiko, fiziKO in mehaniko, Jadranska 19, 1000 Ljubljana, Slovenia
E-mail address: primoz.moravec@fmf.uni-lj.si