

ON COMMUTATORS IN p -GROUPS

LUISE-CHARLOTTE KAPPE AND ROBERT FITZGERALD MORSE

ABSTRACT. For a given prime p , what is the smallest integer n such that there exists a group of order p^n in which the set of commutators does not form a subgroup? In this paper we show that $n = 6$ for any odd prime and $n = 7$ for $p = 2$.

1. INTRODUCTION

In 1898, G.A. Miller [12] introduced the commutator subgroup G' of a group G as the subgroup generated by $K(G) = \{[a, b] : a, b \in G\}$, the set of commutators of G . According to Miller, commutators $[a, b] = a^{-1}b^{-1}ab$ were introduced by Dedekind a few years earlier. In general, it is not true that a subgroup is equal to its set of generators, and in this respect, the commutator subgroup should be no different. Because of their relatively uncomplicated structure, the finite groups of small order with which we are familiar contain no examples where G' contains non-commutators. In the literature, the earliest example of such a group appears in a 1902 paper by Fite [5], where a group of order 256 is given with this property. Another example, also a group of order 256 and more commonly cited in the literature, appears in Carmichael's textbook [3].

The following question then arises: What is the smallest group order for which there exists a group G with the property that the commutators do not form a subgroup? In [11], MacHale states 47 conjectures known to be false and asks for minimal counterexamples. Among these is the conjecture that the set of commutators always forms a subgroup. To the best of our knowledge, no answer to this question appears in the literature. A group of order 96 can be found in [4] but no claim that it is a minimal counterexample is made. It can be easily verified using GAP [6] that this group is indeed of minimal order by enumerating all groups in successive order and checking whether or not the set of commutators forms a subgroup. In fact, there are two groups of order 96 in which $K(G) \neq G'$. However, using GAP provides no insight as to why the set of commutators does not form a subgroup. In a forthcoming publication [9], we will show that $G' = K(G)$ for all groups G of order less than 96 using traditional group theoretic methods.

The topic of this paper arose out of [9] and concerns minimal counterexamples in p -groups for which $K(G) \neq G'$. Specifically, we give a complete

2000 *Mathematics Subject Classification.* 20D15, 20F12.

answer to the following question: For a given prime p , what is the smallest integer n such that there exists a group of order p^n in which the set of commutators does not form a subgroup? The examples in [5] and [3] yield $n \leq 8$ for $p = 2$. In [10], Macdonald constructs groups of order p^8 , where p is any prime, in which $K(G)$ is not a subgroup. Thus we must have $n \leq 8$ for all primes p . In this paper we will show that $n = 6$ for odd primes and $n = 7$ for $p = 2$.

After stating some sufficient conditions for $K(G) = G'$ in the next section, we will show in Sections 3 and 4 that the commutators form a subgroup in groups of order p^n , $n \leq 5$, p an odd prime, and of order 2^n , $n \leq 6$, respectively. The final section of the paper is devoted to the construction of minimal counterexamples. We construct three classes of p -groups, all having the property that $G' \neq K(G)$: one each for $p \geq 5$, $p = 3$ and $p = 2$. We then show that each of the classes contains groups of order p^6 , 3^6 and 2^7 , respectively.

The counterexamples of order 2^7 and 3^6 were originally found through the GAP library of small groups [1]. To obtain counterexamples of order p^6 , $p \geq 5$, we first constructed a metabelian 5-group of exponent 5, order 5^6 and class 4. Using GAP, we enumerated the set of commutators for this group and verified it was strictly contained in the derived subgroup. Using this group as a guide, we generalized its construction to obtain a metabelian p -group of exponent p , order p^6 and class 4 for $p \geq 5$ such that $K(G) \neq G'$.

Our notation is standard. We list here various formulas and definitions used throughout this paper without further reference. Let $x, y, z \in G$ and $w \in G'$. The familiar commutator expansion formulas are

$$[xy, z] = [x, z]^y[y, z] \text{ and } [x, yz] = [x, z][x, y]^z.$$

For a metabelian group we have $[w, x, y] = [w, y, x]$ and the Jacobi identity reduces to $1 = [x, y, z][z, x, y][y, z, x]$. Following [8], we say a finite abelian p -group G has type $(p^{n_1}, p^{n_2}, \dots, p^{n_k})$ if G is the direct product of cyclic groups of order p^{n_i} , $i = 1, \dots, k$, with $n_1 \geq n_2 \geq \dots \geq n_k$.

2. SOME SUFFICIENT CONDITIONS

In this section we state various sufficient conditions implying that the commutators form a subgroup. There are very few such results. The most useful so far seems to be the following.

Theorem 2.1. [16] *Suppose a group G contains a normal abelian subgroup with cyclic factor group. Then $G' = K(G)$.*

In [14] and [15] several other sufficient conditions can be found. We quote those relevant in our context.

Theorem 2.2. [15] *The following two conditions on a group G imply $G' = K(G)$:*

- (i) *G is nilpotent of class two and the minimal number of generators of G' does not exceed three;*

(ii) G' is elementary abelian of order p^3 .

Theorem 2.3. [14] *If G is nilpotent and G' is cyclic, then $G' = K(G)$.*

In [15] it is established that $G' = K(G)$ for $G' \cong C_p \times C_p$ under the hypothesis that G' is the Sylow p -subgroup of the group. This is never satisfied in a p -group. We will show as part of the next theorem that in a p -group, $G' \cong C_p \times C_p$ always implies $K(G) = G'$.

Theorem 2.4. *Let G be a finite p -group with G' elementary abelian of rank less than or equal to 3. Then $K(G) = G'$.*

Proof. If G' has rank 1 or 3, the result follows from Theorem 2.3 and (ii) of Theorem 2.2. Now suppose $G' \cong C_p \times C_p$. If $\text{cl}(G) = 2$, then the result follows by (i) of Theorem 2.2. Thus we can assume that $\text{cl}(G) = 3$. We claim that we can assume $G = \langle a, b \rangle$. Suppose otherwise. Then $[x, y, y] = 1$ for all $x, y \in G$ and thus G is a 2-Engel group, $p = 3$ and the minimal number of generators of G is less than or equal to 3. But in this case $|G'| > 3^2$, a contradiction.

We have now $G' = \langle [a, b], [a, b, a], [a, b, b] \rangle$. We must have $\gamma_3(G) \cong C_p$, since otherwise $\gamma_3(G) = \gamma_2(G)$, a contradiction. If $[a, b, a] = 1$ or $[a, b, b] = 1$, our claim follows by Theorem 2.1. Otherwise, we have $[a, b, a] = [a, b, b]^j$ with $j \not\equiv 0 \pmod p$. Obviously, $G = \langle ab^{-j}, b \rangle$ and $[ab^{-j}, b, ab^{-j}] = 1$. Applying Theorem 2.1 again leads to the desired result. \square

We note that the restriction on the rank is best possible since there are groups with G' an elementary abelian p -group of rank 4 with $K(G) \neq G'$ (see [10] or the example in the last section).

3. GROUPS OF ORDER p^n , $n \leq 5$

In this section we will show that in any group of order p^n , $n \leq 5$, where p is an odd prime, the set of commutators forms a subgroup. These groups are metabelian by [13]. We start with expansion formulas for metabelian groups to be used throughout the rest of the paper.

Lemma 3.1. [7] *Let G be a metabelian group and n a positive integer. Then for all $v, w \in G$*

$$(3.1.1) \quad [v, w^n] = \prod_{i=1}^n [v, \underbrace{w, \dots, w}_i]^{(n)},$$

$$(3.1.2) \quad (vw^{-1})^n = v^n \left(\prod_{0 < i+j < n} [v, \underbrace{w, \dots, w}_i, \underbrace{v, \dots, v}_j]^{(i+j+1)} \right) w^{-n}.$$

The following two propositions consider one abelian type for G' not covered in the previous section, namely (p^2, p) . As we will show, this type only occurs if $p = 3$.

Proposition 3.2. *Let p be a prime with $p \geq 5$. There exists no group of order p^5 having a commutator subgroup of type (p^2, p) .*

Proof. Assume there exists a group G with $|G| = p^5$ and $G' \cong C_{p^2} \times C_p$. Then $G/G' \cong C_p \times C_p$ and $G = \langle a, b \rangle$. Since $p \geq 5$, it follows that G is regular and thus $G_{[p]} = \{g \in G \mid g^p = 1\}$ as well as $G^{(p)} = \{g^p \mid g \in G\}$ are (normal) subgroups of G . If $|G_{[p]}| \geq p^3$, then $G/G_{[p]}$ is abelian, and hence $G' \subseteq G_{[p]}$, a contradiction. It follows $C_p \times C_p \cong G_{[p]} \leq G'$. By III.10.7 in [8] we have $|G/G_{[p]}| = |G^{(p)}|$, and therefore $|G^{(p)}| = p^3$. Since obviously $G^{(p)} \leq G'$, it follows $G' = G^{(p)}$. Suppose next $h \in G$ and h has order p^2 . By the above it follows that there exists $x \in G$ with $h = x^p$. Then for any $y \in G$ we obtain $h^y = (x[x, y])^p$, and regularity yields $h^y = x^p[x, y]^p z^p$ for some $z \in G$. Thus $[x, y]^p z^p \in (G')^p = \langle h^p \rangle$ and we conclude $h^y \in \langle h \rangle$. It follows $\langle h \rangle \triangleleft G$ and $G' = \langle [a, b] \rangle$, a contradiction, since G' is not cyclic. So $[a, b]$ has order p and $[a, b] \in G_{[p]}$. Thus $G' = [a, b]^G \leq G_{[p]}$, another contradiction, since $G/G_{[p]}$ is not abelian. \square

Proposition 3.3. *If G is a group of order 3^5 with G' having type $(9, 3)$, then $K(G) = G'$.*

Proof. For order reasons we can assume $G = \langle a, b \rangle$, $a^3, b^3 \in G'$ and $\text{cl}(G) \leq 4$. This together with (3.1.1) yields $\exp \gamma_3(G) = 3$, since $[[x, y], a^3] = [[x, y], b^3] = 1$ for $x, y \in G$. If $\langle [a, b] \rangle \triangleleft G$, it follows G' is cyclic. Hence we can assume that $G' = \langle [a, b] \rangle \times \langle [a, b, a] \rangle$ with $|[a, b]| = 3^2$ and $|[a, b, a]| = 3$. Since $a^3 \in G'$, we have

$$(3.3.1) \quad a^3 = [a, b]^\alpha [a, b, a]^\beta$$

for integers α and β .

Assume that $\text{cl}(G) \leq 3$. Then commuting (3.3.1) by a yields $[a, b, a]^\alpha = 1$, hence $\alpha \equiv 0 \pmod{3}$. Commuting (3.3.1) by b leads to $[a^3, b] = 1$. Expansion of $[b, a^3]$ by (3.1.1) together with $\exp \gamma_3(G) = 3$ leads to $1 = [b, a]^3$, a contradiction. Hence G has class 4. If $[a, b, a, a] = 1$, it can be shown that $\text{cl}(G) = 3$. Thus we can assume $[a, b, a, a] \neq 1$. Commuting (3.3.1) twice by a yields $\alpha \equiv 0 \pmod{3}$. Subsequently, commuting (3.3.1) once by a leads to $\beta \equiv 0 \pmod{3}$. Thus, after commuting (3.3.1) by b , we obtain $[a^3, b] = 1$. Expansion of $[b, a^3]$ together with $\exp \gamma_3(G) = 3$ yields $[a, b, a, a] = [a, b]^{-3}$. It can be verified that each element of G' can be represented by a commutator of the form $[a, x]$ or $[x, a]$, where $x = b^\epsilon [a, b]^\gamma [a, b, a]^\delta$, $\epsilon = 0, 1$ and $\gamma, \delta = 0, 1, 2$, with suitable choices for ϵ, γ , and δ . \square

We are ready now to prove the main result of this section.

Theorem 3.4. *Let p be an odd prime and G a group of order p^n , $n \leq 5$. Then $G' = K(G)$.*

Proof. By [13], all groups as given in the assumption are metabelian. The order bound on G yields $|G'| = p^m$, $m = 1, 2, 3$, where $m = 3$ can only occur if $|G| = p^5$. The possible types for G' are (p) , (p^2) , (p^3) , (p, p) , (p, p, p) or

(p^2, p) . If G' is cyclic, our result follows from Theorem 2.3, and if G' has type (p, p) or (p, p, p) , the claim follows from Theorem 2.4. In the remaining case that G' has type (p^2, p) , then $|G'| = p^5$. Proposition 3.2 implies $p = 3$, and by Proposition 3.3 we obtain that $K(G) = G'$ as needed. \square

4. GROUPS OF ORDER 2^n , $n \leq 6$

The goal of this section is to show that in any group of order 2^n , $n \leq 6$, the set of commutators forms a subgroup. By [13], such groups are metabelian. Thus it suffices to deal with all the potential types of the commutator subgroup. Due to a result of Blackburn [2], many types do not occur. However, we still have to deal with the case where G' has type $(4, 2)$. It is quite involved which is no surprise in view of the fact that 64 of the 267 groups of order 64 have this type for their commutator subgroup.

Proposition 4.1. *Let G be a group of order 64 with G' having type $(4, 2)$. Then $K(G) = G'$.*

Proof. Our assumptions imply that G/G' has type $(4, 2)$ or $(2, 2, 2)$. Assume first that G/G' has type $(4, 2)$. Then $G = \langle a, b \rangle$ and $a^4, b^2 \in G'$ and $\text{cl}(G) \leq 4$. Let $G' \cong A = \langle x \rangle \times \langle y \rangle$ with $|x| = 4$ and $|y| = 2$. We observe that $\text{Aut}(A) = \langle \sigma, \rho \rangle \cong D_4$, the dihedral group of order 8, with $x^\sigma = xy$, $y^\sigma = y$ and $x^\rho = xy$, $y^\rho = yx^2$. Without loss of generality we can assume $x = [a, b]$.

Assume first that the action of a on G' has order 4. Then a acts like ρ or ρ^3 on G' . If a acts like ρ , then $[a, b]^a = [a, b]y$ and hence $y = [a, b, a]$. It follows $[a, b, a]^a = [a, b, a][a, b]^2$, and consequently $[a, b, a, a] = [a, b]^2$. The remaining elements of G' not yet identified as commutators can be written as elements of $K(G)$ as follows: $[a, b][a, b, a] = [a, b^a]$, $[a, b]^3[a, b, a] = [b^a, a]$ and $[a, b]^2[a, b, a] = [a, b^a, a]$. If a acts like ρ^3 on G' , then $[a, b^a]^a = [a, b^a]y$. Introducing new generators $a' = a$ and $b' = b^a$, then a' acts like ρ on G' , reducing this case to the previous one.

Now let $a^2 \in C_G([a, b])$. Observing $1 = [[x, y, z], a^2] = [[x, y, z], b^2]$ and $\text{cl}(G) \leq 4$ leads to $\exp \gamma_4(G) \leq 2$. Assume $|[a, b, b]| = 4$, then $[a, b]^2 = [a, b, b]^2$. Commuting by b yields $[a, b, b]^2 = 1$, a contradiction. If $|[a, b, a]| = 4$, we arrive at a similar contradiction. We conclude $\exp \gamma_3(G) = 2$. This together with $1 = [[a, b], a^2] = [[a, b], b^2] = [a^2, b^2]$ and expansion by (3.1.1) leads to $1 = [b, a, a, a] = [a, b, b, b][a, b, b, a]$. Hence $\text{cl}(G) = 3$.

Assume first $b^2 \notin Z(G)$. Since $b^2 \in G'$, we have $b^2 = [a, b]^{\pm 1}h$ with $h \in \gamma_3(G)$. Commuting by b leads to $1 = [a, b, b]$ and thus $\langle b, G' \rangle$ is an abelian normal subgroup of G with cyclic factor group. It follows from Theorem 2.1 that $K(G) = G'$.

Now assume $b^2 \in Z(G)$. If in addition $a^2 \in Z(G)$, then $[a, b, a]$, $[a, b, b] \in \langle [a, b] \rangle$ and G' is cyclic, a contradiction.

Thus we can assume $a^2 \notin Z(G)$. We have $[a, b, b] = [a, b]^2$ and b acts like ρ^2 on G' . Furthermore, a acts like σ or $\sigma\rho^2$ on G' . If a acts like σ , then $[a, b, a] = y$, $[a, b^a] = [a, b][a, b, a]$ and $[a, ab, ab] = [a, b]^2[a, b, a]$. It follows $K(G) = G'$. If a acts like $\sigma\rho^2$ on G' , then $[ba, b]^{ba} = [ba, b]y$. Introducing

new generators $a' = ba$ and $b' = b$, then a' acts like σ on G' , reducing this case to the previous one.

Finally, let G/G' have type $(2, 2, 2)$. For order reasons it follows $G = \langle a, b, c \rangle$ and $a^2, b^2, c^2 \in G'$. We have $\text{cl}(G) > 2$, since G' central implies $\exp(G') = 2$, a contradiction. Without loss of generality we can assume $|[a, b]| = 4$. Consider $H = \langle a, b \rangle$. We must have $H' = \langle [a, b] \rangle$, since otherwise H would have order 32 with a noncyclic commutator subgroup of order 8, contradicting Theorem 2.1 in [2].

Let $A = \langle [a, b], [a, c], [b, c] \rangle$, then $G' = A^G$, the normal closure of A in G . Since $\text{rank } G' = 2$, it follows $\text{rank } A \leq 2$. If $\text{rank } A = 1$, then $[a, c], [b, c] \in H'$ and $G' = [a, b]^G$. We claim $[a, b]^G = H'$, which is a contradiction, since G' is not cyclic. It remains to be shown that $[a, b]^c \in H'$. Since $[a, c]^b, [b, c]^a \in H'$ by the above, it follows $[a, b, c] \in H'$ by the Jacobi identity. We conclude $[a, b]^c \in H'$. Thus we can assume $\text{rank } A = 2$ and without loss of generality $A = \langle [a, b], [a, c] \rangle$ and $A^G = A = G'$. If $|[a, c]| = 2$, then $G' = \langle [a, b] \rangle \times \langle [a, c] \rangle$. Suppose $|[a, c]| = 4$. Choosing new generators $a' = a, b' = b$ and $c' = bc$, it can be shown $|[a', b']| = 2$ and $G' = \langle [a', b'], [a', c'] \rangle$. Relabeling the generators as a, b, c , we can assume without loss of generality that $G' = \langle [a, b] \rangle \times \langle [a, c] \rangle$.

We are now ready to show $G' = K(G)$. Observing that $[a, b]^3[a, c]$ is the inverse of $[a, b][a, c]$, it suffices to show that $u = [a, b]^2, v = [a, b][a, c]$ and $w = [a, b]^2[a, c]$ can be expressed as commutators. Since $\langle a, b \rangle' = \langle [a, b] \rangle$, it follows that a and b can only act like $\epsilon, \rho^2, \sigma\rho, \sigma\rho^3$ on G' . Depending on the action of a , we have $u = [a, b, a]$ or $[b, a^2]$. If b acts like ϵ or ρ^2 , then $v = [a, cb]$, and if b acts like $\sigma\rho$, or $\sigma\rho^3$, then $v = [cb, a]$.

It remains to be shown that $w \in K(G)$. If a acts like ρ^2 or $\sigma\rho^3$, then $w = [a, c[a, b]]$, and if a acts like $\sigma\rho$, then $w = [a, c^a]$. Furthermore, if b acts like ϵ or $\sigma\rho$, then $w = [a, cb^2]$ and if b acts like $\sigma\rho^3$, then $w = [a^b, c^b]$. Thus we can assume $b = \rho^2$, and hence $[a, c, b] = 1$. Since we can assume $a = \epsilon$, it follows $[b, c, a] = 1$. The Jacobi identity now yields $[a, b, c] = 1$. This implies that c acts like ϵ or $\sigma\rho$ on G' . In case $c = \sigma\rho$, we have $w = [a^c, c]$. For the remaining case in which a and c act trivially and $b = \rho^2$, we have to consider the value of $[b, c]$. It can be easily verified that for $[b, c] = [a, b]^\alpha[a, c]^\beta$ with $\alpha = 0, 1, 2, 3$ and $\beta = 0, 1$ we have $w = [bx, ca^{\alpha+2}]$, where for $\beta = 1, x = 1$, and for $\beta = 0, x = a$ if α is even and $x = c$ if α is odd. \square

Now we are ready to prove the main result of this section.

Theorem 4.2. *Let G be a group of order 2^n , $n \leq 6$. Then $K(G) = G'$.*

Proof. By [13], all groups of order 2^n , $n \leq 6$, are metabelian. The order bound on G yields $|G'| = 2^m$, $m = 1, 2, 3, 4$. If G' is cyclic, the claim follows from Theorem 2.3. By Theorem 2.1 in [2] it follows that a 2-group has a cyclic commutator subgroup, whenever $G/G' \cong C_2 \times C_2$. This implies that G' can be non-cyclic only if $n = 5$ or 6 . It follows that for $|G| = 32$, the commutator subgroup can only have type $(2, 2)$. If $|G| = 64$, the possible

types for G' are $(2, 2)$, $(2, 2, 2)$ and $(4, 2)$. If G' is elementary abelian of rank 2 or 3, the claim follows from Theorem 2.4. In the case $|G| = 64$ and $G' \cong C_4 \times C_2$, Proposition 4.1 gives the desired result. \square

5. MINIMAL COUNTEREXAMPLES

In this section we construct three classes of p groups each having the property that $G' \neq K(G)$. Within these classes of groups, we obtain specific groups of order p^6 , $p \geq 5$, 3^6 , and 2^7 which are minimal counterexamples for when $G' \neq K(G)$. We start with a lemma about commutator expansions.

Lemma 5.1. *Let $G = \langle a, b \rangle$ be a group of nilpotency class 4 with $[b, a, b] \in Z(G)$, and let $x, y \in G$ with*

$$x = a^\alpha b^\beta [b, a]^\gamma [b, a, a]^\delta c \quad \text{and} \quad y = a^{\alpha'} b^{\beta'} [b, a]^{\gamma'} [b, a, a]^{\delta'} c',$$

where $c, c' \in G' \cap Z(G)$ and $\alpha, \alpha', \beta, \beta', \gamma, \gamma', \delta$, and δ' are integers. Then

$$[x, y] = [b, a]^\lambda [b, a, a]^\mu [b, a, b]^\nu [b, a, a, a]^\rho$$

with

$$\begin{aligned} \lambda &= \alpha'\beta - \alpha\beta', & \mu &= \alpha'\gamma - \alpha\gamma' + \beta \binom{\alpha'}{2} - \beta' \binom{\alpha}{2}, \\ \nu &= \beta'\gamma - \beta\gamma' + \beta\beta'(\alpha' - \alpha) + \alpha' \binom{\beta}{2} - \alpha \binom{\beta'}{2}, & \text{and} \\ \rho &= \alpha'\delta - \alpha\delta' + \gamma \binom{\alpha'}{2} - \gamma' \binom{\alpha}{2} + \beta \binom{\alpha'}{3} - \beta' \binom{\alpha}{3}. \end{aligned}$$

Proof. We observe that G is a metabelian 2-generator group of class 4. Using standard commutator expansion and applying (3.1.1) repeatedly, we arrive at the desired expression for $[x, y]$ after collecting terms. \square

Our next lemma is the key to showing that certain elements in the commutator subgroup are not commutators for the groups in question.

Lemma 5.2. *Let p be an odd prime and $\alpha, \alpha', \beta, \beta', \gamma, \gamma'$ integers. If the 6-tuple $(\alpha, \alpha', \beta, \beta', \gamma, \gamma')$ is a solution to the system of congruences*

$$(5.2.1) \quad \begin{cases} \alpha'\beta - \alpha\beta' \equiv 0 \pmod{p} \\ \alpha'\gamma - \alpha\gamma' + \beta \binom{\alpha'}{2} - \beta' \binom{\alpha}{2} \equiv 0 \pmod{p} \\ \beta'\gamma - \beta\gamma' + \beta\beta'(\alpha' - \alpha) + \alpha' \binom{\beta}{2} - \alpha \binom{\beta'}{2} \equiv 1 \pmod{p}, \end{cases}$$

then $\alpha \equiv \alpha' \equiv 0 \pmod{p}$.

Proof. Let $u = \beta' \binom{\alpha}{2} - \beta \binom{\alpha'}{2}$ and $v = \beta'\beta\alpha - \beta\beta'\alpha' + \alpha \binom{\beta'}{2} - \alpha' \binom{\beta}{2} + 1$. Then the system (5.2.1) can be written as

$$(5.2.2) \quad \begin{cases} \alpha'\beta \equiv \alpha\beta' \pmod{p} \\ \alpha'\gamma - \alpha\gamma' \equiv u \pmod{p} \\ \beta'\gamma - \beta\gamma' \equiv v \pmod{p}. \end{cases}$$

Multiplying the second congruence in (5.2.2) by β and the third by α , and then taking the difference leads to

$$\beta u - \alpha v \equiv \beta \alpha' \gamma - \beta \alpha \gamma' - \alpha \beta' \gamma + \alpha \beta \gamma' \equiv (\alpha' \beta - \alpha \beta') \gamma \equiv 0 \pmod{p}.$$

On the other hand, using the explicit definition of u and v , and $\alpha' \beta \equiv \alpha \beta' \pmod{p}$ to simplify terms, we arrive at $2(u\beta - v\alpha) \equiv -2\alpha \pmod{p}$. Since p is odd, this yields $-2\alpha \equiv 0 \pmod{p}$. We conclude $\alpha \equiv 0 \pmod{p}$.

Now assume $\alpha' \not\equiv 0 \pmod{p}$. Then $\alpha' \beta \equiv \alpha \beta' \pmod{p}$ implies $\beta \equiv 0 \pmod{p}$ and thus $u \equiv 0 \pmod{p}$ and $v \equiv 1 \pmod{p}$. The system (5.2.2) reduces to $\alpha' \gamma \equiv 0 \pmod{p}$ and $\beta' \gamma \equiv 1 \pmod{p}$, a contradiction, since $\alpha' \not\equiv 0 \pmod{p}$ yields $\gamma \equiv 0 \pmod{p}$ and $\beta' \gamma \equiv 0 \pmod{p}$. \square

Although it is not needed in the sequel, it can be shown that the converse of Lemma 5.2 is also true. We now construct a class of p -groups, $p \geq 5$, in which the set of commutators does not form a subgroup.

Proposition 5.3. *Let $p \geq 5$ be a prime and $H = \langle a, b \rangle$ be a nilpotent group of class exactly 4 with $[b, a, b] \in Z(H)$ and $\exp(H') = p$. Then $K(H) \neq H'$.*

Proof. Since H is a 2-generator group of class 4, H is metabelian. We claim now that $[b, a, b][b, a, a, a]$ is not a commutator. By Lemma 5.1 this is equivalent to showing that the following set of congruences has no solutions in integers $\alpha, \alpha', \beta, \beta', \gamma, \gamma', \delta, \delta'$:

$$(5.3.1) \quad \begin{cases} \alpha' \beta - \alpha \beta' \equiv 0 \pmod{p}, \\ \alpha' \gamma - \alpha \gamma' + \beta \binom{\alpha'}{2} - \beta' \binom{\alpha}{2} \equiv 0 \pmod{p}, \\ \beta' \gamma - \beta \gamma' + \beta \beta' (\alpha' - \alpha) + \alpha' \binom{\beta}{2} - \alpha \binom{\beta'}{2} \equiv 1 \pmod{p}, \\ \gamma \binom{\alpha'}{2} - \gamma' \binom{\alpha}{2} + \beta \binom{\alpha'}{3} - \beta' \binom{\alpha}{3} + \delta \alpha' - \alpha \delta' \equiv 1 \pmod{p}. \end{cases}$$

By Lemma 5.2, if the subsystem consisting of the first three congruences of (5.3.1) is solvable, then $\alpha \equiv \alpha' \equiv 0 \pmod{p}$. However, the left side of the last congruence of (5.3.1) is congruent to zero modulo p for $\alpha \equiv \alpha' \equiv 0 \pmod{p}$. It follows that the system (5.3.1) is not solvable. \square

As a corollary, we obtain that the smallest order of a group described in the preceding proposition is p^6 .

Corollary 5.4. *Let $p \geq 5$ be a prime. Then there exists a group G of order p^6 such that $K(G) \neq G'$.*

Proof. Let $V = \langle u \rangle \times \langle v \rangle \times \langle w \rangle \times \langle z \rangle$ be an elementary abelian p -group of rank 4. Let $B = V \rtimes \langle b \rangle$, the semidirect product of V with a cyclic group $\langle b \rangle$ of order p . The defining relations of B are those of V and

$$b^p = 1, \quad [u, b] = w, \quad \text{and} \quad [v, b] = [w, b] = [z, b] = 1.$$

Similarly, let $G = B \rtimes \langle a \rangle$ be the semidirect product of B with a cyclic group $\langle a \rangle$ of order p . The defining relations of G are those of B and

$$[b, a] = u, \quad [u, a] = v, \quad [v, a] = z, \quad a^p = [w, a] = [z, a] = 1.$$

It can be verified that G has order p^6 , class 4, and $\exp(G) = p$ for $p \geq 5$. Furthermore, $u = [b, a]$, $v = [b, a, a]$, $w = [b, a, b]$ and $z = [b, a, a, a]$. Thus G satisfies the conditions of Proposition 5.3. We conclude $K(G) \neq G'$. \square

For 3-groups we have to modify our construction slightly to find a class of groups where $G' \neq K(G)$.

Proposition 5.5. *Let $H = \langle a, b \rangle$ be a nilpotent group of class exactly 4 with $a^3, b^9, [b, a, b] \in Z(H)$. Then $K(H) \neq H'$.*

Proof. Since H is a 2-generator group of class 4, H is metabelian. By hypothesis $[b, a, b] \in Z(H)$. It follows $[b, a, b, b] = [b, a, b, a] = 1$, and hence $\gamma_4(H) = \langle [b, a, a, a] \rangle$. Observing $a^3 \in Z(H)$, (3.1.1) leads to

$$(5.5.1) \quad 1 = [b, a]^3 [b, a, a]^3 [b, a, a, a].$$

We obtain $[b, a, a, a]^3 = [b, a, a]^3 = [b, a, b]^3 = 1$ by commuting (5.5.1) twice by a and once each by a and b , respectively. Hence

$$(5.5.2) \quad 1 = [b, a]^3 [b, a, a, a].$$

Now $b^9 \in Z(H)$ together with (3.1.1) and $\exp \gamma_3(H) = 3$ yields $[a, b]^9 = 1$. If $[a, b]^3 = 1$, it follows by (5.5.2) that $[b, a, a, a] = 1$, a contradiction, since $\text{cl}(H) = 4$. We conclude that $[a, b]$ has order 9.

We claim now that $[b, a, b][b, a, a, a]$ is not a commutator in H . By Lemma 5.1 and (5.5.2) this is equivalent to showing that the following system of congruences is not solvable:

$$(5.5.3) \quad \begin{cases} \alpha' \beta - \alpha \beta' - 3\Gamma \equiv 3 \pmod{9}, \\ \alpha' \gamma - \alpha \gamma' + \beta \binom{\alpha'}{2} - \beta' \binom{\alpha}{2} \equiv 0 \pmod{3}, \\ \beta' \gamma - \beta \gamma' + \beta \beta' (\alpha' - \alpha) + \alpha' \binom{\beta}{2} - \alpha \binom{\beta'}{2} \equiv 1 \pmod{3}, \end{cases}$$

with $\Gamma = \gamma \binom{\alpha'}{2} - \gamma' \binom{\alpha}{2} + \beta \binom{\alpha'}{3} - \beta' \binom{\alpha}{3} + \delta \alpha' - \alpha \delta'$. Assume to the contrary that (5.5.3) is solvable. It follows that the above system is solvable modulo 3, i.e. (5.5.3) is solvable where the first congruence of (5.5.3) is replaced by

$$(5.5.4) \quad \alpha' \beta - \alpha \beta' \equiv 0 \pmod{3}.$$

The resulting system is exactly the system (5.2.1) for $p = 3$. By Lemma 5.2 this system is solvable if and only if $\alpha \equiv \alpha' \equiv 0 \pmod{3}$. We have to show that none of these solutions modulo 9 satisfies the first congruence of (5.5.3). The one solution $\alpha \equiv \alpha' \equiv 0 \pmod{3}$ results in nine solutions modulo 9, namely $\alpha \equiv 0, 3, 6 \pmod{9}$ and $\alpha' \equiv 0, 3, 6 \pmod{9}$, respectively. It can be verified that for any of the nine cases the left side of the first congruence of (5.5.3) is congruent to zero modulo 9. We conclude that (5.5.3) is not solvable. \square

Corollary 5.6. *There exists a group G of order 3^6 such that $K(G) \neq G'$.*

Proof. Consider the abelian group $W = \langle u \rangle \times \langle v \rangle \times \langle w \rangle$, where u has order 9, and v and w each have order 3, thus $|W| = 3^4$. The group G will be constructed by two split extensions starting with W . Let $A = W \rtimes \langle a \rangle$

be the semidirect product of W with the cyclic groups $\langle a \rangle \cong C_3$, where a induces an automorphism of order 3 on W . The action of a on the generators of W is given as follows:

$$(5.6.1) \quad [u, a] = v, \quad [v, a] = u^6, \quad \text{and} \quad [w, a] = 1.$$

The defining relations of A are those of W , (5.6.1), and $a^3 = 1$. We observe $|A| = 3^5$.

Let $G = A \rtimes \langle c \rangle$ be the semidirect product of A with the cyclic group $\langle c \rangle \cong C_3$, where c induces an automorphism of order 3 on A . The action of c on the generators of A is given as follows:

$$(5.6.2) \quad [a, c] = uw^{-1}, \quad [u, c] = vw^{-1}, \quad [v, c] = u^6, \quad \text{and} \quad [w, c] = 1.$$

The defining relations of G are those of A , (5.6.2), and $c^3 = 1$. We observe $|G| = 3^6$.

The verification of the claims leading to the construction of G is for the most part straightforward but lengthy. Here we will only verify that $(a^c)^3 = 1$. By (5.6.2) we have $a^c = auw^{-1}$. Using (3.1.2) we obtain

$$(a^c)^3 = (a(u^{-1}w)^{-1})^3 = [a, u^{-1}w]^{(3)} [a, u^{-1}w, u^{-1}w] [a, u^{-1}w, a] u^3.$$

Now $[a, u^{-1}w] = v$ and $[a, u^{-1}w, a] = u^6$. This together with the above yields $(a^c)^3 = v^3 u^6 u^3 = 1$, proving our claim.

Next we show $W = G'$. We observe $G' \leq W$, since $G/W = \langle aW, cW \rangle \cong C_3 \times C_3$, hence abelian. On the other hand, $v = [u, a] \in G'$, $vw^2 = [u, c] \in G'$, and $uw^{-1} = [a, c] \in G'$. As a consequence we obtain $u, v, w \in G'$. Since $W = \langle u, v, w \rangle$, it follows $W \leq G'$, proving our claim.

To apply Proposition 5.5, we have to choose new generators for G , namely $G = \langle a, b \rangle$ with $b = c^{-1}a$. Straightforward expansion together with the relations of G lead to $[b, a, b] = [c^{-1}a, a, c^{-1}a] = w$. Furthermore, $uw^{-1} = [a, c] = [a, ab^{-1}] = [b, a][b, a, b]^{-1}$. By the above this yields $[b, a] = u$. This implies $[b, a, a] = [u, a] = v$ and $[b, a, a, a] = [v, a] = u^6$. Therefore $[b, a, a, a][b, a]^3 = 1$, and (5.5.2) is satisfied. Since $[w, a] = [w, b] = 1$, we have $[b, a, b] \in Z(G)$. This together with the above implies $\gamma_4(G) = \langle [b, a, a, a] \rangle$ and G has class 4 precisely. Obviously $a^3 \in Z(G)$, since $a^3 = 1$. Finally, with the help of (3.1.2) we obtain $1 = c^{-3} = (ba^{-1})^3 = b^3 u^3 v w$. Thus $1 \neq b^3 = u^6 v^2 w^2$, and consequently, $b^9 = 1$ and hence $b^9 \in Z(G)$. We conclude that G satisfies the assumptions of Proposition 5.5, thus $G' \neq K(G)$. \square

We observe here that the group G of Corollary 5.6 cannot be obtained as a split extension of A by $\langle b \rangle$, since $A \cap \langle b \rangle$ is nontrivial. A similar phenomenon occurs when constructing the minimal counterexample for $p = 2$. But first, since our groups have three generators, we need an expansion formula for this case.

Lemma 5.7. *Let $H = \langle a, b, c \rangle$ be a nilpotent group of class 3 with $\gamma_3(H) = \langle [a, b, b] \rangle$ and $H' = \langle [a, b], [a, c], [b, c], [a, b, b] \rangle$. Then for $x, y \in H$ we have*

$$[x, y] = [a, b]^\lambda [a, c]^\mu [b, c]^\nu [a, b, b]^\rho$$

with $\lambda = \beta'\alpha - \beta\alpha'$, $\mu = \alpha\gamma' - \alpha'\gamma$, $\nu = \beta\gamma' - \beta'\gamma$, and $\rho = \delta\beta' - \delta'\beta + \alpha\beta\beta' - \alpha'\beta\beta' + \alpha\binom{\beta'}{2} - \alpha'\binom{\beta}{2}$, where $x = a^\alpha b^\beta c^\gamma [a, b]^\delta z$ and $y = a^{\alpha'} b^{\beta'} c^{\gamma'} [a, b]^{\delta'} z'$ with $\alpha, \alpha', \beta, \beta', \gamma, \gamma', \delta, \delta'$ integers and $z, z' \in Z(H)$.

Proof. Since H has class 3, it follows that H is metabelian. Using standard commutator expansion and applying (3.1.1) repeatedly, we arrive at the desired expression for $[x, y]$ after collecting terms. \square

Proposition 5.8. *Let $H = \langle a, b, c \rangle$ be a group of class 3 precisely. If $a^4, b^2, c^2, [a, c], [b, c]$ and $(ab)^2 \in Z(H)$, then $K(H) \neq H'$.*

Proof. Since $b^2 \in Z(H)$, (3.1.1) implies

$$(5.8.1) \quad 1 = [a, b]^2 [a, b, b].$$

We obtain $[a, b, a]^2 = [a, b, b]^2 = 1$ by commuting (5.8.1) with a and b respectively. Furthermore, $c^2 \in Z(H)$ together with $[a, c]$ and $[b, c] \in Z(H)$ implies $[a, c]^2 = [b, c]^2 = 1$.

Next we claim that $\gamma_3(H) = \langle [a, b, b] \rangle$. The class restriction on H implies $\gamma_3(H) = \langle [x, y, z] \mid x, y, z \in \{a, b, c\} \rangle$. Since $[a, c], [b, c] \in Z(H)$, it follows $[a, c, x] = [b, c, x] = 1$ for $x \in \{a, b, c\}$. This together with the Jacobi identity leads to $[a, b, c] = 1$. Since $(ab)^2 \in Z(H)$, we have $1 = [(ab)^2, a]$. Expansion yields $1 = [b, a]^2 [b, a, a] [b, a, b]$. Observing (5.8.1) yields $[a, b, a] = 1$. Thus $[x, y, z] = 1$ for all $x, y, z \in \{a, b, c\}$ with the possible exception of $[a, b, b]$. Now $a^4 \in Z(H)$ implies $[b, a^4] = 1$. Expansion using (3.1.1) and the above lead to $[b, a]^4 = 1$. If $[a, b]^2 = 1$, then $[a, b, b] = 1$ by (5.8.1), contradicting that the class of H is precisely 3. Thus $\gamma_3(H) = \langle [a, b, b] \rangle$.

We claim now that $[a, c][a, b, b] \notin K(H)$. By Lemma 5.7 and (5.8.1), this is equivalent to showing that the following system of congruences has no solution:

$$(5.8.2) \quad \begin{cases} \alpha\beta' - \alpha'\beta + 2\Gamma \equiv 2 \pmod{4}, \\ \alpha\gamma' - \alpha'\gamma \equiv 1 \pmod{2}, \\ \beta\gamma' - \beta'\gamma \equiv 0 \pmod{2}, \end{cases}$$

where $\Gamma = \beta'\delta - \beta\delta' + \alpha\beta\beta' - \alpha'\beta\beta' + \alpha\binom{\beta'}{2} - \alpha'\binom{\beta}{2}$. Assume otherwise and suppose (5.8.2) is solvable. It follows that the above system is solvable modulo 2, resulting in the following system

$$(5.8.3) \quad \begin{cases} \alpha\beta' - \alpha'\beta \equiv 0 \pmod{2}, \\ \alpha\gamma' - \alpha'\gamma \equiv 1 \pmod{2}, \\ \beta\gamma' - \beta'\gamma \equiv 0 \pmod{2}. \end{cases}$$

It can be verified that (5.8.3) is solvable if and only if $\beta' \equiv \beta \equiv 0 \pmod{2}$. We have to show that none of these solutions modulo 4 satisfies the first congruence of (5.8.2). The one solution $\beta' \equiv \beta \equiv 0 \pmod{2}$ results in four solutions modulo 4, namely $\beta \equiv 0$ or $2 \pmod{4}$ and $\beta' \equiv 0$ or $2 \pmod{4}$, respectively. For any of these four cases, the left side of the first congruence

of (5.8.2) is congruent to zero modulo 4. We conclude that (5.8.2) is not solvable. \square

We now show that the above class of groups contains a group of order 2^7 .

Corollary 5.9. *There exists a group G of order 2^7 such that $K(G) \neq G'$.*

Proof. Consider the abelian group $W = \langle u \rangle \times \langle u \rangle \times \langle u \rangle$, where u has order 4 and v and w each have order 2, thus $|W| = 2^4$. The group G will be constructed by three split extensions starting with W . Let $B = W \rtimes \langle b \rangle$ be the semidirect product of W with the cyclic group $\langle b \rangle \cong C_2$, where b induces an automorphism of order 2 on W . The action of b on the generators of W is given as follows:

$$(5.9.1) \quad [u, b] = u^2 \quad \text{and} \quad [v, b] = [w, b] = 1.$$

The defining relations of B are those of W , (5.9.1), and $b^2 = 1$. We observe $|B| = 2^5$.

Next let $C = B \rtimes \langle c \rangle$ be the semidirect product of B with the cyclic group $\langle c \rangle \cong C_2$, where c induces an automorphism of order 2 on B . The action of c on the generators of B is given as follows:

$$(5.9.2) \quad [u, c] = [v, c] = [w, c] = 1 \quad \text{and} \quad [b, c] = w.$$

The defining relations of C are those of B , (5.9.2), and $c^2 = 1$. We observe $|C| = 2^6$.

Finally, let $G = C \rtimes \langle d \rangle$ be the semidirect product of C with the cyclic group $\langle d \rangle \cong C_2$, where d induces an automorphism of order 2 on C . The action of d on the generators of C is given as follows:

$$(5.9.3) \quad [u, d] = u^2, \quad [v, d] = [w, d] = 1, \quad [b, d] = u, \quad \text{and} \quad [c, d] = vw.$$

The defining relations of G are those of C , (5.9.3), and $d^2 = 1$. We observe $|G| = 2^7$.

The verification of the claims leading to the construction of G is straightforward but lengthy and is left to the reader. Next we show $W = G'$. We observe $G' \leq W$, since $G/W = \langle bW, cW, dW \rangle \cong C_2 \times C_2 \times C_2$, and so G/W is abelian. On the other hand, $u = [b, d] \in G'$, $w = [b, c] \in G'$, and $v = [c, d][b, c] \in G'$. It follows $W = \langle u, v, w \rangle \leq G'$. We conclude $W = G'$. Furthermore, $\gamma_3(G) = \langle u^2 \rangle$ and $\gamma_4(G) = 1$. Hence G has class 3 precisely.

To apply Proposition 5.8 we choose new generators for G , namely $G = \langle a, b, c \rangle$ with $a = db$. We have $u^2 = [b, d, b] = [b, a, b]^b$. It follows $[a, b, b] = u^2$. Now $u = [b, d] = [b, a][b, a, b]$. This together with the above leads to $[a, b] = u$. Furthermore, $[b, c] = w$ and $v = [c, d][b, c]$. This together with expansion and the relations of G leads to $v = [c, a]^b$. We conclude $v = [a, c]$.

It remains to show that $G = \langle a, b, c \rangle$ satisfies the assumptions of Proposition 5.8. Since $[w, x] = [v, x] = 1$ for $x \in \{b, c, d\}$, it follows $[b, c], [a, c] \in Z(G)$. Now $b^2 = c^2 = d^2 = 1$ imply $b^2, c^2, (ab)^2 \in Z(G)$. Furthermore, $1 = d^2 = (ab)^2 = a^2[a, b]b^2 = a^2u$. It follows $a^4 = u^2$, and thus $a^4 \in Z(G)$.

We conclude that G satisfies the assumptions of Proposition 5.8, hence $G' \neq K(G)$. \square

Acknowledgments. The first author would like to thank the administration at the University of Evansville for their generous hospitality while visiting there. The authors would also like to thank Wolfgang P. Kappe and Marcin Mazur for their careful reading of this paper and their helpful insights and suggestions.

REFERENCES

1. H. U. Besche, B. Eick, and E. A. O'Brien, *The groups of order at most 2000*, Electron. Res. Announc. Amer. Math. Soc. **7** (2001), 1–4 (electronic).
2. N. Blackburn, *On prime-power groups with two generators*, Proc. Cambridge Philos. Soc. **54** (1958), 327–337.
3. R. D. Carmichael, *Introduction to the theory of groups of finite order*, Dover Publications Inc., New York, 1956.
4. D. S. Dummit and R. M. Foote, *Abstract algebra*, Prentice Hall Inc., Englewood Cliffs, NJ, 1991.
5. W. B. Fite, *On metabelian groups*, Trans. Amer. Math. Soc. **3** (1902), no. 3, 331–353.
6. The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4*, 2004, (<http://www.gap-system.org>).
7. G. T. Hogan and W. P. Kappe, *On the H_p -problem for finite p -groups*, Proc. Amer. Math. Soc. **20** (1969), 450–454.
8. B. Huppert, *Endliche Gruppen I*, Die Grundlehren der Mathematischen Wissenschaften, Band 134, Springer-Verlag, Berlin, 1967.
9. L.-C. Kappe, R. F. Morse, and E. Snyder, *In search of the smallest group in which commutators do not form a subgroup*, in preparation.
10. I. D. Macdonald, *The theory of groups*, Clarendon Press, Oxford, 1968.
11. D. MacHale, *Minimum counterexamples in group theory*, Math. Mag. **54** (1981), no. 1, 23–28.
12. G. A. Miller, *On the commutator groups*, Bull. Amer. Math. Soc. **4** (1898), 135–139.
13. G. Pazderski, *The orders of which only belong metabelian groups*, Math. Nachr. **95** (1980), 7–16.
14. D. M. Rodney, *On cyclic derived subgroups*, J. London Math. Soc. (2) **8** (1974), 642–646.
15. ———, *Commutators and abelian groups*, J. Austral. Math. Soc. Ser. A **24** (1977), no. 1, 79–91.
16. E. Spiegel, *Calculating commutators in groups*, Math. Mag. **49** (1976), no. 4, 192–194.

DEPARTMENT OF MATHEMATICAL SCIENCES, STATE UNIVERSITY OF NEW YORK AT BINGHAMTON, BINGHAMTON, NY 13902-6000 USA

E-mail address: menger@math.binghamton.edu

URL: www.math.binghamton.edu/menger

DEPARTMENT OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE, UNIVERSITY OF EVANSVILLE, EVANSVILLE IN 47722 USA

E-mail address: rfmorse@evansville.edu

URL: faculty.evansville.edu/rm43