TWO GENERATOR p-GROUPS OF NILPOTENCY CLASS 2 AND THEIR CONJUGACY CLASSES

AZHANA AHMAD, ARTURO MAGIDIN,
AND ROBERT FITZGERALD MORSE

Abstract. We give a classification of two-generator p-groups of nilpotency class 2. Using this classification, we give a formula for the number of such groups of order p^n in terms of the partitions of n of length 3, and find formulas for the number and size of their conjugacy classes.

1. Introduction

In [1], Bacon and Kappe give a classification of 2-generator p-groups of nilpotency class 2 with the goal of computing their nonabelian tensor squares; that classification was also an attempt to correct errors found in [9]. Later [5], Kappe, Visscher, and Sarmin extended the classification to the case of 2-groups. The idea in these classifications is to start with a generator of minimal order b, and then add a second generator a of minimal order among those that generate the group together with b; then one looks at the intersections $\langle a\rangle \cap [G,G]$ and $\langle b\rangle \cap [G,G]$ and proceeds by considering the different possibilities.

These classifications were used to compute the nonabelian tensor squares of these groups [1, 2, 5], as well as identifying those that are capable [2, 6, 7]. When the first author was developing a formula to count the conjugacy classes of the 2-generator 2-groups of class two, she discovered that the classification was incomplete; based on her example, we also discovered that the classification for the p-groups, $p > 2$, was likewise incomplete.

The goal of this paper is to correct these omissions with a complete classification. Our approach to classifying these groups is to exploit the fact they are all central extensions of a cyclic p-group by an abelian p-group of rank 2. This viewpoint simplifies the counting of conjugacy classes, and the resulting classification also makes it straightforward to count all the groups of this class of order p^n for any given n. Our

2000 *Mathematics Subject Classification.* 20F18, 20J99.
Key words and phrases. p-groups.

count agrees with the one recently obtained by C. Voll using zeta functions [10], providing independent verification of our classification.

As the second and third authors were preparing a separate work concerned with the computation of the nonabelian tensor squares and other functors for these groups, a paper by Miech [8] was brought to our attention. In this paper, Miech uses an approach very similar to ours to classify the 2-generated p-groups with cyclic commutator subgroup for odd p. Miech's classification is somewhat more complex than ours because of the need for more parameters to account for the groups of class 3 that occur, and seems difficult to extend to the $p = 2$ case. Where Miech's classification overlaps with ours, the two agree.

Since both the classification theorem and our formula for counting the conjugacy classes of these group are self-contained and straightforward we state them now.

Theorem 1.1. *Let p be a prime and $n > 2$ a positive integer. Every 2-generated p-group of class exactly 2 corresponds to an ordered 5-tuple of integers, $(\alpha, \beta, \gamma; \rho, \sigma)$, such that:*

(i) $\alpha \geq \beta \geq \gamma \geq 1$,
(ii) $\alpha + \beta + \gamma = n$,
(iii) $0 \leq \rho \leq \gamma$ *and* $0 \leq \sigma \leq \gamma$,

where $(\alpha, \beta, \gamma; \rho, \sigma)$ corresponds to the group presented by

$$G = \left\langle a, b \;\middle|\; [a,b]^{p^\gamma} = [a,b,a] = [a,b,b] = 1, a^{p^\alpha} = [a,b]^{p^\rho}, b^{p^\beta} = [a,b]^{p^\sigma} \right\rangle.$$

Moreover:

(1) *If $\alpha > \beta$, then G is isomorphic to:*
  (a) $(\alpha, \beta, \gamma; \rho, \gamma)$ *when* $\rho \leq \sigma$.
  (b) $(\alpha, \beta, \gamma; \gamma, \sigma)$ *when* $0 \leq \sigma < \sigma + \alpha - \beta \leq \rho$ *or* $\sigma < \rho = \gamma$.
  (c) $(\alpha, \beta, \gamma; \rho, \sigma)$ *when* $0 \leq \sigma < \rho < \min(\gamma, \sigma + \alpha - \beta)$.
(2) *If $\alpha = \beta > \gamma$, or $\alpha = \beta = \gamma$ and $p > 2$, then G is isomorphic to* $(\alpha, \beta, \gamma; \min(\rho, \sigma), \gamma)$.
(3) *If $\alpha = \beta = \gamma$ and $p = 2$, then G is isomorphic to:*
  (a) $(\alpha, \beta, \gamma; \min(\rho, \sigma), \gamma)$ *when* $0 \leq \min(\rho, \sigma) < \gamma - 1$.
  (b) $(\alpha, \beta, \gamma; \gamma - 1, \gamma - 1)$ *when* $\rho = \sigma = \gamma - 1$.
  (c) $(\alpha, \beta, \gamma; \gamma, \gamma)$ *when* $\min(\rho, \sigma) \geq \gamma - 1$ *and* $\max(\rho, \sigma) = \gamma$.

The groups listed in 1(a)–3(c) *are pairwise nonisomorphic.*

It is family 1(c) that is missing in the classifications from [1, 5]. In addition, we discovered that the families of 2-groups given in [5] were not disjoint, listing the groups $(\gamma, \gamma, \gamma; \gamma, \gamma)$ twice for each $\gamma > 0$. We will discuss this in more detail in the final section.

Theorem 1.2. *Let G be a 2-generator p-group of nilpotency class exactly 2. If G has order p^n and has derived subgroup of order p^γ, then G has*

$$p^{n-\gamma}\left(1+p^{-1}-p^{-(\gamma+1)}\right) \tag{1.3}$$

conjugacy classes.

By a result of P. Hall (see [3] Kapital V, Satz 15.2), any p-group G of order p^n has

$$p^e+p^2\big(m+k(p-1)\big) \tag{1.4}$$

conjugacy classes, where $e\in\{0,1\}$ and $e\equiv n \pmod 2$, and $m=\lfloor\frac{n}{2}\rfloor$. The nonnegative integer k was called the *abundance of* G in [4], and is denoted by $a(G)$. An immediate consequence of Theorem 1.2 is that we are able to compute the abundance of the 2-generator p-groups of class exactly 2. By equating (1.3) and (1.4) and solving for $a(G)$ we obtain the following result.

Corollary 1.5. *Let G be a 2-generator p-group of nilpotency class exactly 2. If G has order p^n and has derived subgroup of order p^γ, then $a(G)$, the abundance of G, is*

$$a(G)=\frac{p^{n-\gamma}\left(1+p^{-1}-p^{-(\gamma+1)}\right)-p^e-mp^2}{p^2(p-1)},$$

where $m=\lfloor n/2\rfloor$ and $e\in\{0,1\}$, $e\equiv n \pmod 2$.

The paper is structured as follows. In the next section we fix our notation, establish some preliminary results, and outline our strategy for classifying the 2-generator p-groups of class 2. In Section 3 we prove Theorem 1.1, and in Section 4 we enumerate the number of groups of order p^n in our class for a fixed p and n. In Section 5 we provide formulas for the number and size of the conjugacy classes for these groups as well as prove Theorem 1.2. In the last section, we describe how to translate the descriptions in the previously published classifications into our 5-parameter classification.

2. Preliminaries

We write our groups multiplicatively, with 1 denoting the identity of the group. We let C_m represent the cyclic group of order m. The commutator of x and y is $[x,y]=x^{-1}y^{-1}xy$. If G is nilpotent of class (at most) 2, then the commutator bracket is alternating bilinear, and we have the well-known formula $(xy)^n=x^ny^n[y,x]^{\binom{n}{2}}$, where $\binom{n}{2}=\frac{n(n-1)}{2}$ for all integers n.

Let H be a nilpotent group of class 2. Then H' is a central subgroup of H. Suppose a and b are elements of H, and suppose further that a has finite order m. Then $1 = [a^m, b] = [a, b]^m$. Hence we conclude that the order of $[a, b]$ divides m.

Let G be a 2-generator p-group of class 2 of order p^n. Then G' is a central subgroup of G that is isomorphic to C_{p^γ} with $\gamma \geq 1$, and G/G' is isomorphic to $C_{p^\alpha} \times C_{p^\beta}$ with $n = \alpha + \beta + \gamma$. Without loss of generality assume $\alpha \geq \beta$. Let $\{a, b\}$ be a transversal of G/G'. Then a^{p^α} and b^{p^β} are elements of G' and we have

$$[a^{p^\alpha}, b] = 1 = [a, b]^{p^\alpha} \quad \text{and} \quad [a, b^{p^\beta}] = 1 = [a, b]^{p^\beta}.$$

Hence p^γ, the order of G', divides both p^α and p^β. It follows that $1 \leq \gamma \leq \beta \leq \alpha$.

From this analysis we may view any 2-generator group G of order p^n and class 2 as a central extension of the form

$$1 \longrightarrow C_{p^\gamma} \xrightarrow{\psi} G \xrightarrow{\eta} C_{p^\alpha} \times C_{p^\beta} \longrightarrow 1, \tag{2.1}$$

where $n = \alpha + \beta + \gamma$ and $\alpha \geq \beta \geq \gamma \geq 1$. Therefore to enumerate all 2-generator p-groups of class 2 of order p^n we must consider all positive partitions (α, β, γ) of n of length 3. We denote by $\mathfrak{G}_p(\alpha, \beta, \gamma)$ the set of nonisomorphic central extensions of the form (2.1) with nilpotency class exactly 2. Any group in $\mathfrak{G}_p(\alpha, \beta, \gamma)$ is 2-generated and has order p^n, where $n = \alpha + \beta + \gamma$.

Lemma 2.2. *Let $n \geq 3$. For any positive partition (α, β, γ) of n, the set $\mathfrak{G}_p(\alpha, \beta, \gamma)$ is nonempty.*

Proof. Let (α, β, γ) be a positive partition of n. We claim that

$$G = \langle a, b \mid a^{p^\alpha} = b^{p^\beta} = [a, b]^{p^\gamma} = 1, [a, b, a] = [a, b, b] = 1 \rangle$$

is a group in $\mathfrak{G}_p(\alpha, \beta, \gamma)$. Indeed, the group G is 2-generated and nilpotent of class 2. The derived subgroup G' is cyclic of order p^γ with G/G' isomorphic to $C_{p^\alpha} \times C_{p^\beta}$. □

Let $\mathcal{G}_{p^n} = \{\mathfrak{G}_p(\alpha, \beta, \gamma) \mid (\alpha, \beta, \gamma)$ is a positive partition of $n \geq 3\}$. The following fact is nearly immediate.

Lemma 2.3. *Let p be a prime and let $n \geq 3$. The set $\mathcal{G}_{p^n}$ is a partition of all 2-generator p-groups of class 2 of order p^n*

Proof. Let G be an element of $\mathfrak{G}_p(\alpha, \beta, \gamma)$ and H be an element of $\mathfrak{G}_p(\alpha', \beta', \gamma')$ such that (α, β, γ) and $(\alpha', \beta', \gamma')$ are unequal. Then G and H have nonisomorphic derived subgroups or they have different abelianizations. In either case G and H cannot be isomorphic. □

3. The groups in $\mathfrak{G}_p(\alpha, \beta, \gamma)$

In this section we determine the nonisomorphic types within each $\mathfrak{G}_p(\alpha, \beta, \gamma)$. We will show that each isomorphism class is determined by a pair of nonnegative integers ρ and σ, with $0 \le \rho \le \gamma$ and $0 \le \sigma \le \gamma$, and subject to some ancillary conditions, so that each 2-generated p-group of class exactly 2 corresponds to a unique ordered quintuple $(\alpha, \beta, \gamma; \rho, \sigma)$.

In what follows, we will write "$0 \le \rho, \sigma \le \gamma$" to mean that $0 \le \rho \le \gamma$ and $0 \le \sigma \le \gamma$ both hold.

For any extension

$$1 \longrightarrow N \xrightarrow{\psi} E \xrightarrow{\eta} G \longrightarrow 1,$$

the relations of E are the relations of N (under the injection ψ), the action of G on N via the transversal function $\tau : G \to E$ and the injection ψ, and the relations determined by the relations of G. If $r = g_1 \cdots g_n$ is a relator of G then $\tau(r)$ need not be the identity in E; it is corrected by an element of the center of N. Hence $\tau(r) \cdot \psi(c) = 1$ for some $c \in Z(N)$ is a relator in E.

Any group G in $\mathfrak{G}_p(\alpha, \beta, \gamma)$ is a central extension

$$1 \longrightarrow C_{p^\gamma} \xrightarrow{\psi} G \xrightarrow{\eta} C_{p^\alpha} \times C_{p^\beta} \longrightarrow 1.$$

Since this is a central extension, the action of $C_{p^\alpha} \times C_{p^\beta}$ on C_{p^γ} is trivial. Let $\langle c' \rangle \cong C_{p^\gamma}$ and let $\psi(\langle c' \rangle) \le G$ be generated by $\psi(c') = c$. Let $\langle a' \rangle \times \langle b' \rangle \cong C_{p^\alpha} \times C_{p^\beta}$ with relators $[a', b']$, a'^{p^α}, b'^{p^β}. Following our general analysis above and setting $\tau(a') = a$ and $\tau(b') = b$, the relations of any group in $\mathfrak{G}_p(\alpha, \beta, \gamma)$ are $c^{p^\gamma} = 1$, $[a, b] = c^i$, $a^{p^\alpha} = c^j$, $b^{p^\beta} = c^k$, $c^a = c$, and $c^b = c$. Since G' must be cyclic of order p^γ, we must have $\gcd(i, p) = 1$.

Some values i, j, and k give isomorphic groups. Our goal is to select exactly those values of i, j, and k that enumerate all of the nonisomorphic groups in $\mathfrak{G}_p(\alpha, \beta, \gamma)$ with no repetitions. We assume that $0 < i, j, k \le p^\gamma$.

We begin by making some simplifications. The proposition below shows that the isomorphism type of G depends only on the largest powers of p that divide i, j, and k.

Proposition 3.1. *Fix $\alpha \ge \beta \ge \gamma$, and let i, j, k be positive integers, $0 < i, j, k \le p^\gamma$, with $\gcd(i, p) = 1$. Write $j = up^\rho$, $k = vp^\sigma$, with $\gcd(uv, p) = 1$, $0 \le \rho \le \gamma$, and $0 \le \sigma \le \gamma$. We let $G, H \in \mathfrak{G}_p(\alpha, \beta, \gamma)$*

be the groups

$$\begin{aligned} G &= \left\langle a,b,c \;\middle|\; c^a = c, c^b = c, [a,b] = c^i, a^{p^\alpha} = c^j, b^{p^\beta} = c^k \right\rangle, \\ H &= \left\langle x,y,z \;\middle|\; z^x = z, z^y = z, [x,y] = z, x^{p^\alpha} = z^{p^\rho}, x^{p^\beta} = z^{p^\sigma} \right\rangle. \end{aligned}$$

Then G is isomorphic to H.

Proof. If $\rho = \sigma = \gamma$, then $j = k = p^\gamma$. Set $a_1 = a$, $b_1 = b$, and $c_1 = c^i$; then the elements a_1, b_1, c_1 of G satisfy the same relations as $x, y, z \in H$, and hence we have an onto homomorphism $H \to G$ that maps $x \mapsto a_1$, $y \mapsto b_1$, and $z \mapsto c_1$. Since the two groups have the same order, this map is an isomorphism.

If $\rho < \sigma = \gamma$, then pick s such that $is \equiv u \pmod{p^{\gamma-\rho}}$, and set $a_1 = a$, $b_1 = b^s$, and $c_1 = c^{is}$. Then $[a_1, b_1] = c^{is} = c_1$, $a_1^{p^\alpha} = c^j = c^{up^\rho} = c^{isp^\rho} = c_1^{p^\rho}$, and $b_1^{p^\beta} = c^{p^\gamma} = c_1^{p^\gamma}$, so again we have an onto homomorphism $H \to G$, which proves the two groups are isomorphic.

If $\sigma < \rho = \gamma$, then pick r such that $ir \equiv v \pmod{p^{\gamma-\sigma}}$, set $a_1 = a^r$, $b_1 = b$, and $c_1 = c^{ir}$; again, we obtain a homomorphism from H onto G, showing that G is isomorphic to H.

Finally, assume that $\rho, \sigma < \gamma$. Pick r such that $ir \equiv v \pmod{p^{\gamma-\sigma}}$, s such that $is \equiv u \pmod{p^{\gamma-\rho}}$, and set $t \equiv irs \pmod{p^\gamma}$. Let $a_1 = a^r$, $b_1 = b^s$, and $c_1 = c^t$. The nontrivial relations to check are:

$$\begin{aligned} [a_1, b_1] &= [a,b]^{rs} = c^{irs} = c^t = c_1 = c_1^{a_1} = c_1^{b_1}, \\ a_1^{p^\alpha} &= a^{rp^\alpha} = c^{rup^\rho} = c^{risp^\rho} = c^{tp^\rho} = c_1^{p^\rho}, \\ b_1^{p^\beta} &= b^{sp^\beta} = c^{svp^\sigma} = c^{srip^\sigma} = c^{tp^\sigma} = c_1^{p^\sigma}. \end{aligned}$$

Therefore, there is a homomorphism from H onto G, and hence G is isomorphic to H, as claimed. □

Thus we see that the isomorphism type of a 2-generated p-group of class 2 depends on five parameters: α, β, and γ, giving the isomorphism types of G^{ab} and $[G,G]$; and on parameters ρ and σ. We establish the following notation.

Definition 3.2. Let $\alpha \geq \beta \geq \gamma > 0$ be npositive integers, and let ρ, σ be integers, $0 \leq \rho, \sigma \leq \gamma$. We will use the ordered 5-tuple $(\alpha, \beta, \gamma; \rho, \sigma)$ to denote the group $G \in \mathfrak{G}_p(\alpha, \beta, \gamma)$ presented by

$$G = \left\langle a,b,c \;\middle|\; [a,b] = c,\ c^a = c,\ c^b = c,\ a^{p^\alpha} = c^{p^\rho},\ b^{p^\beta} = c^{p^\sigma} \right\rangle.$$

Proposition 3.1 guarantees that every group in $\mathfrak{G}_p(\alpha, \beta, \gamma)$ is isomorphic to at least one of the groups of the form $(\alpha, \beta, \gamma; \rho, \sigma)$. We

still need to determine which choices of ρ and σ may lead to isomorphic groups. The goal of the next few results is to help discover when $(\alpha, \beta, \gamma; \rho, \sigma)$ is isomorphic to $(\alpha, \beta, \gamma; r, s)$.

Lemma 3.3. *Let p be a prime, and let $\alpha \geq \beta > 0$ be integers. Let $A = C_{p^\alpha} \times C_{p^\beta}$, with a and b generating the respective cyclic factors. Then every automorphism of A is of the form*

$$a \mapsto a^k b^\ell, \qquad b \mapsto a^{mp^{\alpha-\beta}} b^n,$$

where k is determined modulo p^α, where ℓ, m, and n are determined modulo p^β, and where $kn - \ell m p^{\alpha-\beta}$ is relatively prime to p.

Proof. Any endomorphism is uniquely determined as above, so we only need to verify that the endomorphism is invertible precisely when the determinant $kn - \ell m p^{\alpha-\beta}$ is relatively prime to p. If $\alpha = \beta$, the condition is exactly that the corresponding 2×2 matrix with coefficients in $\mathbb{Z}/p^\alpha\mathbb{Z}$ be invertible.

If $\alpha > \beta$, then the condition is equivalent to k and n being relatively prime to p. In this case, the necessity is immediate: if k is divisible by p then the image of a has order strictly less than p^α, and if n is divisible by p then the image of b has order strictly less than p^β. For sufficiency, assume that $\gcd(p, kn) = 1$. Let d be an integer such that $d(kn - \ell m p^{\alpha-\beta}) \equiv 1 \pmod{p^\beta}$. Let f be such that $fk \equiv 1 \pmod{p^\alpha}$, and let $g \equiv f(1 + d\ell m p^{\alpha-\beta}) \pmod{p^\alpha}$. It is now straightforward to verify that $a \mapsto a^g b^{-d\ell}$ and $b \mapsto a^{-dmp^{\alpha-\beta}} b^{dk}$ yields the inverse of the original map. □

Theorem 3.4. *Let p be a prime, and fix $\alpha \geq \beta \geq \gamma > 0$. Let ρ, σ, r, s be integers, $0 \leq \rho, \sigma, r, s \leq \gamma$, and let G be the group $(\alpha, \beta, \gamma; \rho, \sigma)$. If G is isomorphic to $(\alpha, \beta, \gamma; r, s)$, then there exist integers k, ℓ, m, n, v, w such that $\gcd(p, kn - \ell m p^{\alpha-\beta}) = 1$ and $\gcd(p, vw) = 1$, with $(a^k b^\ell)^{p^\alpha} = c^{vp^r}$ and $(a^{mp^{\alpha-\beta}} b^n)^{p^\beta} = c^{wp^s}$. Conversely, if we have integers k, ℓ, m, n, v, and w as above, then G is isomorphic to the group $(\alpha, \beta, \gamma; r, s)$.*

Proof. Let H be the group $(\alpha, \beta, \gamma; r, s)$, and suppose that there is an isomorphism $f\colon H \to G$. To avoid possible confusion, denote the generators of H by a_H, b_H, and c_H. The isomorphism f induces an isomorphism $\overline{f}\colon H^{\mathrm{ab}} \to G^{\mathrm{ab}}$, so we know there exist integers k, ℓ, m, n, x, y with $\gcd(p, kn - \ell m p^{\alpha-\beta}) = 1$ such that $f(a_H) = a^k b^\ell c^x$ and $f(b_H) = a^{mp^{\alpha-\beta}} b^n c^y$. We also know that f restricts to an isomorphism from $[H, H]$ to $[G, G]$, so $f(c_H) = c^v$ for some integer v that is

relatively prime to p. Since c is central and $\gamma \leq \beta \leq \alpha$, we have:

$$\begin{aligned} (a^k b^\ell)^{p^\alpha} &= (a^k b^\ell c^x)^{p^\alpha} = f(a_H^{p^\alpha}) = f(c_H^{p^r}) = c^{vp^r}, \\ \text{and} \quad (a^{mp^{\alpha-\beta}} b^n)^{p^\beta} &= (a^{mp^{\alpha-\beta}} b^n c^y)^{p^\beta} = f(b_H^{p^\beta}) = f(c_H^{p^s}) = c^{vp^s}. \end{aligned}$$

Setting $w = v$ proves the necessity.

Conversely, suppose we have integers k, ℓ, m, n, v, and w with the given properties. Set $a_1 = a^k b^\ell$, $b_1 = a^{mp^{\alpha-\beta}} b^n$, and $c_1 = c$. Since $\gcd(p, kn - \ell m p^{\alpha-\beta}) = 1$, the images of a_1 and b_1 generate G^{ab}, and so by Proposition 3.1, there is an isomorphism between $H = (\alpha, \beta, \gamma; r, s)$ and $\langle a_1, b_1, c_1 \rangle$; since these elements generate G, we obtain the desired isomorphism. □

Thus, to determine whether the group $(\alpha, \beta, \gamma; \rho, \sigma)$ is isomorphic to the group $(\alpha, \beta, \gamma; r, s)$, it suffices to check if there exist integers k, ℓ, m, n, x, w, with $\gcd(p, kn - \ell m p^{\alpha-\beta}) = \gcd(p, xw) = 1$, and such that $(a^k b^\ell)^{p^\alpha} = c^{wp^r}$ and $(a^{mp^{\alpha-\beta}} b^n)^{p^\beta} = c^{xp^s}$. Conversely, if we find all possible exponents wp^r and xp^s for suitable choices of k, ℓ, m, n (and by Proposition 3.1 it suffices to determine the highest powers of p that divide those exponents), we will determine all such isomorphisms.

Suppose G is the group $(\alpha, \beta, \gamma; \rho, \sigma)$ with $0 \leq \rho, \sigma \leq \gamma$. For future reference, we have the following computations:

$$\begin{aligned} \left(a^k b^\ell\right)^{p^\alpha} &= a^{kp^\alpha} b^{\ell p^\alpha} [b, a]^{k\ell \binom{p^\alpha}{2}} \\ &= c^{kp^\rho + \ell p^{\sigma+\alpha-\beta} - k\ell \binom{p^\alpha}{2}}, \end{aligned} \tag{3.5}$$

$$\begin{aligned} \text{and} \quad \left(a^{mp^{\alpha-\beta}} b^n\right)^{p^\beta} &= a^{mp^\alpha} b^{np^\beta} [b, a]^{mnp^{\alpha-\beta} \binom{p^\beta}{2}} \\ &= c^{mp^\rho + np^\sigma - mnp^{\alpha-\beta} \binom{p^\beta}{2}}. \end{aligned} \tag{3.6}$$

By Theorem 3.4, we only need to determine the largest powers of p that divide the exponents of c in the above expressions. The binomial coefficient and the factor $p^{\alpha-\beta}$ lead us to consider separate cases: when $\alpha > \beta$; when $\alpha = \beta$ and either $\beta > \gamma$ or $p > 2$; and when $\alpha = \beta = \gamma$ and $p = 2$. We treat each of these cases in turn.

Theorem 3.7. *Let p be a prime, and fix $\alpha > \beta \geq \gamma > 0$. The groups $(\alpha, \beta, \gamma; \rho, \sigma)$ and $(\alpha, \beta, \gamma; r, s)$, where $0 \leq \rho, \sigma, r, s \leq \gamma$, are isomorphic if and only if:*

(i) *$\rho = r$ and $\sigma = s$; or*
(ii) *$\rho = r$, $\sigma \geq \rho$, and $s \geq r$; or*
(iii) *$\sigma = s$, $\rho \geq \sigma + (\alpha - \beta)$, and $r \geq s + (\alpha - \beta)$.*

In particular, the group $(\alpha, \beta, \gamma; \rho, \sigma)$ is isomorphic to one and only one of the groups listed in 1(a)–1(c) *of Theorem 1.1, according to the conditions listed there.*

Proof. Let G be the group $(\alpha, \beta, \gamma; \rho, \sigma)$, with $\alpha > \beta \geq \gamma > 0$; by Theorem 3.4, any isomorphism is determined by a pair of elements $a^k b^\ell$ and $a^{mp^{\alpha-\beta}} b^n$, with kn relatively prime to p. Since $\alpha > \beta$ and $\alpha > \gamma$, the summands containing the binomial coefficients in the exponents of c in (3.5) and (3.6) are both divisible by p^γ and so vanish.

Thus, the exponent of c in (3.5) is $kp^\rho + \ell p^{\sigma+\alpha-\beta}$, while the exponent of c in (3.6) is $mp^\rho + np^\sigma$. If $\rho \leq \sigma$, then the highest power of p that divides the former is exactly p^ρ (since $\gcd(p, k) = 1$), and the highest power of p that divides the latter is at least p^ρ, possibly larger depending on the value of $m + np^{\sigma-\rho}$; this is condition in (ii). If we have $\rho \geq \sigma + \alpha - \beta$, then the highest power of p that divides the exponent of c in (3.5) is at least $p^{\sigma+\alpha-\beta}$, possibly larger depending on the value of $kp^{\rho-\sigma-\alpha+\beta} + \ell$; whereas the highest power of p that divides the exponent of c in (3.6) is exactly p^σ since $\gcd(p, n) = 1$. Thus, we are in the case contemplated in condition (iii). Finally, if $\sigma < \rho < \sigma + \alpha - \beta$, then the highest power of p that divides the exponent of c in (3.5) is exactly p^ρ since $\gcd(p, k) = 1$, and the largest power in (3.6) is exactly p^σ (again, since $\gcd(p, n) = 1$), and we are in the case contemplated in (i). Thus, the given conditions are necessary for an isomorphism.

Conversely, condition (i) is trivially sufficient. Assume next that $\rho = r$, $\rho \leq \sigma$ and $r \leq s$, and we want to prove that $(\alpha, \beta, \gamma; \rho, \sigma)$ is isomorphic to $(\alpha, \beta, \gamma; r, s)$. Setting $k = 1$, $\ell = 0$, $m = p^{s-r} - p^{\sigma-\rho}$, and $n = 1$, the exponent of c in (3.5) is of course p^ρ, while the exponent of c in (3.6) is

$$(p^{s-\rho} - p^{\sigma-\rho})p^\rho + p^\sigma = p^s - p^\sigma + p^\sigma = p^s,$$

proving that $(\alpha, \beta, \gamma; \rho, \sigma)$ is isomorphic to $(\alpha, \beta, \gamma; r, s)$. Thus, (ii) is sufficient. Finally, suppose that $\sigma = s$, $\rho \geq \sigma + \alpha - \beta$, and $r \geq s + \alpha - \beta$. Then set $k = 1$, $\ell = p^{r-(\sigma+\alpha-\beta)} - p^{\rho-(\sigma+\alpha-\beta)}$, $m = 0$, and $n = 1$. The the exponent in (3.5) is

$$p^\rho + (p^{r-(\sigma+\alpha-\beta)} - p^{\rho-(\sigma+\alpha-\beta)})p^{\sigma+\alpha-\beta} = p^\rho + p^r - p^\rho = p^r,$$

while the exponent in (3.6) is $p^\sigma = p^s$, proving that $(\alpha, \beta, \gamma; \rho, \sigma)$ is indeed isomorphic to $(\alpha, \beta, \gamma; r, s)$ as claimed. □

Theorem 3.8. *Let p be a prime, and fix $\alpha = \beta \geq \gamma > 0$. If $p > 2$ or $\beta > \gamma$, then the groups $(\alpha, \beta, \gamma; \rho, \sigma)$ and $(\alpha, \beta, \gamma; r, s)$ are isomorphic if and only if $\min(\rho, \sigma) = \min(r, s)$. In particular, the group $(\alpha, \beta, \gamma; \rho, \sigma)$ is isomorphic to $(\alpha, \beta, \gamma; \min(\rho, \sigma), \gamma)$, as in* (2) *of Theorem 1.1.*

Proof. For the necessity of the condition, note that selecting $k = 0$, $\ell = 1$, $m = 1$, and $n = 0$ as in Theorem 3.4 shows we may assume without loss of generality that $\rho \leq \sigma$. Then the exponents of c in (3.5) and (3.6) simplify to $p^\rho(k + \ell p^{\sigma-\rho})$ and $p^\rho(m + np^{\sigma-\rho})$. If $\sigma > \rho$, since at most one of k and m are multiples of p we obtain that at least one of these two expressions will be divisible by exactly p^ρ and no higher power, so $\min(r, s)$ is equal to ρ. On the other hand, if $\sigma = \rho$ and $k + \ell$ is divisible by p, then $kn - \ell m \equiv kn + km \equiv k(n + m) \pmod{p}$ and the fact that $kn - \ell m$ is prime to p yields that $m + n$ is prime to p; symmetrically if $m + n$ is divisible by p then $k + \ell$ is necessarily be prime to p, so once again we have $\min(r, s) = \rho$. This proves the necessity.

For sufficiency, we may assume without loss of generality that $\rho = r$, $\rho \leq \sigma$, and $r \leq s$. Then set $k = 1$, $\ell = 0$, $m = p^{s-\rho} - p^{\sigma-\rho}$, and $n = 1$; the exponent of c in (3.5) is $p^\rho = p^r$, and the exponent in (3.6) is

$$(p^{s-\rho} - p^{\sigma-\rho})p^\rho + p^\sigma = p^s - p^\sigma + p^\sigma = p^s,$$

proving that $(\alpha, \beta, \gamma; \rho, \sigma)$ is isomorphic to $(\alpha, \beta, \gamma; r, s)$, as claimed. □

Theorem 3.9. *Let $p = 2$ and fix $\alpha = \beta = \gamma > 0$. The groups $(\alpha, \beta, \gamma; \rho, \sigma)$ and $(\alpha, \beta, \gamma; r, s)$, where $0 \leq \rho, \sigma, r, s \leq \gamma$, are isomorphic if and only if:*

(i) $\min(\rho, \sigma) = \min(r, s)$ *and* $\max(\rho, \sigma) = \max(r, s)$*; or*
(ii) *exactly one of ρ, σ, r, s is equal to $\gamma - 1$ and the remaining three are equal to γ; or*
(iii) $\min(\rho, \sigma) = \min(r, s) < \gamma - 1$.

In particular, the group $(\alpha, \beta, \gamma; \rho, \sigma)$ is isomorphic to exactly one of the groups in 3(a)–3(c) *of Theorem 1.1 according to the conditions listed there.*

Proof. Let G be the group $(\alpha, \beta, \gamma; \rho, \sigma)$; without loss of generality we may assume that $\rho \leq \sigma$, since all conditions are symmetric and picking $k = 0$, $\ell = 1$, $m = 1$, and $n = 0$ will yield an isomorphism between $(\alpha, \beta, \gamma; \rho, \sigma)$ and $(\alpha, \beta, \gamma; \sigma, \rho)$.

Since $p = 2$ and $\alpha = \beta = \gamma$, the binomial coefficients in (3.5) and (3.6) are congruent to $2^{\gamma-1}$ modulo 2^γ. Thus, the exponent of c in (3.5) simplifies to $k2^\rho + \ell 2^\sigma + k\ell 2^{\gamma-1}$, while the exponent of c in (3.6) becomes $m2^\rho + n2^\sigma + mn2^{\gamma-1}$.

To prove necessity of the conditions, assume first that $\rho = \sigma = \gamma - 1$; since $k + \ell + k\ell$ and $m + n + mn$ are both odd, the highest power of 2 that divides the exponents of c in both (3.5) and (3.6) is exactly $2^{\gamma-1}$, so we are in case (i). If $\rho = \gamma - 1$ and $\sigma = \gamma$, then the exponents of c simplify to $k2^{\gamma-1}(1 + \ell)$ and $m2^{\gamma-1}(1 + n)$. At most one of ℓ and n

are even, so at least one of the two is divisible by 2^γ, and the other is divisible by at least $2^{\gamma-1}$, yielding either case (i) or (ii). If $\rho = \sigma = \gamma$, then the exponents simplify to $k\ell 2^{\gamma-1}$ and $mn2^{\gamma-1}$. We cannot have all of k, m, n, and ℓ odd, so at least one of the two exponents is divisible by 2^γ and the other by at least $2^{\gamma-1}$, again yielding cases (i) or (ii). Finally, consider the case where $\rho < \gamma - 1$; then the exponent in (3.5) simplifies to $2^\rho(k + \ell 2^{\sigma-\rho} + k\ell 2^{\gamma-1-\rho})$, and the one in (3.6) simplifies to $2^\rho(m + n2^{\sigma-\rho} + mn2^{\gamma-1-\rho})$. If $\sigma = \rho$, since at most one of $k+\ell$ and $m+n$ is even (as $kn-\ell m$ is odd), then at least one of the two exponents is divisible by 2^ρ and no higher power of 2, yielding case (iii). And if $\sigma > \rho$, since at most one of k and m is even, we again have that at most one of the two exponents is divisible by a power of 2 higher than 2^ρ, again yielding case (iii). Thus, the three conditions are necessary.

The sufficiency of (i) follows since $\alpha = \beta$, as noted above. For (ii), we simply note that $(\gamma, \gamma, \gamma; \gamma - 1, \gamma)$ is isomorphic to $(\gamma, \gamma, \gamma; \gamma, \gamma)$ by setting $k = \ell = n = 1$ and $m = 0$. Finally, if ρ is chosen with $\rho < \gamma - 1$, and σ and s are both greater than or equal to ρ and less than or equal to γ, then we want to show that $(\gamma, \gamma, \gamma; \rho, \sigma)$ is isomorphic to $(\gamma, \gamma, \gamma, \rho, s)$; this can be seen by setting $k = n = 1$, $\ell = 0$, and $m = 2^{s-\rho} - 2^{\sigma-\rho} - 2^{\gamma-1-\rho}(2^{s-\rho} - 2^{\sigma-\rho})$. □

Putting the previous three theorems together yields Theorem 1.1 in Section 1.

4. The number of nonisomorphic groups in $\mathfrak{G}_p(\alpha, \beta, \gamma)$

In this section we use our classification to give a formula for the number of groups in $\mathfrak{G}_p(\alpha, \beta, \gamma)$.

Recall that for fixed integers $\alpha \geq \beta \geq \gamma > 0$, we use the notation $\mathfrak{G}_p(\alpha, \beta, \gamma)$ to denote the set of nonisomorphic groups of class exactly two that have abelianization isomorphic to $C_{p^\alpha} \times C_{p^\beta}$ and commutator subgroup isomorphic to C_{p^γ}. We seek a formula for the cardinality of $\mathfrak{G}_p(\alpha, \beta, \gamma)$ in terms of α, β, and γ (the analysis below will show the number of elements does not depend on p).

Consider first the case where $\alpha = \beta$. If $p > 2$ or $\beta > \gamma$, Theorem 1.1 says that each group in the class we are interested in is isomorphic to one and only one of $(\alpha, \beta, \gamma; \rho, \gamma)$ with $0 \leq \rho \leq \gamma$, giving $\gamma + 1$ nonisomorphic groups. If $p = 2$ and $\beta = \gamma$, then all of these are pairwise nonisomorphic, with the exception of $(\alpha, \beta, \gamma; \gamma-1, \gamma)$ and $(\alpha, \beta, \gamma; \gamma, \gamma)$ which are isomorphic, giving only γ nonisomorphic groups. However, in this case there is a further group, namely $(\alpha, \beta, \gamma; \gamma - 1, \gamma - 1)$, which is not isomorphic to any of the γ groups already counted, so we

again obtain $\gamma+1$ nonisomorphic groups. Thus, when $\alpha=\beta$, the set $\mathfrak{G}_p(\alpha,\beta,\gamma)$ has exactly $\gamma+1$ elements.

Next, we consider the case where $\alpha-\beta>\gamma$. In addition to the $\gamma+1$ groups given by $(\alpha,\beta,\gamma;\rho,\gamma)$ with $0\leq\rho\leq\gamma$, we also have one group for each choice of a pair (ρ,σ) satisfying $0\leq\sigma<\rho\leq\gamma$; this gives $\binom{\gamma+1}{2}$ further groups. Adding the two totals, we obtain $(\gamma+1)+\frac{1}{2}\gamma(\gamma+1)$ elements in $\mathfrak{G}_p(\alpha,\beta,\gamma)$ (we will see below the reason for expressing the count in this manner).

Finally, we come to the case where $0<\alpha-\beta\leq\gamma$. There are $\gamma+1$ nonisomorphic groups corresponding to the quintuples $(\alpha,\beta,\gamma;\rho,\gamma)$ with $0\leq\rho\leq\gamma$. In addition, we also have $\alpha-\beta$ groups of the form $(\alpha,\beta,\gamma;\rho,\sigma)$ with $\sigma<\rho\leq\sigma+\alpha-\beta$ for each choice of σ that satisfies $0\leq\sigma\leq\gamma-(\alpha-\beta)$. Finally, for $\sigma=\gamma-(\alpha-\beta)+k$ with $0<k<\alpha-\beta$, we will have exactly $(\alpha-\beta)-k$ choices of ρ that satisfy $\rho\leq\gamma$ and $\sigma<\rho\leq\sigma+\alpha-\beta$, and each such choice of ρ yields a further nonisomorphic group. The total number is then q, where:

$$\begin{aligned}
q &= (\gamma+1)+(\alpha-\beta)(\gamma-(\alpha-\beta)+1)+((\alpha-\beta-1)+\cdots+1)\\
&= (\gamma+1)+(\alpha-\beta)(\gamma-(\alpha-\beta-1))+\frac{1}{2}(\alpha-\beta-1)(\alpha-\beta)\\
&= (\gamma+1)+\frac{1}{2}(\alpha-\beta)(2\gamma-2(\alpha-\beta-1)+(\alpha-\beta-1))\\
&= (\gamma+1)+\frac{1}{2}(\alpha-\beta)(2\gamma+1-(\alpha-\beta)).
\end{aligned}$$

Consider now the expression $(\gamma+1)+\frac{1}{2}\kappa(2\gamma+1-\kappa)$. If we set $\kappa=0$, we obtain the number of nonisomorphic groups when $\alpha=\beta$. If $\kappa=\gamma$, we obtain the number of nonisomorphic groups when $\gamma<\alpha-\beta$. And if $\kappa=\alpha-\beta$, we obtain the number of nonisomorphic groups when $0<\alpha-\beta<\gamma$. Therefore, we obtain the following result:

Theorem 4.1. *Let p be a prime, and let $\alpha\geq\beta\geq\gamma>0$ be integers. The cardinality of $\mathfrak{G}_p(\alpha,\beta,\gamma)$ is:*

$$|\mathfrak{G}_p(\alpha,\beta,\gamma)|=(\gamma+1)+\frac{1}{2}\min(\gamma,\alpha-\beta)(2\gamma+1-\min(\gamma,\alpha-\beta)).$$

Note that if $\gamma=0$, the expression in Theorem 4.1 evaluates to 1. This is, of course, the number of nonisomorphic groups that are central extensions of the trivial group by the abelian group $C_{p^\alpha}\times C_{p^\beta}$. Thus, if instead of considering only positive values of α,β,γ with $\alpha+\beta+\gamma=n$ we consider nonnegative values (that is, instead of considering only partitions of n of length exactly 3 we consider partitions of length at most 3), we obtain the number of nonisomorphic 2-generated groups of order p^n and class *at most* two (recall that a group is k-generated

n	1	2	3	4	5	6	7	8	9	10
$\lvert\mathcal{G}(2,p^n,2)\rvert$	0	0	2	3	5	9	13	18	26	34
$\lvert\mathcal{G}(2,p^n,1)\cup\mathcal{G}(2,p^n,2)\rvert$	1	2	4	6	8	13	17	23	31	40

n	11	12	13	14	15	16	17	18	19	20
$\lvert\mathcal{G}(2,p^n,2)\rvert$	44	58	72	89	111	134	160	193	227	266
$\lvert\mathcal{G}(2,p^n,1)\cup\mathcal{G}(2,p^n,2)\rvert$	50	65	79	97	119	143	169	203	237	277

n	21	22	23	24	25	26	27	28	29	30
$\lvert\mathcal{G}(2,p^n,2)\rvert$	312	361	415	479	545	619	703	792	888	998
$\lvert\mathcal{G}(2,p^n,1)\cup\mathcal{G}(2,p^n,2)\rvert$	323	373	427	492	558	633	717	807	903	1014

TABLE 1. Number of nonisomorphic 2-generated groups of order p^n and class at most 2.

if it can be generated by k elements, although it may be generated by fewer).

Let $\mathcal{G}(k, p^n, c)$ denote a set that contains one and only one representative from each isomorphism class of a k-generated group of order p^n and class exactly c. From the considerations above we have the following result:

Theorem 4.2. *Let p be a prime and n be a positive integer. The number of nonisomorphic 2-generated groups of order p^n and class exactly 2 is given by*

$$|\mathcal{G}(2,p^n,2)| = \sum_{\substack{\alpha+\beta+\gamma=n\\ \alpha\geq\beta\geq\gamma>0}} \left((\gamma+1)+\frac{1}{2}\min(\gamma,\alpha-\beta)\left(2\gamma+1-\min(\gamma,\alpha-\beta)\right)\right).$$

The number of nonisomorphic 2-generated groups of order p^n and class at most 2 is given by:

$$|\mathcal{G}(2,p^n,1)\cup\mathcal{G}(2,p^n,2)| = \sum_{\substack{\alpha+\beta+\gamma=n\\ \alpha\geq\beta\geq\gamma\geq0}} \left((\gamma+1)+\frac{1}{2}\min(\gamma,\alpha-\beta)\left(2\gamma+1-\min(\gamma,\alpha-\beta)\right)\right).$$

In Table 1 we give the number of nonisomorphic 2-generated groups of order p^n and class exactly 2, and of class at most 2, for $1 \leq n \leq 30$.

5. Conjugacy classes

The goal of this section is to prove Theorem 1.2. This theorem provides a formula for the number of conjugacy classes in terms of only n and γ. As an intermediate step to proving this result, we first express the conjugacy count in terms of α, β, and γ. This intermediate step also provides a count for each conjugacy class of each possible size. The following proposition provides such an analysis and is the key to proving Theorem 1.2.

Proposition 5.1. *Let G be any group in $\mathfrak{G}_p(\alpha,\beta,\gamma)$ and set*

$$\Phi_\alpha = \phi\left(p^{\alpha-(\gamma-\delta)}\right) \quad \text{and} \quad \Phi_\beta = \phi\left(p^{\beta-(\gamma-\delta)}\right),$$

where ϕ is Euler's Totient function and $1 \leq \delta \leq \gamma$. Then:

(i) Every conjugacy class of G has order p^i for some $i \in \{0,\ldots,\gamma\}$ and for each $i \in \{0,\ldots,\gamma\}$ there exists a conjugacy class of G of order p^i.

(ii) For each $\delta = 1,2,\ldots,\gamma$, the number of conjugacy classes of order p^δ in G is

$$\mathcal{C}_\delta(G) = p^{\gamma-\delta}\left(\Phi_\alpha + \Phi_\beta + \Phi_\alpha\Phi_\beta + \Phi_\alpha\sum_{i=\gamma-\delta+1}^{\beta-1}\phi(p^{\beta-i}) + \Phi_\beta\sum_{i=\gamma-\delta+1}^{\alpha-1}\phi(p^{\alpha-i})\right).$$

(iii) The number of conjugacy classes of G is

$$p^{\alpha+\beta-\gamma} + \sum_{\delta=1}^{\gamma}\mathcal{C}_\delta(G).$$

Every element of G can be expressed uniquely as $a^ib^j[a,b]^k$, where $0 \leq i < p^\alpha$, $0 \leq j < p^\beta$ and $0 \leq k < p^\gamma$. Let $g = a^ib^j[a,b]^k$ and $h = a^{i'}b^{j'}[a,b]^{k'}$ be arbitrary elements of G. Then

$$\begin{aligned} g^h &= (a^ib^j[a,b]^k)^{(a^{i'}b^{j'}[a,b]^{k'})} = (a^i)^{b^{j'}}(b^j)^{a^{i'}}[a,b]^k \\ &= a^ib^j[a,b]^{ij'-i'j}[a,b]^k = a^ib^j[a,b]^{ij'-i'j+k}. \end{aligned} \tag{5.2}$$

Hence the distinct elements conjugate to g are determined by the distinct values of $ij'-i'j$ modulo p^γ; in particular, there are at most p^γ elements conjugate to g.

The following lemma is used to proof of Proposition 5.1.

Lemma 5.3. *Let i, j, m, and n be integers, with $0 \leq m < n$, and let $\gcd(i,j) = d$. If $\gcd(d,n) = 1$ then there exist integers u and v such that $0 \leq u,v < n$ and $(iu - jv) \equiv m \pmod{n}$.*

Proof. Since $\gcd(i,j) = d$, there exist integers x and y such that $d = ix + jy = ix - j(-y)$. By hypothesis d and n are relatively prime. So there exist integers w and z such that $1 = wd + zn \equiv wd \pmod{n}$. Substituting d and multiplying by m in the previous congruence we obtain

$$m \equiv mw(ix - j(-y)) \equiv imwx - jmw(-y) \pmod{n}.$$

Set $u = mwx$ and $v = mw(-y)$ and the result holds. □

We apply Lemma 5.3 as follows: let g and h be arbitrary elements of the p-group G as above. Set p^ζ to be the largest common p-power factor of i, j, and p^γ (so $0 \le \zeta \le \gamma$). Write $i = \bar{\imath}p^\zeta$ and $j = \bar{\jmath}p^\zeta$, and let $d = \gcd(\bar{\imath}, \bar{\jmath})$. Note that either $\zeta = \gamma$, or $\gcd(d,p) = 1$. Then

$$g^h = a^i b^j [a,b]^{ij'-i'j}[a,b]^k = a^i b^j [a,b]^{p^\zeta(\bar{\imath}j'-i'\bar{\jmath})}[a,b]^k.$$

If $\zeta = \gamma$, this expression is always equal to g (since $\zeta = \gamma$ if and only if $g \in Z(G)$, this makes perfect sense). If $\zeta < \gamma$, then $\gcd(d, p^\gamma) = 1$ and applying Lemma 5.3 we have that for each value x, there exist i' and j' such that $\bar{\imath}j' - i'\bar{\jmath} \equiv x \pmod{p^\gamma}$. Therefore the expression $p^\zeta(\bar{\imath}j' - i'\bar{\jmath}) + k$ has $p^{\gamma-\zeta}$ distinct values modulo p^γ. Hence for any noncentral element $g = a^{\bar{\imath}p^\zeta} b^{\bar{\jmath}p^\zeta}[a,b]^k$ of G for which $1 \le \zeta < \gamma$, the number of its conjugates is $p^{\gamma-\zeta}$ and for a central element $g \in Z(G)$, the number of its conjugates is p^0.

From the analysis above, any conjugate of $g = a^i b^j [a,b]^k$ has the form

$$a^i b^j [a,b]^{k'},$$

where $k' = p^\zeta(\bar{\imath}j' - i'\bar{\jmath}) + k$. Suppose $h = a^i b^j [a,b]^{\hat{k}}$ and $k \not\equiv \hat{k} \pmod{p^\zeta}$. Then $p^\zeta(\bar{\imath}j' - i'\bar{\jmath}) + k \ne p^\zeta(\bar{\imath}j' - i'\bar{\jmath}) + \hat{k}$ and g and h are not conjugate. Hence for any given pair i, j, all elements of the form $a^i b^j [a,b]^k$ have conjugacy classes of the same size, and therefore there are p^ζ distinct values of k that give rise to distinct conjugacy classes.

Since the conjugacy classes of order one correspond to elements in the center of G, we need the following:

Proposition 5.4. *Let G be an element $\mathfrak{G}_p(\alpha,\beta,\gamma)$. Then $Z(G)$, the center of G, has order $p^{\alpha+\beta-\gamma}$.*

Proof. All elements in the center of G have the form $a^{ip^\gamma} b^{jp^\gamma}[a,b]^k$ where $1 \le i \le p^{\alpha-\gamma}$, $1 \le j \le p^{\gamma-\beta}$, and $1 \le k \le p^\gamma$. Hence there are $p^{\alpha-\gamma}p^{\beta-\gamma}p^\gamma = p^{\alpha+\beta-\gamma}$ different elements in the center. □

Proof of Proposition 5.1. (i). Each value of p^δ, $\delta = 0, 1, \ldots, \gamma$, is the size of a conjugacy class of G: setting $\zeta = \gamma - \delta$, the conjugates of a^{p^ζ} have the form $a^{p^\zeta}[a,b]^{p^\zeta j'}$ for some j', and there are exactly $p^{\gamma-\zeta} = p^\delta$

distinct values of $p^\zeta j'$ modulo p^γ; thus, the conjugacy class of a^{p^ζ} has exactly p^δ elements. So each of the given values occurs as the size of a conjugacy class; and the discussion above shows that every conjugacy class is of size p^δ for some δ, $0 \leq \delta \leq \gamma$.

(ii). To count the number of conjugacy classes of order p^δ, we set $\zeta = \gamma - \delta$. Then for each i, j pair such that the greatest common p-power divisor is p^ζ, there are $p^\zeta = p^{\gamma-\delta}$ distinct values of k that form distinct conjugacy classes. This observation reduces the problem to determining all i, j pairs that give rise to elements with conjugacy classes of order p^δ. We break this analysis into five pairwise mutually exclusive cases.

Case 1. If $i = \bar{\imath}p^\zeta$ and $j = 0$. There are $p^{\alpha-\zeta}$ multiples of p^ζ between 1 and p^α; $\bar{\imath}$ needs to be a number between 1 and $p^{\gamma-\zeta}$ that is relatively prime to p; hence, there are $\phi(p^{\alpha-\zeta}) = \phi(p^{\alpha-\gamma+\delta}) = \Phi_\alpha$ possible values for $\bar{\imath}$.

Case 2. If $i = 0$ and $j = \bar{\jmath}p^\zeta$. The analysis follows as in Case 1, so there are Φ_β possible values for $\bar{\jmath}$.

Case 3. If $i = \bar{\imath}p^\zeta$, $j = \bar{\jmath}p^\zeta$, where $p \nmid \bar{\imath}$, and $p \nmid \bar{\jmath}$. Since the largest p-power divisor of both i and j is p^ζ, the number of possible $\bar{\imath}$ and $\bar{\jmath}$ pairs is $\phi(p^{\alpha-(\gamma-\delta)})\phi(p^{\beta-(\gamma-\delta)}) = \Phi_\alpha\Phi_\beta$, by our analysis from Case 1 and 2.

Case 4. If $i = \bar{\imath}p^\zeta$, $j = \bar{\jmath}p^\zeta$, where $p \nmid \bar{\imath}$, and $p \mid \bar{\jmath}$. In this case p divides $\bar{\jmath}$ and we have to account for all p-powers from $\zeta + 1$ to $\beta - 1$. Once this largest p-power that divides j is fixed, the argument for counting the number of conjugacy classes of size p^δ follows from Case 3. Hence we sum over the possible p-powers to obtain

$$\sum_{i=\zeta+1}^{\beta-1} \phi(p^{\alpha-\zeta})\phi(p^{\beta-i}) = \phi(p^{\alpha-\zeta})\sum_{i=\zeta+1}^{\beta-1} \phi(p^{\beta-i}) = \Phi_\alpha \sum_{i=\gamma-\delta+1}^{\beta-1} \phi(p^{\beta-i}).$$

Case 5. If $i = \bar{\imath}p^\zeta$, $j = \bar{\jmath}p^\zeta$, where $p \mid \bar{\imath}$, and $p \nmid \bar{\jmath}$, the analysis follows as in Case 4 to yield

$$\sum_{i=\zeta+1}^{\alpha-i} \phi(p^{\alpha-i})\phi(p^{\beta-\zeta}) = \phi(p^{\beta-\zeta})\sum_{i=\zeta+1}^{\alpha-1} \phi(p^{\alpha-i}) = \Phi_\beta \sum_{i=\gamma-\delta+1}^{\alpha-1} \phi(p^{\alpha-i}).$$

The five cases now correspond to the five summands on the right hand side of the expression for $\mathcal{C}_\delta(G)$ in the statement of Proposition 5.1.

(iii). The total number of conjugacy classes is the sum of the number of conjugacy classes of each order. By part *(i)* the orders of the conjugacy classes are exactly p^δ for $\delta = 0, 1, \ldots, \gamma$. The elements in the center of G correspond to those conjugacy classes with size $p^0 = 1$, and

we sum over $\delta = 1, \ldots, \gamma$ for the conjugacy classes of size p^δ determined in *(ii)* to obtain the count. □

The following lemma and corollary are used to simplify the formula from Proposition 5.1 (iii).

Lemma 5.5. *Let $a > b > j > 0$ be integers and set $m = a - b$. Then:*

$$\sum_{i=j}^{a-1} \phi(p^{a-i}) = p^m \left(\sum_{i=j}^{b-1} \phi(p^{b-i}) + p^{-m} \sum_{i=1}^{m} \phi(p^i) \right), \tag{5.6}$$

$$\sum_{i=j}^{b-1} \phi(p^{b-i}) = p^{-m} \left(\sum_{i=j}^{a-1} \phi(p^{a-i}) - \sum_{i=1}^{m} \phi(p^i) \right), \tag{5.7}$$

$$\sum_{i=1}^{m} \phi(p^i) = p^m - 1. \tag{5.8}$$

Proof. These follow immediately using $\phi(p^m) = (p-1)p^{m-1}$ for all $m \geq 1$ and applying the identity

$$\sum_{j=0}^{n} p^i = \frac{p^{n+1} - 1}{p - 1}$$

to show (5.8). □

Corollary 5.9. *Let G and H be two groups in $\mathcal{G}(2, p^n, 2)$ whose derived subgroups have order p^γ. Then G and H have the same number of conjugacy classes.*

Proof. Fix n and let (α, β, γ) and $(\alpha', \beta', \gamma)$ be two positive partitions of n. If $\alpha = \alpha'$ then $\beta = \beta'$ then both G and H are elements of $\mathfrak{G}_p(\alpha, \beta, \gamma)$, hence they have the same number of conjugacy classes by Proposition 5.1. Suppose then that $\alpha \neq \alpha'$, and without loss generality take $\alpha > \alpha'$. Then $\alpha - \alpha' = \beta' - \beta = \mu$. Since $\alpha + \beta = \alpha' + \beta'$, the centers of G and H have the same orders by Proposition 5.4. Hence it suffices to show that $\mathcal{C}_\delta(G) = \mathcal{C}_\delta(H)$ for $\delta = 1, \ldots, \gamma$. Since $\alpha = \alpha' + \mu$ and $\beta = \beta' - \mu$, we have

$$\Phi_\alpha = \phi(p^{\alpha-(\gamma-\delta)}) = (p-1)p^{\alpha'+\mu-(\gamma-\delta)-1} = (p-1)p^{\alpha'-(\gamma-\delta)-1}p^\mu = \Phi_{\alpha'}p^\mu$$

and similarly we obtain $\Phi_\beta p^\mu = \Phi_{\beta'}$. Thus,

$$\Phi_\alpha \Phi_\beta = \Phi_{\alpha'} p^\mu \Phi_{\beta'} p^{-\mu} = \Phi_{\alpha'} \Phi_{\beta'}.$$

We complete the proof by showing that the sums of the remaining four terms of $\mathcal{C}_\delta(G)$ and $\mathcal{C}_\delta(H)$ are equal. We express the sum

$$\Phi_\alpha + \Phi_\beta + \Phi_\alpha \sum_{i=\gamma-\delta+1}^{\beta-1} \phi(p^{\beta-i}) + \Phi_\beta \sum_{i=\gamma-\delta+1}^{\alpha-1} \phi(p^{\alpha-i})$$

in terms of α' and β' using (5.6) and (5.7) to obtain

$$\begin{aligned}\Phi_{\alpha'}p^\mu + \Phi_{\beta'}p^{-\mu} + \Phi_{\alpha'}p^\mu \left(p^{-\mu} \left(\sum_{i=\gamma-\delta+1}^{\beta'-1} \phi(p^{\beta'-i}) - \sum_{i=1}^{\mu} \phi(p^i) \right) \right) \\ + \Phi_{\beta'}p^{-\mu} \left(p^\mu \left(\sum_{i=\gamma-\delta+1}^{\alpha'-1} \phi(p^{\alpha'-i}) + p^{-\mu} \sum_{i=1}^{\mu} \phi(p^i) \right) \right).\end{aligned}$$

Simplifying, we get

$$\begin{aligned}&\Phi_{\alpha'}p^\mu + \Phi_{\beta'}p^{-\mu} + \Phi_{\alpha'} \sum_{i=\gamma-\delta+1}^{\beta'-1} \phi(p^{\beta'-i}) - \Phi_{\alpha'} \sum_{i=1}^{\mu} \phi(p^i) \\ &\quad + \Phi_{\beta'} \sum_{i=\gamma-\delta+1}^{\alpha'-1} \phi(p^{\alpha'-i}) + \Phi_{\beta'}p^{-\mu} \sum_{i=1}^{\mu} \phi(p^i) \\ &= \Phi_{\alpha'} \sum_{i=\gamma-\delta+1}^{\beta'-1} \phi(p^{\beta'-i}) + \Phi_{\beta'} \sum_{i=\gamma-\delta+1}^{\alpha'-1} \phi^{\alpha'-i} \\ &\qquad + \Phi_{\alpha'} \left(p^\mu - \sum_{i=1}^{\mu} \phi(p^i) \right) + \Phi_{\beta'}p^{-\mu} \left(1 + \sum_{i=1}^{\mu} \phi(p^i) \right) \\ &= \Phi_{\alpha'} + \Phi_{\beta'} + \Phi_{\alpha'} \sum_{i=\gamma-\delta+1}^{\beta'-1} \phi(p^{\beta'-i}) + \Phi_{\beta'} \sum_{i=\gamma-\delta+1}^{\alpha'-1} \phi(p^{\alpha'-i}),\end{aligned}$$

where the last equality is obtained using (5.8). Hence $\mathcal{C}_\delta(G) = \mathcal{C}_\delta(H)$ as desired. □

Proof of Theorem 1.2. Let G be a 2-generated p-group of class exactly 2 and order p^n, and suppose that G' has order p^γ. By Corollary 5.9, to count the number of conjugacy classes we may, without loss of generality, assume that $G \in \mathfrak{G}_p(n-2\gamma, \gamma, \gamma)$. Set $\mu = n - 3\gamma$. Then $\Phi_\alpha = \phi(p^{\mu+\delta})$, $\Phi_\beta = \phi(p^\delta)$,

$$\sum_{i=\gamma-\delta+1}^{\alpha-1} \phi(p^{\alpha-i}) = \sum_{i=1}^{\mu+\delta-1} \phi(p^i), \quad \text{and} \quad \sum_{i=\gamma-\delta+1}^{\beta-1} \phi(p^{\beta-i}) = \sum_{i=1}^{\delta-1} \phi(p^i).$$

Using (5.8) to simplify the equations above we obtain:

$$\begin{aligned}
\mathcal{C}_\delta(G) &= p^{\gamma-\delta}\Big(\phi(p^{\mu+\delta})+\phi(p^\delta)+\phi(p^{\mu+\delta})\phi(p^\delta)\Big)\\
&\qquad + p^{\gamma-\delta}\Big(\phi(p^{\mu+\delta})(p^{\delta-1}-1)+\phi(p^\delta)(p^{\mu+\delta-1}-1)\Big)\\
&= p^{\gamma-\delta}\Big(\phi(p^{\mu+\delta})\phi(p^\delta)+\phi(p^{\mu+\delta})p^{\delta-1}+\phi(p^\delta)p^{\mu+\delta-1}\Big)\\
&= p^{\gamma-\delta}\left(\phi(p^{\mu+\delta})\phi(p^\delta)+\phi(p^\delta)p^{\mu+\delta-1}+\phi(p^\delta)p^{\mu+\delta-1}\right)\\
&= p^{\gamma-\delta}\phi(p^\delta)\Big(\phi(p^{\mu+\delta})+p^{\mu+\delta-1}+p^{\mu+\delta-1}\Big)\\
&= p^{\gamma-\delta}\phi(p^\delta)\Big((p-1)p^{\mu+\delta-1}+p^{\mu+\delta-1}+p^{\mu+\delta-1}\Big)\\
&= p^{\gamma-\delta}\phi(p^\delta)p^{\mu+\delta-1}(p+1)=p^{\gamma+\mu-1}\phi(p^\delta)(p+1)\\
&= p^{n-2\gamma-1}\phi(p^\delta)(p+1).
\end{aligned}$$

Summing over δ and adding the order of the center of G, we obtain

$$\begin{aligned}
\sum_{\delta=0}^{\gamma}\mathcal{C}_\delta(G) &= p^{n-2\gamma}+p^{n-2\gamma-1}(p+1)\sum_{\delta=1}^{\gamma}\phi(p^\delta)\\
&= p^{n-2\gamma}+p^{n-2\gamma-1}(p+1)(p^\gamma-1)\\
&= p^{n-2\gamma}+p^{n-2\gamma-1}(p^{\gamma+1}-p+p^\gamma-1)\\
&= p^{n-2\gamma}+p^{n-\gamma}-p^{n-2\gamma}+p^{n-\gamma-1}-p^{n-2\gamma-1}\\
&= p^{n-\gamma}+p^{n-\gamma-1}-p^{n-2\gamma-1}\\
&= p^{n-\gamma}\left(1+p^{-1}-p^{-(\gamma+1)}\right),
\end{aligned}$$

as claimed. □

We conclude this section with a direct consequence of Corollary 5.9.

Corollary 5.10. *Let (α,β,γ) and (α',β',γ') be two partitions of n of length 3, and let $G\in\mathfrak{G}_p(\alpha,\beta,\gamma)$, $H\in\mathfrak{G}_p(\alpha',\beta',\gamma')$. Then G and H have the same number of conjugacy classes if and only if $\gamma=\gamma'$. In particular, the set*

$$\big\{k \;\big|\; \text{there exists } G\in\mathcal{G}(2,p^n,2) \text{ with } k \text{ conjugacy classes}\big\}$$

has exactly $\lfloor n/3\rfloor$ elements.

Proof. If $\gamma=\gamma'$, then the number of conjugacy classes are equal. Conversely, if the number of conjugacy classes are equal, then

$$p^{n-\gamma}+p^{n-\gamma-1}-p^{n-1}=p^{n-\gamma'}+p^{n-\gamma'-1}-p^{n-1}.$$

Since $0<\gamma<n$, the largest power of p that divides the left hand side is $p^{n-\gamma-1}$, and the highest power of p that divides the right hand side

is $p^{n-\gamma'-1}$, so $\gamma = \gamma'$. Since $0 < \gamma \leq \lfloor n/3 \rfloor$ must hold, there are exactly $\lfloor n/3 \rfloor$ possible values of γ. □

6. Connections to previously published descriptions

As mentioned in the introduction, the attempts to classify the 2-generated p-groups of class 2 that appeared in [1, 5] were incomplete, and in the case of $p = 2$, two families that were claimed to be disjoint are not. There is also overlap between our Theorem 1.1 and the results in [8], where the two agree.

In this final section, we connect our description with those given in the works mentioned above; this is particularly important for the classifications in [1, 5], since the lists given there have been used in other articles, e.g., [2, 6, 7].

We begin with the work of Miech, since it is closest to our description. Miech considers 2-generated nonabelian p-groups with cyclic commutator subgroup. Miech uses x, y, z where we use a, b, c, and uses a, b, c where we use α, β, γ, but otherwise his approach is essentially the same as ours, with the added complications necessitated by not assuming the groups are of class two. The three parameters, a, b, c describe the same quantities as our α, β, γ: $p^a \geq p^b$ are the abelian invariants of the abelianization of the group, and p^c is the order of the commutator subgroup. Because of the more general situation considered in [8], only the inequalities $a \geq b$, $a \geq c$ may be taken a priori.

Once these three quantities are fixed, Miech parameterizes the groups with 4-tuples, $[Rp^r, Sp^s, p^m, p^n]$, that describe the groups generated by x, y, and z and with relations: $[y, x] = z$, $z^{p^c} = 1$, $x^{p^a} = z^{Rp^r}$, $y^{p^b} = z^{Sp^s}$, $[z, x] = p^m$, $[z, y] = p^n$, where the seven inequalities $r + m \geq c$, $r + n \geq c$, $s + n \geq c$, $1 \leq m \leq c$, $1 \leq n \leq c$, $0 \leq r \leq c$, and $0 \leq s \leq c$ hold, and such that $p^b \equiv Sp^{m+s} \pmod{p^c}$ and $\gcd(RS, p) = 1$. Because the groups considered include groups of class three, one cannot restrict attention to r and s in general, as we did, hence the need to keep track of the parameters R and S. The groups then break down into 21 families that are described in eight theorems, depending on the relative values of b and c, and of $a - b$ and c; these families, like ours, specify inequalities between the parameters R, S, r, s, m, and n. Only those families in which $m = n = c$ is possible correspond to groups of class two; in those, the inequalities always force $R = S = 1$, as we expect. The parameters r and s then correspond to our ρ and σ, respectively. The only other difference is that rather than use p^c as the parameter when $x^{p^a} = e$ or $y^{p^b} = e$, Miech sometimes sets $Rp^r = 0$ or $Sp^s = 0$,

respectively, rather than setting $R = 1$ and $r = c$, or $S = 1$ and $s = c$, respectively, as we see below.

Our four families (Families 1(a)–1(c) and 2 from Theorem 1.1) fall into seven of the families described by Miech; setting $m = n = c$ and simplifying the ancillary inequalities and conditions on the parameters to account for this, they are:

(I) $[p^r, 0, 0, 0]$ when $b \geq c$ and $a - b > c$ [8, Thm 2(a)], which are included in our Family 1(a).

(II) $[p^r, p^s, 0, 0]$ when $b \geq c$, $a - b > c$, and $0 \leq s < r \leq c$ [8, Thm 2(c)], which fall either in our Family 1(b) or in 1(c).

(III) $[0, p^s, 0, 0]$ when $a > b \geq c$, $a - b \leq c$, and $s < c - (a - b)$ [8, Thm 3(b)], which are included in our Family 1(b).

(IV) $[p^r, 0, 0, 0]$ when $a > b \geq c$, $a - b \leq c$, and $r \leq c$ [8, Thm 3(c)]; these are included in our Family 1(a).

(V) $[p^r, p^s, 0, 0]$ when $a > b \geq c$, $a - b \leq c$, $s < r < s + a - b + 1$, and $s < c$ [8, Thm 3(f)], which are in our Family 1(c).

(VI) $[0, p^s, 0, 0]$ when $a > b \geq c$, $a - b \leq c$, $s \leq c - (a - b)$ [8, Thm 3(h)], which are in our Family 1(b).

(VII) $[0, p^s, 0, 0]$ when $a = b$ and $0 \leq s \leq c$ [8, Thm 5(b)]; these correspond to our Family 2, with the roles of a and b reversed.

None of the other families or possible values of the parameters given by Miech correspond to groups of class 2.

Moving now to the descriptions found in [1, 5], the groups fall into four families, one of which can only occur in the case $p = 2$. The notation in these papers is very hard to reconcile with our own, since they use both a, b, c and α, β, γ but for purposes very different from ours. We replace these variables in the descriptions that follow with x, y, z for the elements, and t, u, v, w for the parameters at play. The descriptions below for $p > 2$ appear in [1, Thm 2.4], and in [5, Thm 2.5] for $p = 2$.

(i) $\big(\langle z\rangle \times \langle x\rangle\big) \rtimes \langle y\rangle$, with $[x, y] = z$, $|z| = p^t$, $|y| = p^u$, and $t \geq u \geq v \geq 1$. By setting $a = x$, $b = y$, and $c = z$, we see that these groups are of type $(t, u, v; v, v)$.

(ii) $\langle x\rangle \rtimes \langle y\rangle$, with $[x, y] = x^{p^{t-v}}$, $|x| = p^t$, $|y| = p^u$, $|[x, y]| = p^v$, $t \geq u$, $t \geq 2v$, $u \geq v \geq 1$; when $p = 2$, we also place the restriction $t + u > 3$. If $t - v \geq u$, then the groups are of type $(t - v, u, v; v, 0)$, which can be seen by setting $a = x$, $b = y$, and $c = x^{p^{t-v}}$; if $t - v < u$, then we get $(u, t - v, v; 0, v)$ by setting $a = y$, $b = x$, and $c = x^{p^{t-v}}$.

(iii) $\big(\langle z\rangle \times \langle x\rangle\big) \rtimes \langle y\rangle$, with $[x, y] = x^{p^{t-v}} z$, $[z, y] = x^{-p^{2(t-v)}} z^{-p^{t-v}}$, $|x| = p^t$, $|y| = p^u$, $|z| = p^w$, $|[x, y]| = p^v$, $v > w \geq 1$, $t + w \geq 2v$,

$u \geq v$; if p is odd we also require $t \geq u$. If $t + w - v \geq u$, then we let $a = x$, $b = y$, and $c = x^{p^{t-v}} z$ and we obtain that the group is of type $(t + w - v, u, v; w, v)$. If $t + w - v < u$, we reverse the choice of a and b and get that the group is of type $(u, t + w - v, v; v, w)$.

(iv) $\big(\langle z\rangle \times \langle x\rangle\big)\langle y\rangle$, with $|x| = |y| = 2^{v+1}$, $|z| = 2^{v-1}$, $[x, y] = x^2 z$, $[z, y] = x^{-4} y^{-2}$, $|[x, y]| = 2^v$, $x^{2^v} = y^{2^v}$, $v > 0$. These groups have no counterparts for odd prime, and they correspond to our family 3(b), groups of type $(v, v, v; v - 1, v - 1)$, with $a = x$, $b = y$, and $c = x^2 z$.

As is clear, these families miss all the groups in family 1(c). The smallest group that does not occur in these families is group $(4, 2, 2; 1, 0)$, of order p^8; it was the realization by the first author that this group (with $p = 2$) was not included in any of the families (i)–(iv) above that led to our Theorem 1.1.

In addition to this omission, when $p = 2$ the four families are not disjoint. If we let $u = v = t - 1 = w + 1$ in family (iii) above, the values lead to the group $(v, v, v; v - 1, v)$, which is isomorphic to the group $(v, v, v; v, v)$ that occurs in family (i). The condition $t + u > 3$ in family (ii) prevents this group from occurring for a third time when $v = 1$. This overlap shows up inadvertently in [7, Thm 8.1(d)].

Acknowledgments

The second author was supported by a grant from the Research Competitiveness Fund of the Louisiana Board of Regents. The third author began this research while visiting the National University of Ireland, Galway; he thanks Graham Ellis for his hospitality and stimulating conversations on computing with group extensions. Funding for the third author's visit to NUI Galway was made possible by the De Brún Centre for Computational Algebra. Many thanks go to Primož Moravec and Russell Blyth for their suggestions and comments on this paper.

References

[1] Michael R. Bacon and Luise-Charlotte Kappe, *The nonabelian tensor square of a 2-generator p-group of class* 2, Arch. Math. (Basel) **61** (1993), no. 6, 508–516. MR 1254062 (**95h:**20041)

[2] ———, *On capable p-groups of nilpotency class two*, Illinois J. Math. **47** (2003), no. 1-2, 49–62. Special issue in honor of Reinhold Baer (1902–1979). MR 2031305 (**2004j:**20036)

[3] B. Huppert, *Endliche Gruppen. I*, Die Grundlehren der Mathematischen Wissenschaften, Band 134, Springer-Verlag, Berlin, 1967. MR 0224703 (37 #302)

[4] A. Jaikin-Zapirain, *On the abundance of finite p-groups*, J. Group Theory **3** (2000), no. 3, 225–231. MR 1772019 (**2001j:**20029)

[5] Luise-Charlotte Kappe, Matthew P. Visscher, and Nor Haniza Sarmin, *Two-generator two-groups of class two and their nonabelian tensor squares*, Glasg. Math. J. **41** (1999), no. 3, 417–430. MR 1720422 (**2000k:**20037)

[6] Arturo Magidin, *Capability of nilpotent products of cyclic groups*, J. Group Theory **8** (2005), no. 4, 431–452. MR 2152690 (**2006c:**20073)

[7] ———, *Capable 2-generator 2-groups of class two*, Comm. Algebra **34** (2006), no. 6, 2183–2193. MR 2236108 (**2007b:**20037)

[8] R. J. Miech, *On p-groups with a cyclic commutator subgroup*, J. Austral. Math. Soc. **20** (1975), no. 2, 178–198. MR 0404441 (53 #8243)

[9] D. Ya. Trebenko, *Nilpotent groups of class two with two generators*, Current analysis and its applications (Russian), 1989, pp. 201–208, 228. MR 1054426 (**91f:**20044)

[10] Chistopher Voll, *Enumerating finite class-2-nilpotent groups on 2 generators*, Comptes Rendus Mathmatique **347** (2009), no. 23-24, 1347–1350. MR 2588779

School of Mathematical Sciences, Universiti Sains Malaysia, 11800 USM Penang Malaysia

Mathematics Department, P.O. Box 41010, University of Louisiana at Lafayette, Lafayette LA 70504-1010 USA

E-mail address: magidin@member.ams.org

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