Algebras and Representation Theory
https://doi.org/10.1007/s10468-022-10182-x

On Group Invariants Determined by Modular Group Algebras: Even Versus Odd Characteristic

Diego García-Lucas[1] · Ángel del Río[1] · Mima Stanojkovski[2]

Received: 26 September 2022 / Accepted: 20 October 2022

Abstract
Let p be a an odd prime and let G be a finite p-group with cyclic commutator subgroup G'. We prove that the exponent and the abelianization of the centralizer of G' in G are determined by the group algebra of G over any field of characteristic p. If, additionally, G is 2-generated then almost all the numerical invariants determining G up to isomorphism are determined by the same group algebras; as a consequence the isomorphism type of the centralizer of G' is determined. These claims are known to be false for $p = 2$.

Keywords Finite p-groups · Modular group algebra · Invariants · Modular isomorphism problem

Mathematics Subject Classification (2010) 20D15

1 Introduction

Let G be a group, R a commutative ring and let RG denote the group ring of G with coefficients in R. The problem of describing how much information about the group G is carried by the group algebra RG has a long tradition in mathematics, with applications in particular to the representation of groups and in general to group theory; cf. [7, 8, 10, 11, 18, 31–33, 39, 42, 43, 48]. The last question can be rewritten more compactly as:

Which group invariants of G are algebra invariants of RG?

Presented by: Andrew Mathas

✉ Ángel del Río
adelrio@um.es

Diego García-Lucas
diego.garcial@um.es

Mima Stanojkovski
mima.stanojkovski@unitn.it

[1] Departamento de Matemáticas, Universidad de Murcia, Murcia, Spain

[2] Dipartimento di Matematica, University of Trento, Via Sommarive 14, 38123, Povo TN, Italy

Published online: 21 December 2022

By a *group invariant* of G we understand a feature of G that is shared with any group isomorphic to G while an *algebra invariant* is a feature that is shared with any group H with the property that RG and RH are isomorphic as R-algebras. For instance, the cardinality of G can be expressed as the R-rank of RG and is thus an algebra invariant of RG. Moreover, the group G is abelian if and only if RG is a commutative ring, i.e. the property of being abelian is an algebra invariant of RG. The ultimate version of the above question is the *Isomorphism Problem* which asks for the determination of pairs (G, R) for which the isomorphism type of G is an algebra invariant of RG:

> **Isomorphism Problem for group algebras**: Given a commutative ring R and two groups G and H, does RG and RH being isomorphic as R-algebras imply that the groups G and H are isomorphic? In symbols,
>
> $$RG \cong RH \implies G \cong H\ ?$$

The answer to this question is a function of the ring R: for instance, it is easily shown that any two non-isomorphic finite abelian groups of the same order have isomorphic group rings with complex coefficients. However, by a seminal result of G. Higman [18], if G and H are non-isomorphic abelian groups then $\mathbb{Z}G'$ and $\mathbb{Z}H$ are not isomorphic. More surprisingly, there even exist two non-isomorphic finite metabelian groups G and H such that kG and kH are isomorphic for every field k [12]. Nonetheless, the Isomorphism Problem has a positive solution for $R = \mathbb{Z}$ and G and H metabelian [48]. This extends Higman's result for abelian groups [18] and has been followed by positive results for more families of groups, such as nilpotent groups [35] and supersolvable groups [24]. These early results yielded to strong expectations that the Isomorphism Problem for integral group rings ($R = \mathbb{Z}$ and G, H finite) would have a positive solution until Hertweck's construction of two non-isomorphic finite groups with isomorphic integral group rings [17]. Among the classical variations of the Isomorphism Problem, the one that remained unanswered the longest deals with the case where R is a field of positive characteristic p and G and H are p-groups, formally:

> **Modular Isomorphism Problem**: Given a field k of characteristic $p > 0$ and two finite p-groups G and H, are kG and kH isomorphic as k-algebras if and only if G and H are isomorphic as groups?

The contributions to this problem are numerous, including positive solutions for specific families of p-groups and the uncovering of algebra invariants in this context; cf. [1–4, 6, 13–15, 19, 20, 22, 25, 27–30, 34, 36, 38, 40, 41, 45–47, 49]. The first negative solution to the Modular Isomorphism Problem was given recently in the form of a series of pairs of non isomorphic 2-groups $G_{m,n}$ and $H_{m,n}$ which are 2-generated and have cyclic commutator subgroup satisfying $kG_{m,n} \cong kH_{m,n}$ for every $n > m > 2$ and every field k of characteristic 2 [16]. However, if p is odd then the Modular Isomorphism Problem is still open, even in the class of 2-generated groups with cyclic commutator subgroup. The aim of this paper is to investigate this class of groups from the point of view of algebra invariants and to demonstrate a substantial difference between the cases $p = 2$ and $p > 2$ within this class. For example, if G' denotes the commutator subgroup of G, our first result shows that both the exponent of $\mathrm{C}_G(G')$ and the isomorphism types of $\mathrm{C}_G(G')/G'$ and $\mathrm{C}_G(G')/\mathrm{C}_G(G')'$ are algebra invariants of kG provided G' is cyclic and p is odd; cf. Theorem A. Note that, on the contrary, for every choice of $n > m > 2$, the groups $G_{m,n}$ and $H_{m,n}$ satisfy neither of the points (1)-(2)-(3) from Theorem A.

Theorem A *Let k be a field of odd characteristic p and let G and H be finite p-groups. If G' is cyclic and $kG \cong kH$ then the following hold:*

(1) $\mathrm{C}_G(G')$ *and* $\mathrm{C}_H(H')$ *have the same exponent.*
(2) $\mathrm{C}_G(G')/G' \cong \mathrm{C}_H(H')/H'$.
(3) $\mathrm{C}_G(G')/\mathrm{C}_G(G')' \cong \mathrm{C}_H(H')/\mathrm{C}_H(H')'$.

Our next results concern 2-generated p-groups with cyclic commutator subgroup. In order to present them we introduce some numerical invariants of these groups. Since the Modular Isomorphism Problem has a positive solution for abelian groups [13] we only consider non-abelian groups. To this end, let G be a 2-generated non-abelian p-group, that is, G' is non-trivial and G is generated by exactly 2 elements. A *basis* of G is then a pair (b_1, b_2) of elements of G such that

$$G/G' = \langle b_1 G' \rangle \times \langle b_2 G' \rangle \text{ and } |b_2 G'| \text{ divides } |b_1 G'|.$$

Moreover, we define

$$\mathrm{O}(G) = \min{}_{\mathrm{lex}}\{(|b_1 \mathrm{C}_G(G')|, |b_2 \mathrm{C}_G(G')|, -|b_1|, -|b_2|) : (b_1, b_2) \text{ is a basis of } G\},$$

where $\min_{\mathrm{lex}}$ refers to the minimum with respect to the lexicographic order. The following result implies that if G' is cyclic then so is H' and $\mathrm{O}(G)$ is an algebra invariant of kG.

Theorem B *Let k be a field of odd characteristic p and let G and H be finite p-groups with $kG \cong kH$. If G is 2-generated and G' is cyclic, then H is 2-generated, H' is cyclic and* $\mathrm{O}(G) = \mathrm{O}(H)$.

Observe that the hypothesis that p is odd in Theorem B is necessary because

$$\mathrm{O}(G_{m,n}) = (2, 2, -2^n, -2^m) \neq (2, 1, -2^n, -2^m) = \mathrm{O}(H_{m,n}).$$

This shows again a clear contrast between odd and even characteristic.

For any p-group G that is 2-generated and for which G' is cyclic, the vector $\mathrm{O}(G)$ can essentially be extended to a vector $\mathrm{inv}(G) = (p, m, n_1, n_2, \sigma_1, \sigma_2, o_1, o_2, o_1', o_2', u_1, u_2)$ of numerical invariants characterizing the isomorphism class of G; cf. Section 3 and [5]. It is well known that the first four entries p, m, n_1 and n_2 of $\mathrm{inv}(G)$ are algebra invariants of kG. However, the sixth entry is not determined by the modular group algebra because $\mathrm{inv}(G_{m,n}) = (2, 2, n, m, -1, -1, 0, 0, 0, 0, 1, 1)$ is different from $\mathrm{inv}(H_{m,n}) = (2, 2, n, m, -1, 1, 0, 0, 0, 0, 1, 1)$. Note that, for $p > 2$, one always has $\sigma_1 = \sigma_2 = 1$ and therefore the counterexample from [16] does not have a direct equivalent in odd characteristic. We will see that Theorem B is actually equivalent to the following.

Theorem C *Let k be a field of odd characteristic p and let G be a finite non-abelian p-group. If G is 2-generated with G' cyclic then all but the last 2 entries of* $\mathrm{inv}(G)$ *are algebra invariants of kG.*

In other words, Theorem C ensures that, for $p > 2$, the first 10 entries of $\mathrm{inv}(G)$ are determined by the modular group algebra kG of G over any field k of characteristic p. Unfortunately we have not been able to decide whether the last two entries of $\mathrm{inv}(G)$ are algebra invariants of kG. The smallest groups for which Theorem C does not solve the Modular Isomorphism Problem occur for $(n_1, n_2, m, o_1, o_2, o_1', o_2') = (3, 2, 2, 0, 1, 1, 1)$, in which case $u_2 = 1$ and $u_1 \in \{1, \dots, p-1\}$. That is, the last parameters yield $p - 1$ non-isomorphic 2-generated p-groups with cyclic commutator subgroup. In a paper in preparation, we develop new techniques (different from those presented in this paper) to prove that, for this special case and many others, u_1 is actually also an algebra invariant of kG. Theorem C enables us, however, to improve Theorem A in the 2-generated case by showing that the isomorphism type of $\mathrm{C}_G(G')$ is an algebra invariant of kG:

Corollary D *Let k be a field of odd characteristic p and let G be a finite 2-generated p-group with G' cyclic. Then the isomorphism type of $\mathrm{C}_G(G')$ is an algebra invariant of kG.*

The following corollary also follows from Theorem C (see Section 2 for the definition of the type invariants of a p-group).

Corollary E *Let k be a field of odd characteristic p and let G be a finite 2-generated p-group with G' cyclic. Then the type invariants of G are algebra invariants of kG.*

The paper is organized as follows. In Section 2 we establish the notation, recall some known facts about the Modular Isomorphism Problem and prove a key lemma which we refer to as the Transfer Lemma (Lemma 2.6). In Section 3 we recall the classification of finite 2-generated p-groups with cyclic commutator subgroup from [5] in the specific case where $p > 2$. Additionally, we prove a series of results about these groups which will be used in the next and final section to prove the main results of the paper.

2 Notation and Preliminaries

In this section, we introduce the notation that will be used throughout this paper. We also collect some classical results on the Modular Isomorphism Problem that will be useful in the coming sections, as well as a new criterion for the transfer of ideals between modular group algebras; cf. Lemma 2.6.

Throughout the paper, p will denote a prime number, k a field of characteristic p and G and H finite p-groups. The modular group algebra of G over k is denoted by kG and the augmentation ideal of kG is denoted by $\mathrm{I}(G)$. It is a classical result that $\mathrm{I}(G)$ is also the Jacobson ideal of kG. For every normal subgroup N of G, we write $\mathrm{I}(N; G)$ for the relative augmentation ideal $\mathrm{I}(N)kG$.

We let $\leq_{\mathrm{lex}}$ denote the lexicographic order on tuples of integers of the same length. Then $\min_{\mathrm{lex}}$ and $\max_{\mathrm{lex}}$ stand for minimum and maximum with respect to $\leq_{\mathrm{lex}}$. For a non-zero integer n, let $v_p(n)$ denote the p-adic valuation of n, that is, the greatest integer t such that p^t divides n. Moreover, set $v_p(0) = +\infty$. For coprime integers m and n, write $o_m(n)$ for the multiplicative order of n modulo m, i.e. the smallest non-negative integer k with $n^k \equiv 1 \bmod m$. Given non-zero integers s, t and n with $n \geq 0$ we set

$$\mathcal{S}(s \mid n) = \sum_{i=0}^{n-1} s^i \quad \text{and} \quad \mathcal{T}(s, t \mid n) = \sum_{0 \leq i < j < n} s^i t^j.$$

The last notation allows us, in some cases, to compactly express powering of products in a group G. For instance, if $g, h \in G$ and r, s, n are integers with $n \geq 0$ then, writing $a = [h, g] = h^{-1}g^{-1}hg$, we get the following identities:

$$\text{if } g^h = h^{-1}gh = g^r \text{ then } (hg)^n = h^n g^{\mathcal{S}(r|n)}, \tag{2.1}$$

$$\text{if } a^g = a^r \text{ and } a^h = a^s \text{ then } (gh)^n = g^n h^n a^{\mathcal{T}(r,s|n)}. \tag{2.2}$$

The next lemma describes elementary properties of the operators $\mathcal{S}$ and $\mathcal{T}$ that are collected in Lemmas 8.2 and 8.3 of [5].

Lemma 2.1 *Let p be an odd prime number and let $n > 0$ and s, t be integers satisfying $s \equiv t \equiv 1 \bmod p$. Then the following hold:*

(1) $v_p(s^n - 1) = v_p(s-1) + v_p(n)$, $v_p(\mathcal{S}(s \mid n)) = v_p(n)$ *and* $o_{p^n}(s) = p^{\max(0, n - v_p(s-1))}$.
(2) *if* $v_p(s-1) = a$ *and* p^{m-a} *divides* n *then* $\mathcal{S}(s \mid n) \equiv n \bmod p^m$.
(3) $\mathcal{T}(s, t \mid p^n) \equiv 0 \bmod p^n$.

Lemma 2.2 *Let p be an odd prime number and m and r be integers with $m > 0$ and $r \equiv 1 \bmod p$. Then for every integer $0 \le x < p^m$ there is a unique integer $0 \le y < p^m$ such that $\mathcal{S}(r \mid y) \equiv x \mod p^m$.*

Proof Let x and y be integers with $0 \le x \le y$. Then $\mathcal{S}(r \mid y) - \mathcal{S}(r \mid x) = r^x \mathcal{S}(r \mid y - x)$ and hence from Lemma 2.1(1) it follows that $\mathcal{S}(r \mid x) \equiv \mathcal{S}(r \mid y) \mod p^m$ if and only if $x \equiv y \mod p^m$. This shows that $\mathcal{S}(r \mid \cdot)$ induces an injective, thus bijective, map $\mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$. Then the result follows immediately. □

The group theoretic notation we use is mostly standard. For an arbitrary group G, let $|G|$ denote its order, $\mathrm{Z}(G)$ its center, $\{\gamma_i(G)\}_{i \ge 1}$ its lower central series, $G' = \gamma_2(G)$, its commutator subgroup, $\exp(G)$ its exponent and $\mathrm{d}(G) = \min\{|X| : X \subseteq G \text{ and } G = \langle X \rangle\}$, its minimum number of generators. Moreover, if $g \in G$ and $X \subseteq G$ then $|g|$ denotes the order of g and $\mathrm{C}_G(X)$ the centralizer of X in G. We write $\times$ both for internal and external direct products of groups. For $n \ge 1$, we denote by C_n the cyclic group of order n.

Let now G be a finite p-group and let $p^e = \exp(G)$. For every $0 \le n \le e$ we define the following subgroups of G:

$$\Omega_n(G) = \left\langle g \in G : g^{p^n} = 1 \right\rangle \quad \text{and} \quad \mho_n(G) = \left\langle g^{p^n} : g \in G \right\rangle.$$

If N is a normal subgroup of G, we also write

$$\Omega_n(G : N) = \left\langle g \in G : g^{p^n} \in N \right\rangle,$$

that is, $\Omega_n(G : N)$ is the only subgroup of G containing N such that

$$\Omega_n(G : N)/N = \Omega_n(G/N).$$

The group G is said to be *regular* if for every $g, h \in G$ there exist $c_1, \ldots, c_k \in \langle g, h \rangle'$ such that $(gh)^p = g^p h^p c_1^p \cdots c_k^p$, in other words

$$(gh)^p \equiv g^p h^p \bmod \mho_1(\langle g, h \rangle').$$

It is well known that if p is odd and G' is cyclic then G is regular, while this is not the case for $p = 2$; cf. [21, Satz III.10.2, Satz III.10.3(a)]. Moreover, if G is regular, [21, Hauptsatz III.10.5, Satz III.10.7] ensure that the following hold:

- $\Omega_n(G) = \{g \in G : g^{p^n} = 1\}$ and $\mho_n(G) = \{g^{p^n} : g \in G\}$,
- $|\Omega_n(G)| \cdot |\mho_n(G)| = |G|$ for every $0 \le n \le e$.

For every $n \ge 1$ and G regular we define w_n by means of

$$p^{\omega_n} = |\Omega_n(G)/\Omega_{n-1}(G)| = |\mho_{n-1}(G)/\mho_n(G)|$$

and remark that $\omega_1 \geq \omega_2 \geq \ldots \geq \omega_e > 0$. Following [21, § III.10] we set $\omega(G) = \omega_1$ and, for $1 \leq i \leq \omega(G)$, we define

$$e_i = |\{1 \leq n \leq e : \omega_n \geq i\}|.$$

It follows that $e = e_1 \geq e_2 \geq \ldots \geq e_{\omega(G)}$ and the entries of the list $(e_1, \ldots, e_{\omega(G)})$ are called the *type invariants* of G.

The *Jennings series* $(\mathrm{D}_n(G))_{n\geq 1}$ of the p-group G is defined by

$$\mathrm{D}_n(G) = \{g \in G : g - 1 \in \mathrm{I}(G)^i\} = \prod_{ip^j \geq n} \mho_j(\gamma_i(G)) \tag{2.3}$$

The Jennings series is also known as the *Brauer-Jennings-Zassenhaus series* or the *Lazard series* or the *dimension subgroup series* of kG (see [32, Section 11.1] for details). A property of these series that we will use is that, for abelian groups, the orders of the terms completely determine the structure of the group. For more on the Jennings series, see for instance [43, Section III.1], [26, Section 4] and [28, Section 2.3].

The next proposition and lemma collect some well-known results which will be used throughout the paper.

Proposition 2.3 *Let k be a field of positive characteristic p and let G be a finite p-group. Then the following statements hold:*

(1) *If H is a finite p-group and $\phi : kG \to kH$ is an isomorphism of k-algebras then*

$$\phi(\mathrm{I}(G'; G)) = \mathrm{I}(H'; H) \text{ and } \phi(\mathrm{I}(\mathrm{Z}(G)G'; G)) = \mathrm{I}(\mathrm{Z}(H)H'; H).$$

(2) *The following group invariants of G are algebra invariants of kG:*

   (a) *The isomorphism type of G/G'.*
   (b) *The exponent of G.*
   (c) *The isomorphism type of the consecutive quotients $\mathrm{D}_i(G)/\mathrm{D}_{i+1}(G)$ and $\mathrm{D}_i(G')/\mathrm{D}_{i+1}(G')$ of the Jennings series of G and G'.*
   (d) *The minimum number of generators $\mathrm{d}(G)$ of G and $\mathrm{d}(G')$ of G'.*
   (e) *The isomorphism types of $\mathrm{Z}(G) \cap G'$ and $\mathrm{Z}(G)/\mathrm{Z}(G) \cap G'$.*

(3) *The Modular Isomorphism Problem has a positive solution in the following cases:*

   (a) *G is abelian.*
   (b) *G is metacyclic.*
   (c) *G is 2-generated of class 2 and p is odd.*

Lemma 2.4 *Let k be a field of characteristic $p > 0$, let G and H be finite p-groups and let L_G and L_H be normal subgroups of G and H, respectively. Assume that there is an isomorphism $\phi : kG \to kH$ such that $\phi(\mathrm{I}(L_G; G)) = \mathrm{I}(L_H; H)$. Then, for each $i \geq 1$, there is an isomorphism of groups*

$$\mathrm{D}_i(L_G)/\mathrm{D}_{i+1}(L_G) \cong \mathrm{D}_i(L_H)/\mathrm{D}_{i+1}(L_H).$$

Remark 2.5 Although all the statements of Proposition 2.3 are well known, some of them appear in the literature with the assumption that $k = \mathbb{F}_p$, the field with p elements, and the proof of others is hidden inside proofs of other statements. We add a few words so that the reader can track the results in the literature.

The proof of (1) can be found inside the proof of [6, Theorem 2.(ii)]. Statements (a) and (b) from (2) are proven in [42, 47], [39, 47] and [23], respectively. The statement in (2)(c) for the Jenning series of G is proved in [32, Lemma 14.2.7(i)] while the statement for G' is proved for $k = \mathbb{F}_p$ in [1, Lemma 2] and it can be generalized to arbitrary k using the argument from [32, Lemma 14.2.7(i)]. Observe that the two statements in (2)(c) also follow from Lemma 2.4 specialized to $L_G = G$ and $L_G = G'$, respectively. Statement (2)(d) is a consequence of (2)(c) because $[\mathrm{D}_1(G) : \mathrm{D}_2(G)] = p^{\mathrm{d}(G)}$. In [39, Theorem 6.11] point (2)(e) is stated for $k = \mathbb{F}_p$, but its proof can be easily generalized to hold for any k.

Statement (3)(a) is proven in [13, Theorem 2] while statements (b) and (c) of (3) are proven for $k = \mathbb{F}_p$ in [1, 41] and [4], respectively. The latter proofs generalize gracefully for any k. Note that the analogue of (3)(c) for $p = 2$ appears in [4] for $k = \mathbb{F}_2$, but the proof does not generalize to arbitrary k.

Finally, Lemma 2.4 is proven for $k = \mathbb{F}_p$ in [39, Lemma 6.26] and the proof can be easily generalized to hold for any field of characteristic p.

We close this section with a lemma that we will make use of to obtain new group algebra invariants from old ones. A version of this lemma, specialized for $N_\Gamma = \Gamma'$ and with a different proof, appears in [37].

Lemma 2.6 (Transfer Lemma) *Let p be a prime number and G and H finite p-groups. For $\Gamma \in \{G, H\}$ let N_Γ be a subgroup of Γ containing Γ'. If k is a field of characteristic p and $\phi : kG \to kH$ is a ring isomorphism such that $\phi(\mathrm{I}(N_G; G)) = \mathrm{I}(N_H; H)$ then $\phi(I(\Omega_t(G : N_G); G)) = I(\Omega_t(H : N_H); H)$ for every positive integer t.*

Proof Fix $\Gamma \in \{G, H\}$. As Γ/N_Γ is abelian we have $\Omega_t(\Gamma : N_\Gamma) = \{g \in \Gamma : g^{p^t} \in N_\Gamma\}$. Then, if $t \geq 2$ we have $\Omega_t(\Gamma : N_\Gamma) = \Omega_1(\Gamma : \Omega_{t-1}(\Gamma : N_\Gamma))$ and hence we assume without loss of generality that $t = 1$. For brevity write $L_\Gamma = \Omega_1(\Gamma : N_\Gamma)$ and we will prove that $\phi(I(L_G; G)) = I(L_H, H)$.

Let $\tau_\Gamma : k\Gamma \to k\Gamma$ be the ring homomorphism extending the identity on Γ and the Frobenius map $x \to x^p$ on k. Moreover, for a normal subgroup K of Γ, let $\pi_K : k\Gamma \to k(\Gamma/K)$ denote the natural projection with $\ker \pi_K = \mathrm{I}(K; \Gamma)$. As Γ/N_Γ is abelian, the assignment $g \mapsto g^p$ on Γ induces a ring homomorphism $\lambda_\Gamma : k(\Gamma/N_\Gamma) \to k(\mho_1(\Gamma/N_\Gamma))$. We denote by σ_Γ the k-linear map extending the restriction of λ_Γ to Γ/N_Γ. By the definition of L_Γ and the hypothesis $\phi(\mathrm{I}(N_G; G)) = \mathrm{I}(N_H; H)$, we have that σ_Γ induces an isomorphism $\hat{\sigma}_\Gamma : k(\Gamma/L_\Gamma) \to k(\mho_1(\Gamma/N_\Gamma))$ and ϕ induces an isomorphism $\hat{\phi} : k(G/N_G) \to k(H/N_H)$ making the following diagram commute:

$$\begin{tikzcd}
 & k(G/L_G) \arrow[r, "\hat{\sigma}_G"] & k(\mho_1(G/N_G)) \arrow[d, "\tau_G"] \\
kG \arrow[ur, "\pi_{L_G}"] \arrow[r, "\pi_{N_G}"] \arrow[d, "\phi"] & k(G/N_G) \arrow[ur, "\sigma_G"] \arrow[r, "\lambda_G"] \arrow[d, "\hat{\phi}"] & k(\mho_1(G/N_G)) \arrow[d, "\hat{\phi}"] \\
kH \arrow[r, "\pi_{N_H}"] \arrow[dr, "\pi_{L_H}"] & k(H/N_H) \arrow[r, "\lambda_H"] \arrow[dr, "\sigma_H"] & k(\mho_1(H/N_H)) \\
 & k(H/L_H) \arrow[r, "\hat{\sigma}_H"] & k(\mho_1(H/N_H)) \arrow[u, "\tau_H"]
\end{tikzcd}$$

As ϕ is a bijection, then so is $\hat{\phi}$. Moreover, each $\hat{\sigma}_\Gamma$ is bijective and each τ_Γ is injective, thus we have

$$\begin{aligned} \phi(\mathrm{I}(L_G; G)) &= \phi(\ker \pi_{L_G}) = \phi(\ker(\tau_G \circ \hat{\sigma}_G \circ \pi_{L_G})) \\ &= \phi(\ker(\lambda_G \circ \pi_{N_G})) = \ker(\lambda_H \circ \pi_{N_H}) \\ &= \ker(\tau_H \circ \hat{\sigma}_H \circ \pi_{L_H}) = \ker(\pi_{L_H}) = \mathrm{I}(L_H; H), \end{aligned}$$

as desired. □

3 Finite 2-generated *p*-groups with Cyclic Commutator and *p* Odd

In this section $\boxed{\textit{p is an odd prime number.}}$ We start by recalling the classification of non-abelian 2-generated p-groups with cyclic commutator subgroup from [5]. Each such group G is showed to be uniquely determined, up to isomorphism, by an integral vector[1]

$$\mathrm{inv}(G) = (p, m, n_1, n_2, 1, 1, o_1, o_2, o_1', o_2', u_1, u_2)$$

of length 12 whose entries are determined as described below. The first four are straightforward and satisfy:

- $|G| = p^m$,
- $G/G' \cong C_{p^{n_1}} \times C_{p^{n_2}}$ with $n_1 \geq n_2 \geq 1$.

To continue, we define a *basis* of G to be a pair (b_1, b_2) of elements of G such that $G/G' = \langle b_1 G' \rangle \times \langle b_2 G' \rangle$ and $|b_i G'| = p^{n_i}$. Let $\mathcal{B}$ denote the set of bases of G. Moreover, for every $g \in G$, let $o(g) \in \mathbb{Z}_{\geq 0}$ be such that $p^{o(g)}$ is the order of $g\mathrm{C}_G(G')$ in $G/\mathrm{C}_G(G')$, in symbols $p^{o(g)} = |g\mathrm{C}_G(G')|$. Equivalently, $o(g) = m - v_p(r(g) - 1)$, where $r(g)$ denotes the unique integer satisfying $2 \leq r(g) \leq p^m + 1$ and $a^g = a^{r(g)}$ for each $a \in G'$. Define:

- $(o_1, o_2) = \min_{\mathrm{lex}}\{(o(b_1), o(b_2)) : (b_1, b_2) \in \mathcal{B}\}$ and

$$r_1 = 1 + p^{m-o_1} \quad \text{and} \quad r_2 = \begin{cases} 1 + p^{m-o_2}, & \text{if } o_2 > o_1; \\ r_1^{p^{o_1 - o_2}}, & \text{otherwise.} \end{cases} \tag{3.1}$$

Let now $\mathcal{B}_r = \mathcal{B}_r(G)$ be the set consisting of all bases (b_1, b_2) of G with the property that, for every $a \in G'$ and $i = 1, 2$, one has $a^{b_i} = a^{r_i}$, equivalently, $r(b_i) \equiv r_i \mod p^m$. The set $\mathcal{B}_r$ is not empty as proved in [5, Proposition 2.3(5)]. For every $b = (b_1, b_2) \in \mathcal{B}$, let $o'(b) = (o_1'(b), o_2'(b))$ and $u(b) = (u_2(b), u_1(b))$ be defined by

$$p^{n_i + o_i'(b)} = |b_i|, \quad b_i^{p^{n_i}} = [b_2, b_1]^{u_i(b) p^{m - o_i'(b)}} \quad \text{and} \quad 1 \leq u_i(b) < p^{m - o_i'(b)}. \tag{3.2}$$

Define subsequently:

- $(o_1', o_2') = \max_{\mathrm{lex}}\{o'(b) : b \in \mathcal{B}_r\}$ and
- $(u_2, u_1) = \min_{\mathrm{lex}}\{u(b) : b \in \mathcal{B}_r \text{ with } o'(b) = (o_1', o_2')\}$.

We have described how the entries of $\mathrm{inv}(G)$ are computed directly as structural invariants of G. Conversely, for a list of non-negative integers $I = (p, m, n_1, n_2, o_1, o_2, o_1', o_2', u_1, u_2)$,

[1] The classification in [5] is performed for all primes p and for $p = 2$ the fifth and sixth entries of $\mathrm{inv}(G)$ may also be -1.

defining r_1 and r_2 as in Eq. 3.1, the group $\mathcal{G}_I$ is defined as

$$\mathcal{G}_I = \left\langle b_1, b_2, a = [b_2, b_1] \mid a^{p^m} = 1, a^{b_i} = a^{r_i}, b_i^{p^{n_i}} = a^{u_i p^{m-o'_i}} \ (i = 1, 2) \right\rangle.$$

Denoting by $[G]$ the isomorphism class of a group G, the main result of [5] for p odd takes the following form.

Theorem 3.1 *The maps $[G] \mapsto \mathrm{inv}(G)$ and $I \mapsto [\mathcal{G}_I]$ define mutually inverse bijections between the isomorphism classes of 2-generated non-abelian groups of odd prime-power order and the set of lists of integers $(p, m, n_1, n_2, o_1, o_2, o'_1, o'_2, u_1, u_2)$ satisfying the following conditions.*

(1) *p is prime and $n_1 \geq n_2 \geq 1$.*
(2) *$0 \leq o_i < m$, $0 \leq o'_i \leq m - o_i$ and $p \nmid u_i$ for $i = 1, 2$.*
(3) *One of the following conditions holds:*

  (a) *$o_1 = 0$ and $o'_1 \leq o'_2 \leq o'_1 + o_2 + n_1 - n_2$.*
  (b) *$o_2 = 0 < o_1$, $n_2 < n_1$ and $o'_1 + \min(0, n_1 - n_2 - o_1) \leq o'_2 \leq o'_1 + n_1 - n_2$.*
  (c) *$0 < o_2 < o_1 < o_2 + n_1 - n_2$ and $o'_1 \leq o'_2 \leq o'_1 + n_1 - n_2$.*

(4) *$o_2 + o'_1 \leq m \leq n_1$ and one of the following conditions hold:*

  (a) *$o_1 + o'_2 \leq m \leq n_2$.*
  (b) *$2m - o_1 - o'_2 = n_2 < m$ and $u_2 \equiv 1 \mod p^{m-n_2}$.*

(5) *$1 \leq u_1 \leq p^{a_1}$, where $a_1 = \min(o'_1, o_2 + \min(n_1 - n_2 + o'_1 - o'_2, 0))$.*
(6) *One of the following conditions holds:*

  (a) *$1 \leq u_2 \leq p^{a_2}$.*
  (a) *$o_1 o_2 \neq 0$, $n_1 - n_2 + o'_1 - o'_2 = 0 < a_1$, $1 + p^{a_2} \leq u_2 \leq 2p^{a_2}$, and $u_1 \equiv 1 \mod p$;*

  where

$$a_2 = \begin{cases} 0, & \text{if } o_1 = 0; \\ \min(o_1, o'_2, o'_2 - o'_1 + \max(0, o_1 + n_2 - n_1)), & \text{if } o_2 = 0 < o_1; \\ \min(o_1 - o_2, o'_2 - o'_1), & \text{otherwise.} \end{cases}$$

In the remainder of the section, G denotes a finite non-abelian 2-generated p-group with cyclic commutator subgroup, with invariant vector

$$\mathrm{inv}(G) = (p, m, n_1, n_2, 1, 1, o_1, o_2, o'_1, o'_2, u_1, u_2).$$

and associated r_1 and r_2 as in Eq. 3.1.

Thanks to Theorem 3.1(2) and Lemma 2.1(1) we have

$$v_p(r_i - 1) = m - o_i > 0 \text{ for } i = 1, 2. \tag{3.3}$$

The following two lemmas are Lemma 2.2 and Lemma 4.2 from [5].

Lemma 3.2 *Let $b = (b_1, b_2)$ be a basis of G. Then $(o(b_1), o(b_2)) = (o_1, o_2)$ if and only if one of the following conditions holds:*

(1) *$o(b_1) = 0$.*
(2) *$0 = o(b_2) < o(b_1)$ and $n_2 < n_1$.*

(3) $0 < o(b_2) < o(b_1) < o(b_2) + n_1 - n_2$.

Lemma 3.3 *Let $b \in \mathcal{B}_r$. Then $o'(b) = (o'_1, o'_2)$ if and only if the following conditions hold:*

(1) *If $o_1 = 0$ then $o'_1(b) \leq o'_2(b) \leq o'_1(b) + o_2 + n_1 - n_2$.*
(2) *If $o_2 = 0 < o_1$ then $o'_1(b) + \min(0, n_1 - n_2 - o_1) \leq o'_2(b) \leq o'_1(b) + n_1 - n_2$.*
(3) *If $o_1 o_2 \neq 0$ then $o'_1(b) \leq o'_2(b) \leq o'_1(b) + n_1 - n_2$.*

For the following result, recall from the introduction that

$$O(G) = \min_{\text{lex}}\{(|b_1 \mathrm{C}_G(G')|, |b_2 \mathrm{C}_G(G')|, -|b_1|, -|b_2|) \mid (b_1, b_2) \in \mathcal{B}\}.$$

Lemma 3.4 *The following equality holds:* $\mathrm{O}(G) = (p^{o_1}, p^{o_2}, -p^{n_1+o'_1}, -p^{n_2+o'_2})$.

Proof For every $g \in G$ let $r(g)$ be the unique integer $2 \leq r(g) \leq p^m + 1$ such that $a^g = a^{r(g)}$ for every a in G'. From Lemma 2.1(1) it follows that

$$p^{o(g)} = |g\mathrm{C}_G(G')| = p^{m - v_p(r(g)-1)} = o_{p^m}(r(g)) \text{ for all } g \in G. \tag{3.4}$$

In particular, if $b \in \mathcal{B}_r$ and $i = 1, 2$, then $o(b_i) = o_i$. Thus the first two entries of $\mathrm{O}(G)$ are p^{o_1} and p^{o_2}. To deal with the remaining two entries, fix two bases $b = (b_1, b_2)$ and $b' = (b'_1, b'_2)$ of G with $b' \in \mathcal{B}_r$ and such that $\mathrm{O}(G) = (|b_1 \mathrm{C}_G(G')|, |b_2 \mathrm{C}_G(G')|, -|b_1|, -|b_2|)$ and $o'(b') = (o'_1, o'_2)$. In particular, we have $|b_i \mathrm{C}_G(G')| = |b'_i \mathrm{C}_G(G')| = p^{o_i}$. Moreover, $|b_i| = p^{n_i + o'_i(b)}$ and $|b'_i| = p^{n_i + o'_i}$. Thus $(-p^{n_1+o'_1(b)}, -p^{n_2+o'_2(b)}) = (-|b_1|, -|b_2|) \leq_{\text{lex}} (-p^{n_1+o'_1}, -p^{n_2+o'_2})$ or equivalently $o'(b) \geq_{\text{lex}} (o'_1, o'_2)$. On the other hand, the two automorphisms of G' given by $a \mapsto a^{b_i}$ and $a \mapsto a^{b'_i}$ have order p^{o_i}. Since $\mathrm{Aut}(G')$ is cyclic, there exist integers x_1 and x_2, both coprime to p, such that $b'' = (b_1^{x_1}, b_2^{x_2}) \in \mathcal{B}_r$. Thus $p^{n_i + o'_i(b'')} = |b_i^{x_i}| = |b_i| = p^{n_i + o'_i(b)}$ and hence $o'(b) = o'(b'') \leq_{\text{lex}} (o'_1, o'_2)$. We conclude that $o'(b) = (o'_1, o'_2)$ and hence $\mathrm{O}(G) = (p^{o_1}, p^{o_2}, -p^{n_1+o'_1}, -p^{n_2+o'_2})$. □

In the remainder of the section let $b = (b_1, b_2) \in \mathcal{B}_r$ be a fixed basis of G such that $o'(b) = (o'_1, o'_2)$ and denote $a = [b_2, b_1]$.

Then the following hold:

$$|a| = p^m, \quad |b_i G'| = p^{n_i}, \quad |b_i \mathrm{C}_G(G')| = p^{o_i} \quad |b_i| = p^{n_i + o'_i} \quad \text{and} \quad a^{b_i} = a^{r_i}. \tag{3.5}$$

In particular, every element of G is of the form $b_1^x b_2^y a^z$ for some integers x, y, z. Moreover, it follows from Eqs. 2.1 and 2.2 that, for every non-negative integer e, one has

$$(b_1^x b_2^y a^z)^{p^e} = b_1^{xp^e} b_2^{yp^e} a^{\mathcal{S}(r_1|x)\mathcal{S}(r_2|y)\mathcal{T}(r_1^x, r_2^y|p^e) + z\mathcal{S}(r_1^x r_2^y|p^e)}, \tag{3.6}$$

$$[a^e, b_1^x b_2^y a^z] = a^{e(r_1^x r_2^y - 1)}, \tag{3.7}$$

$$[b_1^x b_2^y a^z, b_1] = a^{\mathcal{S}(r_2|y) + z(r_1 - 1)}, \tag{3.8}$$

$$[b_1^x b_2^y a^z, b_2] = a^{-\mathcal{S}(r_1|x) r_2^y + z(r_2 - 1)}. \tag{3.9}$$

The next lemma describes some characteristic features of G.

Lemma 3.5 *The following statements hold:*

(1) $\mathrm{Z}(G) \cap G' = \left\langle a^{p^{\max(o_1, o_2)}} \right\rangle$.
(2) $\exp(G) = p^{\max(n_1 + o'_1, n_2 + o'_2)}$.

(3) *If* $i \geq 2$ *then* $\gamma_i(G) = \left\langle a^{p^{(i-2)(m-\max(o_1,o_2))}} \right\rangle$ *and the class of* G *is* $1 + \left\lceil \frac{m}{m-\max(o_1,o_2)} \right\rceil$.

Proof (1) Let w be a non-negative integer. As $v_p(r_i - 1) = m - o_i$ and $a^{b_i} = a^{r_i}$, we have that $a^{p^w} \in \mathrm{Z}(G)$ if and only if, for each $i \in \{1, 2\}$, one has $w + m - o_i \geq m$. Then $\mathrm{Z}(G) \cap G' = \left\langle a^{p^{\max(o_1,o_2)}} \right\rangle$.

(2) Let $e = \max(n_1 + o_1', n_2 + o_2')$. By Eq. 3.5, we have that $\exp(G) \geq p^e$ so we show that $\mho_e(G) = 1$. To this end, note that $e \geq m$ as a consequence of Theorem 3.13.1 and thus $\mho_e(G') = 1$. Now regularity yields that p^e-th powering induces a homomorphism $G/G' \to G$ and so, as a consequence of Eq. 3.5, we get $\mho_e(G) = 1$.

(3) We work by induction on i and, as the base case $i = 2$ is clear, we assume that $i > 2$ and the claim holds for $i - 1$. In other words, write $f = (i - 3)(m - \max(o_1, o_2))$ so that $\gamma_{i-1}(G) = \left\langle a^{p^f} \right\rangle$. It follows then from Eq. 3.7 that

$$\gamma_i(G) = \left\langle [a^{p^f}, b_1], [a^{p^f}, b_2] \right\rangle = \left\langle a^{p^f(r_1-1)}, a^{p^f(r_2-1)} \right\rangle = \left\langle a^{p^f \min(r_1-1,r_2-1)} \right\rangle.$$

We conclude by computing

$$v_p(p^f \min(r_1 - 1, r_2 - 1)) = f + m - \max(o_1, o_2) = (i - 2)(m - \max(o_1, o_2)).$$

□

Since each $\mathcal{S}(r_i \mid -)$ induces a bijection $\mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ (see Lemma 2.2) there are unique integers $1 \leq \delta_1 \leq p^{o_1}$ and $1 \leq \delta_2 \leq p^{o_2}$ satisfying the following congruences:

$$\mathcal{S}\left(r_2 \mid \delta_1 p^{m-o_1}\right) \equiv 1 - r_1 \mod p^m, \tag{3.10}$$

$$\mathcal{S}\left(r_1 \mid \delta_2 p^{m-o_2}\right) r_2^{\delta_1 p^{m-o_1}} \equiv r_2 - 1 \mod p^m. \tag{3.11}$$

Moreover, Eq. 3.1 and Lemma 2.1(1) yield that p does not divide $\delta_1\delta_2$.

Lemma 3.6 *The following hold:*

$$\begin{cases} \delta_1 = \delta_2 = 1, & \textit{if } o_1 = 0; \\ \delta_1 + \delta_2 \equiv 0 \mod p^{o_2}, & \textit{otherwise.} \end{cases} \tag{3.12}$$

Proof Assume first that $o_1 = 0$, implying that $\delta_1 = 1$, $r_1 = 1 + p^m$ and $r_2 = 1 + p^{m-o_2}$. Then Lemma 2.1(1)-(2) implies

$$\delta_2 p^{m-o_2} \equiv \mathcal{S}\left(r_1 \mid \delta_2 p^{m-o_2}\right) r_2^{p^{m-o_1}} \equiv r_2 - 1 = p^{m-o_2} \mod p^m$$

and hence $\delta_2 = 1$. Suppose now that $o_1 > 0$, which ensures that $o_1 > o_2$ and $r_2 = r_1^{p^{o_1-o_2}}$. As a consequence, we have $v_p(r_2 - 1) = m - o_2 > v_p(r_1 - 1) = m - o_1$. Moreover, by the definition of the δ_i's, there are integers λ and μ such that $\mathcal{S}\left(r_2 \mid \delta_1 p^{m-o_1}\right) = 1 - r_1 + \lambda p^m$ and $\mathcal{S}\left(r_1 \mid \delta_2 p^{m-o_2}\right) r_2^{\delta_1 p^{m-o_1}} = r_2 - 1 + \mu p^m$. Then the following identities hold:

$$\begin{aligned} r_1^{(\delta_1+\delta_2)p^{m-o_2}} - 1 &= r_1^{\delta_2 p^{m-o_2}} r_2^{\delta_1 p^{m-o_1}} - 1 \\ &= (r_1^{\delta_2 p^{m-o_2}} - 1) r_2^{\delta_1 p^{m-o_1}} + r_2^{\delta_1 p^{m-o_1}} - 1 \\ &= (r_1 - 1)\mathcal{S}\left(r_1 \mid \delta_2 p^{m-o_2}\right) r_2^{\delta_1 p^{m-o_1}} + (r_2 - 1)\mathcal{S}\left(r_2 \mid \delta_1 p^{m-o_1}\right) \\ &= p^m(\mu(r_1 - 1) + \lambda(r_2 - 1)) \equiv 0 \mod p^{2m-o_1}. \end{aligned}$$

We have shown that $p^m = o_{p^{2m-o_1}}(r_1)$ divides $(\delta_1 + \delta_2)p^{m-o_2}$ and hence $\delta_1 + \delta_2 \equiv 0 \mod p^{o_2}$, as desired. □

Lemma 3.7 *One has* $\mathrm{Z}(G) = \begin{cases} \left\langle b_1^{p^m}, b_2^{p^m}, b_1^{p^{m-o_2}} a \right\rangle, & \textit{if } o_1 = 0; \\ \left\langle b_1^{p^m}, b_2^{p^m}, b_1^{-\delta_1 p^{m-o_2}} b_2^{\delta_1 p^{m-o_1}} a \right\rangle, & \textit{otherwise.} \end{cases}$

Proof Let $g = b_1^x b_2^y a^z$ be an arbitrary element of G with $x, y, z \in \mathbb{Z}$. We characterize when $g \in \mathrm{Z}(G)$ in terms of conditions on the exponents x, y, z. For this, note that Eqs. 3.8 and 3.9 ensure that $g = b_1^x b_2^y a^z \in \mathrm{Z}(G)$ if and only if the following congruences hold:

$$\mathcal{S}\,(r_2 \mid y) \equiv z(1 - r_1) \mod p^m, \tag{3.13}$$

$$\mathcal{S}\,(r_1 \mid x)\, r_2^y \equiv z(r_2 - 1) \mod p^m. \tag{3.14}$$

In particular, the elements $b_1^{p^m}, b_2^{p^m}$ and $c = b_1^{\delta_2 p^{m-o_2}} b_2^{\delta_1 p^{m-o_1}} a$ are all central. Let

$$d = \begin{cases} b_1^{p^{m-o_2}} a, & \text{if } o_1 = 0; \\ b_1^{-\delta_1 p^{m-o_2}} b_2^{\delta_1 p^{m-o_1}} a, & \text{otherwise.} \end{cases}$$

By Eq. 3.12 we have $\left\langle b_1^{p^m}, b_2^{p^m}, d \right\rangle = \left\langle b_1^{p^m}, b_2^{p^m}, c \right\rangle \subseteq \mathrm{Z}(G)$. If $o_1 = 0$ and $g = b_1^x b_2^y a^z \in \mathrm{Z}(G)$ then it follows from Eq. 3.1 that Eq. 3.13 is equivalent to $y \equiv 0 \mod p^m$ and hence Eq. 3.14 is equivalent to $x \equiv z p^{m-o_2} \mod p^m$. Thus $g \in \left\langle b_1^{p^m}, b_2^{p^m}, d \right\rangle$ and hence $\mathrm{Z}(G) = \left\langle b_1^{p^m}, b_2^{p^m}, d \right\rangle$, as desired.

Suppose otherwise that $o_1 > 0$ and define $B = \left\langle b_2^{p^{m-o_1}} \right\rangle$, $N = b_2^{p^{\min(m,n_2)}}$ and $f : \mathrm{Z}(G) \to B/N$ by $f(b_1^x b_2^y a^z) = b_2^y N$. The map f is well defined because, on the one hand if $b_1^x b_2^y a^z = b_1^u b_2^v a^w$ then $y \equiv v \mod p^{n_2}$ and hence $b_2^y N = b_2^v N$; and on the other hand if $b_1^x b_2^y a^z \in \mathrm{Z}(G)$ then Eq. 3.13 ensures that $m - o_1 = v_p(r_1 - 1) \le \mathcal{S}\,(r_2 \mid y) = v_p(y)$ and hence $b_2^y \in B$.

We claim that $\ker f = \left\langle b_1^{p^m}, b_2^{p^m}, a^{p^{o_1}} \right\rangle$. The inclusion from right to left is clear. Assume $g = b_1^x b_2^y a^z \in \ker f$. If $m \le n_2$ this implies that p^m divides y. Then from Eq. 3.13 and Lemma 2.1(1) we have that $v_p(z) \ge o_1$ and hence from Eq. 3.14 we deduce that $v_p(x) \ge m - o_2 + o_1 > m$. This shows that $g \in \left\langle b_1^{p^m}, b_2^{p^m}, a^{p^{o_1}} \right\rangle$, as desired. Suppose now that $m > n_2$. Then $g = b_1^x a^z$ for some integers x and z and hence again from Eq. 3.13 we deduce that $v_p(z) \ge o_1$ and from Eq. 3.14 we conclude that $v_p(x) \ge m - o_2 + o_1 > m$. Therefore, again $g \in \left\langle b_1^{p^m}, b_2^{p^m}, a^{p^{o_1}} \right\rangle$ and the claim is proven.

We finally show that $\mathrm{Z}(G) = \left\langle b_1^{p^m}, b_2^{p^m}, c \right\rangle$. To this end, observe that B/N is generated by $f(c)$, as p does not divide δ_1. This together with the claim and the fact that f is a group homomorphism implies that $\mathrm{Z}(G) = \langle c, \ker f \rangle = \left\langle b_1^{p^m}, b_2^{p^m}, a^{p^{o_1}}, c \right\rangle$. To complete the proof we show that $a^{p^{o_1}} \in \left\langle b_1^{p^m}, b_2^{p^m}, c \right\rangle$. To this end, observe that the group $H = \left\langle b_1^{p^{m-o_2}}, b_2^{p^{m-o_1}}, a \right\rangle$ is regular and that $H' = \left\langle a^{p^{2m-o_1-o_2}} \right\rangle$. Indeed, $[a, b_1^{p^{m-o_2}}] = a^{r_1^{p^{m-o_2}} - 1}$, $[a, b_2^{p^{m-o_1}}] = a^{r_2^{p^{m-o_1}} - 1}$ and $[b_2^{p^{m-o_1}}, b_1^{p^{m-o_2}}] = a^{\mathcal{S}(r_1 | p^{m-o_2}) \mathcal{S}(r_2 | p^{m-o_1})}$, and these three elements generate the same subgroup $\left\langle a^{p^{2m-o_1-o_2}} \right\rangle$ since

$$v_p(r_1^{p^{m-o_2}} - 1) = v_p(r_2^{p^{m-o_1}} - 1) = v_p(\mathcal{S}\left(r_1 \mid p^{m-o_2}\right) \mathcal{S}\left(r_2 \mid p^{m-o_1}\right)) = 2m - o_1 - o_2.$$

As $(a^{p^{2m-o_1-o_2}})^{p^{o_1}} = a^{p^{2m-o_2}} = 1$, from the regularity of H it follows that $c^{p^{o_1}} = b_1^{\delta_2 p^{m-o_2+o_1}} b_2^{\delta_1 p^m} a^{p^{o_1}}$. Now $o_1 > 0$ implies $m - o_2 + o_1 > m$ and so the proof is complete. □

Lemma 3.8 *Let $t = m - \max(o_1, o_2)$. Then the following hold:*

(1) $|\mathrm{Z}(G) \cap G'| = p^t$, $\mathrm{Z}(G)G' = \left\langle a, b_i^{p^m}, b_1^{-p^{m-o_2}} b_2^{p^{m-o_1}} \right\rangle$ *and* $G/\mathrm{Z}(G)G' \cong C_{p^m} \times C_{p^t}$.

(2) $$\mathrm{C}_G(G') = \Omega_t(G : \mathrm{Z}(G)G') = \begin{cases} \left\langle a, b_1, b_2^{p^{o_2}} \right\rangle, & \textit{if } o_1 = 0; \\ \left\langle a, b_1^{p^{o_1}}, b_1^{p^{o_1-o_2}} b_2^{-1} \right\rangle, & \textit{otherwise.} \end{cases}$$

(3) $\mathrm{C}_G(G')' = \mho_{m-t}(G')$.

(4) *If* $o_1 = 0$ *then* $\exp(\mathrm{C}_G(G')) = p^{n_1+o_1'}$.

(5) *If* $o_2 = 0$ *then* $\exp(\mathrm{C}_G(G')) = p^{\max(n_1+o_1'-o_1, n_2+o_2')}$.

Proof (1) This is a direct consequence of Lemma 3.5(1) and Lemma 3.7.

(2) Let $g = b_1^x b_2^y a^z$ be an arbitrary element of G. Then Eq. 3.7 yields that $g \in \mathrm{C}_G(G')$ if and only if $a^{r_1^x r_2^y - 1} = 1$. If $o_1 = 0$ then the last equality holds if and only if $(1 + p^{m-o_2})^y - 1 \equiv 0 \bmod p^m$, equivalently if p^{o_2} divides y. So

$$o_1 = 0 \text{ implies } \mathrm{C}_G(G') = \left\langle a, b_1, b_2^{p^{o_2}} \right\rangle. \tag{3.15}$$

Suppose now that $o_1 > 0$. Then $r_1 = 1 + p^{m-o_1}$ and $r_2 = r_1^{p^{o_1-o_2}}$ yielding that $[a, g] = a^{(1+p^{m-o_1})^{x+yp^{o_1-o_2}}-1}$. As $o_{p^m}(1 + p^{m-o_1}) = p^{o_1}$, we have that $g \in \mathrm{C}_G(G')$ if and only if $x + yp^{o_1-o_2} \equiv 0 \bmod p^{o_1}$, that is there exists an integer v with $x = -yp^{o_1-o_2} + vp^{o_1}$. We have proven that

$$o_1 > 0 \text{ implies } \mathrm{C}_G(G') = \left\langle a, b_1^{p^{o_1}}, b_1^{p^{o_1-o_2}} b_2^{-1} \right\rangle. \tag{3.16}$$

To conclude, let $L = \mho_t(G : Z(G)G')$. By (1), Eqs. 3.15 and 3.16 we have that $\mathrm{C}_G(G') \subseteq L$ and $G/\mathrm{C}_G(G') \cong G/L \cong C_{p^{m-t}}$ and therefore $\mathrm{C}_G(G') = L$.

(3) The group G' being cyclic, $\mho_{m-t}(G') = \Omega_t(G')$ and so (2) and the regularity of G yield that $\mho_t(L') = [L, \mho_t(L)] \subseteq [L, \mathrm{Z}(G)G'] = 1$, that is $L' \subseteq \Omega_t(G') = \mho_{m-t}(G')$. For the other inclusion, it suffices to observe that

$$\mho_{m-t}(G') = \left\langle a^{p^{m-t}} \right\rangle = \begin{cases} \left\langle [b_1, b_2^{p^{o_2}}] \right\rangle, & \text{if } o_1 = 0; \\ \left\langle [b_1^{p^{o_1}}, (b_1^{p^{o_1-o_2}} b_2^{-1})] \right\rangle, & \text{otherwise.} \end{cases}$$

(4)-(5) Assume that $o_1 = 0$. Then we have $b_1 \in \mathrm{C}_G(G')$ and $|b_1| = p^{n_1+o_1'}$, from which we derive $\exp(G) \geq p^{n_1+o_1'}$. Let now $e = n_1 + o_1'$. Then Theorem 3.1(3)-(4) yields that $m \leq e$ and $n_2 + o_2' - o_2 \leq e$. It follows from Eqs. 3.5, 3.6 and Lemma 2.1(1)-(3) that $(b_1^x b_2^{yp^{o_2}} a^z)^{p^e} = 1$ for every $x, y, z \in \mathbb{Z}$. We have shown that $\exp(\mathrm{C}_G(G')) = p^{n_1+o_1'}$. A similar argument works when $o_2 = 0 < o_1$. □

In the following lemma, $\mathrm{Soc}(G')$ denotes the *socle* of G'. We remark that $\mathrm{Soc}(G') = \left\langle a^{p^{m-1}} \right\rangle$, because G' is cyclic of order p^m and $m \geq 1$.

Lemma 3.9 *Write $\overline{G} = G/Soc(G')$ and assume that $m \geq 2$. Then $\overline{G}$ is a non-abelian group and one has* $\operatorname{inv}(\overline{G}) = (p, m-1, n_1, n_2, 1, 1, \overline{o}_1, \overline{o}_2, \overline{o}'_1, \overline{o}'_2, \overline{u}_1, \overline{u}_2)$ *where:*

$$\begin{aligned}
\overline{o}_i &= \max(0, o_i - 1), \textit{for } i = 1, 2;\\
\overline{o}'_1 &= \begin{cases} o'_1, & \textit{if } o_1 = 0,\ 0 < \min(o'_1, o_2) \textit{ and } o'_2 = o'_1 + o_2 + n_1 - n_2;\\ \max(0, o'_1 - 1), & \textit{otherwise};\end{cases}\\
\overline{o}'_2 &= \begin{cases} o'_2, & \textit{if } o_2 = 0,\ n_1 - n_2 < o_1 \textit{ and } 0 < o'_2 = o'_1 + n_1 - n_2 - o_1;\\ \max(0, o'_2 - 1), & \textit{otherwise}.\end{cases}
\end{aligned}$$

Proof That the first four entries of $\operatorname{inv}(\overline{G})$ are $p, m-1, n_1$ and n_2 is obvious. Since we are dealing with two groups G and $\overline{G}$, in this proof we distinguish $\mathcal{B}_r = \mathcal{B}_r(G)$ and $\mathcal{B}_r(\overline{G})$.

Let $\overline{g}$ denote the natural image in $\overline{G}$ of an element $g \in G$. Then $r(\overline{g})$ is the unique integer in the interval $[2, p^{m-1}+1]$ that is congruent to $r(g)$ modulo p^{m-1}. By Eq. 3.4 we have

$$m - 1 - o(\overline{b_i}) = v_p(r(\overline{b_i}) - 1) = m - \max(1, o_i).$$

Hence $o(\overline{b_i}) = \max(0, o_i - 1)$ and thus Lemma 3.2 yields that $\overline{o}_i = \max(0, o_i - 1)$. Moreover, $\overline{b} = (\overline{b}_1, \overline{b}_2)$ is an element of $\mathcal{B}_r(\overline{G})$. Note that the following hold:

$$b_i^{p^{n_i+o'_i}} = 1; \quad \overline{b}_i^{p^{n_i+o'_i-1}} = \begin{cases} \overline{a}^{p^{m-1}} = 1, & \text{if } o'_i \neq 0;\\ \overline{b}_i^{p^{n_i-1}} \neq 1 & \text{if } o'_i = 0;\end{cases} \quad \text{and} \quad \overline{b}_i^{p^{n_i+o'_i-2}} = \begin{cases} \overline{a}^{p^{m-2}} \neq 1, & \text{if } o'_i > 1;\\ \overline{b}_i^{p^{n_i-1}} \neq 1, & \text{if } o'_1 = 1.\end{cases}$$

Therefore we derive that $o'_i(\overline{b}) = \log_p |\overline{b}_i| - n_i = \max(0, o'_i - 1)$.

To finish the proof we distinguish three cases according to Lemma 3.3 and search for some $\hat{b} \in \mathcal{B}_r(\overline{G})$ satisfying the corresponding conditions in the lemma. Then Lemma 3.3 will guarantee that $o'_i = o'_i(\hat{b}_i)$ for $i = 1, 2$. In most cases $\overline{b}$ already satisfies the desired conditions and hence, in such cases, we take $\hat{b} = \overline{b}$ and hence $\overline{o}'_i = o'_i(\overline{b}) = \max(0, o'_i - 1)$. Otherwise we modify slightly $\overline{b}$ to obtain the desired $\hat{b}$.

Case 1. Suppose first that $o_1 = 0$. By Theorem 3.1(3) we have

$$o'_1 \leq o'_2 \leq o'_1 + o_2 + n_1 - n_2$$

and hence $o'_1(\overline{b}) = \max(0, o'_1 - 1) \leq \max(0, o'_2 - 1) \leq \overline{o}'_2(\overline{b})$. Moreover, unless $0 < \min(o'_1, o_2)$ and $o'_2 = o'_1 + o_2 + n_1 - n_2$, we also have $o'_2(\overline{b}) \leq o'_1(\overline{b}) + \overline{o_2} + n_1 - n_2$. As $\overline{o}_1 = 0$, the conditions in Lemma 3.3 hold for $\hat{b} = \overline{b}$ and hence we have $\overline{o}'_i = o'_i(\overline{b}) = \max(0, o'_i - 1)$, as desired. Assume now that $0 < \min(o'_1, o_2)$ and $o'_2 = o'_1 + o_2 + n_1 - n_2$. Then $o'_1(\overline{b}) = o'_1 - 1$, $o'_2(\overline{b}) = o'_2 - 1$ and $\overline{o}_2 = o_2(\overline{b}) = o_2 - 1$ and hence $\overline{b}$ does not satisfy the hypotheses of Lemma 3.3. Then we take $\hat{b} = (\overline{b}_1 \overline{b}_2^{p^{\overline{o}_2}}, \overline{b}_2)$, which belongs to $\mathcal{B}_r(\overline{G})$ because $[\overline{b_2}^{p^{\overline{o_2}}}, \overline{a}] = 1$. Using Eq. 3.6, the regularity of G and $m \leq n_1$ we compute

$$\hat{b}_1^{p^{n_1}} = \overline{b}_1^{p^{n_1}} \overline{b}_2^{p^{n_1+\overline{o}_2}} = \overline{a}^{p^{m-o'_1}} \overline{b}_2^{p^{n_1+o_2-1}} = \overline{a}^{p^{m-o'_1}} \overline{b}_2^{p^{n_2+o'_2-o'_1-1}} = \overline{a}^{p^{m-o'_1}+p^{m-o'_1-1}}$$

and hence $|\hat{b}_1| = p^{n_1+o'_1}$ so that $o'_1(\hat{b}) = o'_1$, $o'_2(\hat{b}) = o'_2 - 1$ and we conclude from Lemma 3.3 that $\overline{o}'_1 = o'_1$ and $\overline{o}'_2 = o'_2 - 1$. This yields the desired conclusion because in this case $n_1 - n_2 \geq 0 = o_1$ and $o'_2 \geq o'_1 > 0$.

Case 2. Suppose that $o_2 = 0 < o_1$ so that Theorem 3.1(3) ensures

$$o'_1 + \min(0, n_1 - n_2 - o_1) \leq o'_2 \leq o'_1 + n_1 - n_2.$$

Assume first that $n_1 - n_2 \geq o_1$. Then we have $n_1 - n_2 \geq \overline{o}_1$ and $o'_1 \leq o'_2 \leq o'_1 + n_1 - n_2$ and consequently also $o'_1(\overline{b}) \leq o'_2(\overline{b}) \leq o'_1(\overline{b}) + n_1 - n_2$. Hence $\overline{o}'_i = o'_i(\overline{b}) = \max(0, o'_i - 1)$.

Suppose now that $n_1 - n_2 < o_1$. Then by Theorem 3.1(3) we have $0 < n_1 - n_2$. If $o'_2 = 0$ or $o'_2 > o'_1 + n_1 - n_2 - o_1$ then we also have $o'_1(\overline{b}) + \min(0, n_1 - n_2 - \overline{o}_1) \leq o'_2(\overline{b}) \leq o'_1(\overline{b}) + n_1 - n_2$ and again we have $\overline{o}_i = o'_i(\overline{b}) = \max(0, o'_i - 1)$. Assume now that $0 < o'_2 = o'_1 + n_1 - n_2 - o_1$. It follows that $o'_1 > 0$ and hence $o'_1(\overline{b}) + \min(0, n_1 - n_2 - o_1(\overline{b})) = o'_1 + \min(0, n_1 - n_2 - o_1) > o'_2(b) - 1 = o'_2(\overline{b})$. Therefore Lemma 3.3 yields $o'(\overline{b}) \neq \overline{o}'$. In this case we take the basis $\hat{b} = (\overline{b}_1, \overline{b}_1^{p^{\overline{o}_1}} \overline{b}_2)$, which again belongs to the set $\mathcal{B}_r(\overline{G})$ because $[\overline{b}_1^{p^{\overline{o}_1}}, \overline{a}] = 1$. Then $o'_1(\overline{b}) = o'_1 - 1$ and if $k = \mathcal{S}\left(r_1 \mid p^{o_1 - 1}\right) \mathcal{S}\left(r_2 \mid 1\right) \mathcal{T}\left(r_1^{p^{o_1-1}}, r_2 \mid p^{n_2}\right) + \mathcal{S}\left(r_1^{p^{o_1-1}} r_2 \mid p^{n_2}\right)$ then Lemma 2.1 and Theorem 3.1(4) imply $v_p(k) \geq n_2 \geq m + o'_2$. Using Eq. 3.6 we get

$$(\overline{b}_1^{p^{o_1-1}} \overline{b}_2)^{p^{n_2}} = a^{p^{m-1-o'_2} + p^{m-o'_2} + k}.$$

Therefore $|\overline{b}_1^{p^{o_1-1}} \overline{b}_2| = p^{n_2 + o'_2}$ and we conclude that $o'_1(\hat{b}) = o'_1 - 1, o'_2(\hat{b}) = o'_2$ and hence $\overline{o}'_1 = o'_1 - 1$ and $\overline{o}'_2 = o'_2$.

Case 3. Finally, suppose that $o_1 o_2 \neq 0$. Then $\overline{o}_1 = o_1 - 1 > o_2 - 1 = \overline{o}_2 \geq 0$ and Theorem 3.1(3) guarantees $o'_1 \leq o'_2 \leq o'_1 + n_1 - n_2$. Hence $o'_1(\overline{b}) + \min(0, n_1 - n_1 - \overline{o}_1) \leq o'_1(\overline{b}) \leq o'_2(\overline{b}) \leq o'_1(\overline{b}) + n_1 - n_2$ and we get $\overline{o}'_i = o'_i(\overline{b}) = \max(0, o'_i - 1)$. □

4 Proofs of the Main Results

In this section we prove Theorem A, Theorem B and Theorem C. The first one will be included in Lemma 4.2, which relies on Lemma 4.1. Theorem B is proven shortly after Lemma 4.2, while Theorem C is a consequence of Lemma 4.3 and 4.4. We conclude the section by proving Corollary D and Corollary E, here presented as Corollary 4.5 and Corollary 4.6, respectively.

Lemma 4.1 *Let p be an odd prime and let G be a finite p-group with cyclic commutator subgroup. Write, moreover, $|G'| = p^m$ and $|G' \cap \mathrm{Z}(G)| = p^t$. Then the following hold:*

$$\mathrm{C}_G(G') = \{g \in G : g^{p^t} \in \mathrm{Z}(G)G'\} \quad \text{and} \quad \mathrm{C}_G(G')' = \mho_{m-t}(G').$$

Moreover, for every subgroup N of G contained in $\mathrm{C}_G(G')$ one has

$$\exp(N) = p^{\min\{n \,:\, \mathrm{D}_{p^n}(N) = 1\}}.$$

Proof The abelian case is straightforward so we assume that $G' \neq 1$. By a Theorem of Cheng [9] the group G can be expressed as a central product

$$G = H * G_1 * \cdots * G_s * A,$$

where each G_i is a 2-generated group of nipotency class 2, the group H is 2-generated with $H' = G'$ and A is abelian. For each $i = 1, \ldots, s$, write $G_i = \langle x_i, y_i \rangle$ and $|G'_i| = p^{m_i}$. Set $K = G_1 * \cdots * G_s * A$. As $G' = H'$ and $[H, G_i] = [H, A] = 1$ it follows that $Z(H) \cap H' = Z(G) \cap G'$ and $\mathrm{C}_G(G') = \mathrm{C}_G(H') = \mathrm{C}_H(H')K$. Let $L = \{g \in G :$

$g^{p^t} \in \mathrm{Z}(G)G'\}$ and note that $A \subseteq L$. Moreover, since each G_i is of class 2, we have that $Z(G_i) = \left\langle G_i', x_i^{p^{m_i}}, y_i^{p^{m_i}} \right\rangle$ and hence

$$\mathrm{Z}(G) = \left\langle \mathrm{Z}(H), A, x_i^{p^{m_i}}, y_i^{p^{m_i}} \ : \ i = 1, \dots, s \right\rangle.$$

For each i, observe that $m_i \leq t \leq m$ because $G_1' * \cdots * G_s'$ is contained in $\mathrm{Z}(G) \cap G'$. Therefore, for each choice of i, one has $\mho_t(G_i) \subseteq \mathrm{Z}(G)$ and we derive that $K \subseteq L$. Moreover, it follows from $[H, K] = 1$ that $Z(H)H' \subseteq Z(G)G'$. Since $|\mathrm{Z}(H) \cap H'| = p^t$, Lemma 3.8(2) yields $\mathrm{C}_G(G') = \mathrm{C}_H(H')K = \{h \in H : h^{p^t} \in \mathrm{Z}(H)H'\}K \subseteq L$. For the other inclusion take $g = hk \in L$ with $h \in H$ and $k \in K$ and note that $h \in H \cap L \subseteq \mathrm{C}_H(H')$ by Lemma 3.8(2). This shows that $\mathrm{C}_G(G') = L$.

We now show that $\mathrm{C}_G(G')' = \mho_{m-t}(G')$. For this, let $g, h \in C_G(G')$. Then $h^{p^t} \in G'\mathrm{Z}(G)$ and, as $C_G(G')$ has nilpotency class 2, we have that $[g, h]^{p^t} = [g, h^{p^t}] = 1$. We have proven that $C_G(G')' \subseteq \mho_{m-t}(G')$ while Lemma 3.8(3) ensures that $\mho_{m-t}(G') = \mho_{m-t}(H') = \mathrm{C}_H(H')' \subseteq \mathrm{C}_G(G')'$.

Finally let N be a subgroup of G such that $N \subseteq \mathrm{C}_G(G')$. Then N has nilpotency class 2, so that Eq. 2.3 yields $\mathrm{D}_{p^n}(N) = \mho_n(N)$ and the result follows. □

The following result is a stronger version of Theorem A.

Theorem 4.2 *Let k be a field of odd characteristic p and let G be a finite p-group with cyclic commutator subgroup. If H is another group with kG and kH isomorphic as k-algebras then*

(a) *For every algebra isomorphism $\phi : kG \to kH$ preserving augmentation one has that*

$$\phi(\mathrm{I}(\mathrm{C}_G(G'); G)) = \mathrm{I}(\mathrm{C}_H(H'); H);$$

(b) $\mathrm{D}_i(\mathrm{C}_G(G'))/\mathrm{D}_{i+1}(\mathrm{C}_G(G')) \cong \mathrm{D}_i(\mathrm{C}_H(G'))/\mathrm{D}_{i+1}(\mathrm{C}_H(H'))$ *for every $i \geq 1$;*
(c) $\exp(\mathrm{C}_G(G')) = \exp(\mathrm{C}_H(H'))$*;*
(d) $\mathrm{C}_G(G')/G' \cong \mathrm{C}_H(H')/H'$*;*
(e) $\mathrm{C}_G(G')/\mathrm{C}_G(G')' \cong \mathrm{C}_H(H')/\mathrm{C}_H(H')'$.

Proof Let H be a group such that $kG \cong kH$ and let $\Gamma \in \{G, H\}$. It is well known that there exists an isomorphism $kG \to kH$ preserving augmentation (see e.g. the remark on page 63 of [43]). Then H' is also cyclic as a consequence of Proposition 2.3(2)(d). Moreover, the number $|\mathrm{Z}(G) \cap G'| = p^t$ is an algebra invariant of kG by Proposition 2.3(2)(e). By Lemma 4.1 and Proposition 2.3(1), the hypotheses of Lemma 2.6 hold for $L_\Gamma = \mathrm{C}_\Gamma(\Gamma')$ and $N_\Gamma = Z(\Gamma)\Gamma'$. Therefore, if $\phi : kG \to kH$ is an algebra isomorphism then $\phi(\mathrm{I}(\mathrm{C}_G(G'); G)) = \mathrm{I}(\mathrm{C}_H(H'); H)$ and hence $\mathrm{D}_i(\mathrm{C}_G(G'))/\mathrm{D}_{i+1}(\mathrm{C}_G(G')) \cong \mathrm{D}_i(\mathrm{C}_H(G'))/\mathrm{D}_i(\mathrm{C}_H(H'))$ by Lemma 2.4. This implies that the lists of orders of the terms of the Jennings series of $\mathrm{C}_G(G')$ and $\mathrm{C}_H(H')$ are equal and, by Lemma 4.1, these groups have the same exponent. Finally, observe that since $\mathrm{I}(\mathrm{C}_G(G'); G)/\mathrm{I}(G'; G) \cong \mathrm{I}(\mathrm{C}_G(G')/G'; G/G')$, if $\hat{\phi} : k(G/G') \to k(H/H')$ is the isomorphism induced by ϕ then $\hat{\phi}(\mathrm{I}(\mathrm{C}_G(G')/G'; G/G')) = \mathrm{I}(\mathrm{C}_H(H')/H'; H/H')$. This and the fact that the groups $\mathrm{C}_G(G')/G'$ and $\mathrm{C}_H(H')/H'$ are both abelian yield, by using the argument in [32, Lemma 14.2.7(ii)], that they are isomorphic. Writing $p^m = |G'|$, Lemma 4.1 ensures that $\mathrm{I}(\mathrm{C}_G(G')'; G) = \mathrm{I}(G'; G)^{p^{m-t}}$ and so ϕ induces another isomorphism $\tilde{\phi} : k(G/\mathrm{C}_G(G')') \to k(H/\mathrm{C}_H(H')')$, and the same argument yields that $\mathrm{C}_G(G')/\mathrm{C}_G(G')' \cong \mathrm{C}_H(H')/\mathrm{C}_H(H')'$. □

In the remainder of the section we prove Theorem B, Theorem C, Corollary D and Corollary E. For that we fix a field k of odd characteristic p, a finite 2-generated p-group G with cyclic commutator subgroup and a group H such that $kG \cong kH$. Then, by Proposition 2.3(2)(d), the group H is also 2-generated with a cyclic commutator subgroup. Moreover, Proposition 2.3(2)(a) yields that, if one of the two groups is abelian, then $G \cong H$. We assume hence without loss of generality that G and H are non-abelian. Now, by Proposition 2.3(2)(a), the first six entries of $\mathrm{inv}(G)$ and $\mathrm{inv}(H)$ coincide. Thus we set

$$\mathrm{inv}(\Gamma) = (p, m, n_1, n_2, 1, 1, o_1^\Gamma, o_2^\Gamma, o_1'^\Gamma, o_2'^\Gamma, u_1^\Gamma, u_2^\Gamma) \quad \text{for } \Gamma \in \{G, H\} \tag{4.1}$$

and observe that $m \geq 1$. To simplify the notation we denote $o^\Gamma = (o_1^\Gamma, o_2^\Gamma)$ and $o'^\Gamma = (o_1'^\Gamma, o_2'^\Gamma)$. We will prove that $o^G = o^H$ and $o'^G = o'^H$ in Lemma 4.3 and Lemma 4.4, respectively. These results will imply Theorem C. Combining Theorem C with Lemma 3.4, we will obtain Theorem B.

For the proofs of Lemma 4.3 and 4.4, we argue by induction on m. The induction base case is covered by Proposition 2.3(3)(c), as well as the case where G has nilpotency class 2. Because of this, we assume without loss of generality that both G and H are of nilpotency class greater than 2 and so $m \geq 2$: Lemma 3.5(3) implies that $o^G \neq (0, 0)$ and $o^H \neq (0, 0)$. Additionally we assume that, if $\tilde{G}$ is a 2-generated finite p-group with cyclic commutator subgroup of cardinality $|\tilde{G}'| < p^m$, then $(o^{\tilde{G}}, o'^{\tilde{G}})$ is an algebra invariant of $k\tilde{G}$. Denote now

$$\overline{\Gamma} = \Gamma/\mathrm{Soc}(\Gamma'), \quad \mathrm{inv}(\overline{\Gamma}) = (p, m-1, n_1, n_2, 1, 1, o_1^{\overline{\Gamma}}, o_2^{\overline{\Gamma}}, o_1'^{\overline{\Gamma}}, o_2'^{\overline{\Gamma}}, u_1^{\overline{\Gamma}}, u_2^{\overline{\Gamma}}), \quad o^{\overline{\Gamma}} = (o_1^{\overline{\Gamma}}, o_2^{\overline{\Gamma}}), \quad o'^{\overline{\Gamma}} = (o_1'^{\overline{\Gamma}}, o_2'^{\overline{\Gamma}}).$$

By Proposition 2.3(1), if $\phi : kG \to kH$ is an isomorphism of algebras, then $\phi(\mathrm{I}(G'; G)) = \mathrm{I}(H'; H)$ and, as $\mathrm{I}(G'; G)^{p^{m-1}} = \mathrm{I}(G')^{p^{m-1}} kG = \mathrm{I}(\mathrm{Soc}(G'))kG = \mathrm{I}(\mathrm{Soc}(G'); G)$, it follows that $\phi(\mathrm{I}(\mathrm{Soc}(G'); G)) = \mathrm{I}(\mathrm{Soc}(H'); G)$. We derive that

$$k\overline{G} \cong \frac{kG}{\mathrm{I}(\mathrm{Soc}(G'); G)} \cong \frac{kH}{\mathrm{I}(\mathrm{Soc}(H'); H)} \cong k\overline{H}$$

and the induction hypothesis yields that

$$o^{\overline{G}} = o^{\overline{H}} \quad \text{and} \quad o'^{\overline{G}} = o'^{\overline{H}}. \tag{4.2}$$

As in the previous section, fix $b = (b_1, b_2) \in \mathcal{B}_r(\Gamma)$ with $o'(b) = o'^\Gamma$ for $\Gamma \in \{G, H\}$. Thus b_1, b_2 and $a = [b_2, b_1]$ have different meanings depending on whether they are considered as elements in G or H. The context, however, shall always be clear and any confusion avoided.

Lemma 4.3 *One has $o^G = o^H$.*

Proof By means of contradiction assume $o^G \neq o^H$ and without loss of generality suppose $o^G <_{\mathrm{lex}} o^H$. Recall that $\mathrm{Z}(G) \cap G' \cong \mathrm{Z}(H) \cap H'$, by Proposition 2.3(2)(e), so Lemma 3.5(1) implies $\max\{o_1^G, o_2^G\} = \max\{o_1^H, o_2^H\}$. Combining this with Theorem 3.1(3) it follows that $n_2 < n_1$, for otherwise $o_1^G = o_1^H = 0$ and the previous maximum equals $o_2^G = o_2^H$. As a consequence of Lemma 3.9 and Eq. 4.2 we get that

$$\max(0, o_i^G - 1) = o_i^{\overline{G}} = o_i^{\overline{H}} = \max(0, o_i^H - 1).$$

Then either $\{o_1^G, o_1^H\} = \{0, 1\}$ or $\{o_2^G, o_2^H\} = \{0, 1\}$, equivalently either $(o_1^G, o_1^H) = (0, 1)$ or $o_1^G = o_1^H$ and $(o_2^G, o_2^H) = (0, 1)$. Moreover, by Theorem 3.1(3), we have that for each

$\Gamma \in \{G, H\}$ either $o_1^\Gamma = 0$, or $o_2^\Gamma = 0 < o_1^\Gamma$ or $0 < o_1^\Gamma - o_2^\Gamma < n_1 - n_2$. Hence one of the following conditions holds:

(1) $o^G = (0, 1)$ and $o^H = (1, 0)$;
(2) $o^G = (o_1, 0)$ and $o^H = (o_1, 1)$ with $1 < o_1 < 1 + n_1 - n_2$.

We will prove in both cases that $\mathrm{Z}(G)G'/G'$ and $\mathrm{Z}(H)H'/H'$ have different exponent which, in view of Proposition 2.3(2) (e), is not compatible with $kG \cong kH$.

(1) First assume $o^G = (0, 1)$ and $o^H = (1, 0)$. Then, applying Lemma 3.7, we have

$$\mathrm{Z}(G) = \left\langle b_1^{p^m}, b_2^{p^m}, b_1^{p^{m-1}} a \right\rangle \quad \text{and} \quad \mathrm{Z}(H) = \left\langle b_1^{p^m}, b_2^{p^m}, b_2^{-p^{m-1}} a \right\rangle.$$

It follows in particular that

$$\mathrm{Z}(G)/\mathrm{Z}(G) \cap G' \cong \mathrm{Z}(G)G'/G' = \left\langle b_1^{p^{m-1}} G' \right\rangle \times \left\langle b_2^{p^m} G' \right\rangle \cong \mathrm{C}_{p^{n_1-m+1}} \times \mathrm{C}_{p^{n_2-m}},$$

$$\mathrm{Z}(H)/\mathrm{Z}(H) \cap H' \cong \mathrm{Z}(H)H'/H' = \left\langle b_1^{p^m} G' \right\rangle \times \langle b_2 p^{m-1} G' \rangle \cong \mathrm{C}_{p^{n_1-m}} \times \mathrm{C}_{p^{n_2-m+1}},$$

and, as $n_2 < n_1$, the exponent of $\mathrm{Z}(G)/\mathrm{Z}(G) \cap G'$ is p^{n_1-m+1} while the exponent of $\mathrm{Z}(H)/\mathrm{Z}(H) \cap H'$ is p^{n_1-m}.

(2) Assume $o^G = (o_1, 0)$ and $o^H = (o_1, 1)$ with $1 < o_1 < 1 + n_1 - n_2$. It follows from Lemma 3.7 that

$$\mathrm{Z}(G) = \left\langle b_1^{p^m}, b_2^{p^m}, b_2^{-p^{m-o_1}} a \right\rangle \quad \text{and} \quad \mathrm{Z}(H) = \left\langle b_1^{p^m}, b_2^{p^m}, b_1^{p^{m-1}} b_2^{-p^{m-o_1}} a \right\rangle$$

and therefore we also have

$$\mathrm{Z}(G)/\mathrm{Z}(G) \cap G' \cong \mathrm{Z}(G)G'/G' = \left\langle b_1^{p^m} G' \right\rangle \times \left\langle b_2^{p^{m-o_1}} G' \right\rangle \cong \mathrm{C}_{p^{n_1-m}} \times \mathrm{C}_{p^{n_2-m+o_1}},$$

$$\mathrm{Z}(H)/\mathrm{Z}(H) \cap H' \cong \mathrm{Z}(H)H'/H' = \left\langle b_1^{p^{m-1}} b_2^{p^{m-o_1}} G' \right\rangle \times \left\langle b_2^{p^{m-o_1+1}} G' \right\rangle \cong \mathrm{C}_{p^{n_1-m+1}} \times \mathrm{C}_{p^{n_2-m+o_1-1}}.$$

As $o_1 \leq n_1 - n_2$, the exponent of $\mathrm{Z}(G)/\mathrm{Z}(G) \cap G'$ is $n_1 - m$, and the exponent of $\mathrm{Z}(H)/\mathrm{Z}(H) \cap H'$ is $n_1 - m + 1$. This concludes the proof.

□

In light of Lemma 4.3, until the end of the section we write $o^G = o^H = (o_1, o_2)$.

Lemma 4.4 *One has $o'^G = o'^H$.*

Proof By means of contradiction we assume that $o'^G \neq o'^H$ and without loss of generality we also assume that $o'^G <_{\text{lex}} o'^H$. In particular $G \not\cong H$ and hence Proposition 2.3(3)(b) yields that G and H are not metacyclic. It follows that $\max(o_1'^G, o_2'^G, o_1'^H, o_2'^H) < m$ and, as a consequence of Lemma 3.9 and Eq. 4.2, one of the following holds:

(1) $o_2'^H = o_2'^G + 1$ and exactly one of the following holds:

$$(a)\ o_2'^G = 0, \quad (b)\ o_2 = 0,\ n_1 - n_2 < o_1 \text{ and } o_2'^G = o_1'^G + n_1 - n_2 - o_1.$$

(2) $o_1'^H = o_1'^G + 1$ and exactly one of the following holds:

$$(a)\ o_1'^G = 0, \quad (b)\ o_1 = 0,\ 0 < \min(o_1'^G, o_2) \text{ and } o_2'^G = o_1'^G + o_2 + n_1 - n_2.$$

<u>Claim</u>: We can write $\{i, j\} = \{1, 2\}$ with $0 = o_i < o_j$, $o'_j = o_j'^G = o_j'^H$ and $o_i'^G + 1 = o_i'^H$. Moreover, if $i = 2$, we have that $n_1 - n_2 < o_1$.

We prove the claim separately for cases (1) and (2). More precisely, in case (1) we will prove the claim with $i = 2$ and $j = 1$ and in case (2) we prove the claim with $i = 1$ and $j = 2$.

We first show that $o_1'^G = o_1'^H$. By Proposition 2.3(2)(b) we have $\exp(G) = \exp(H)$ and so Lemma 3.5(2) yields that

$$\max(n_1 + o_1'^G, n_2 + o_2'^G) = \max(n_1 + o_1'^H, n_2 + o_2'^H) = \max(n_1 + o_1'^H, n_2 + o_2'^G + 1).$$

This implies that such maximum is $n_1 + o_1'^G = \max(n_1 + o_1'^H, n_2 + o_2'^G + 1) \geq n_1 + o_1'^H$. As $o'^G <_{\mathrm{lex}} o'^H$, it follows that $o_1'^G = o_1'^H$. Thus, if the claim fails, one necessarily has $o_2'^G = 0$ and hence $2m - o_1 + o_2'^G = 2m - o_1 > m$. From Theorem 3.1(4) we thus derive $m \leq n_2$. If $o_1'^G > 0$ then Theorem 3.1(3) yields $0 = o_2 < o_1$ and $n_1 - n_2 - o_1 < 0$. So, when $o_1'^G > 0$, the claim follows. Otherwise, that is if $o_1'^G = o_2'^G = 0$, we have $p^{n_2} \leq p^{n_1} = \exp(G) = \exp(H) = \max(p^{n_1}, p^{n_2+1})$ and therefore $n_1 \geq n_2 + 1$. Hence, using Lemma 3.5(3) and the fact that $(p^k - 2)(m - \max(o_1, o_2)) + n_2 - k \geq n_2 \geq m$ for $k \geq 1$, we have

$$\begin{aligned} \mathrm{D}_{p^{n_2}}(G) &= \left\langle b_1^{p^{n_2}} \right\rangle, & \mathrm{D}_{p^{n_2}}(H) &= \left\langle b_1^{p^{n_2}}, a^{p^{m-1}} \right\rangle, \\ \mathrm{D}_{p^{n_2}+1}(G) &= \left\langle b_1^{p^{n_2+1}} \right\rangle, & \mathrm{D}_{p^{n_2}+1}(H) &= \left\langle b_1^{p^{n_2+1}} \right\rangle. \end{aligned}$$

We obtain the following contradiction to Proposition 2.3(2)(c):

$$\mathrm{C}_p \cong \frac{\mathrm{D}_{p^{n_2}}(G)}{\mathrm{D}_{p^{n_2}+1}(G)} \cong \frac{\mathrm{D}_{p^{n_2}}(H)}{\mathrm{D}_{p^{n_2}+1}(H)} \cong \mathrm{C}_p \times \mathrm{C}_p.$$

Suppose now that (2) holds. If $o_2'^G \neq o_2'^H$ then, by Lemma 3.9, the hypotheses in (1) are satisfied and from the claim we obtain the contradiction $o_1'^G = o_1'^H = o_1'^G + 1$. Hence we have $o_2'^G = o_2'^H$. Therefore, if the claim fails, we necessarily have $o'^G = (0, o_2')$ and $o'^H = (1, o_2')$ and hence $p^{\max(n_1+1, n_2+o_2')} = \exp(H) = \exp(G) = p^{\max(n_1, n_2+o_2')}$. Therefore $n_1 + o_1'^G = n_1 < n_2 + o_2' = n_2 + o_2'^G$ and Theorem 3.1(3) yields $o_1 = 0$. It follows from $o^G \neq (0, 0)$ that $o_2 \neq 0$. This finishes the proof of the claim.

Combining the claim with Theorem 3.1(3) we deduce that $n_i + o_i'^G \geq n_j + o_j' - o_j$ and hence, applying (4) and (5) of Lemma 3.8 we have

$$\exp(\mathrm{C}_\Gamma(\Gamma')) = \begin{cases} p^{n_i + o_i'^G}, & \text{if } \Gamma = G; \\ p^{n_i + o_i'^G + 1}, & \text{if } \Gamma = H. \end{cases} \tag{4.3}$$

This yields a contradiction to Lemma 4.2. □

This completes the proof Theorem C. As a consequence, we set $o'^G = o'^H = (o_1', o_2')$ until the end of this section. The following is the same as Corollary D.

Corollary 4.5 *One has* $\mathrm{C}_G(G') \cong \mathrm{C}_H(H')$.

Proof By Theorem 4.2(b) we have $|\mathrm{D}_i(\mathrm{C}_G(G'))/\mathrm{D}_{i+1}(\mathrm{C}_G(G'))| = |\mathrm{D}_i(\mathrm{C}_G(H'))/\mathrm{D}_{i+1}(\mathrm{C}_H(H'))|$ for each $i \geq 1$, hence also $|\mathrm{D}_i(\mathrm{C}_G(G'))| = |\mathrm{D}_i(\mathrm{C}_H(H'))|$ for each $i \geq 1$. In order to prove the lemma we will write a presentation for a group Δ depending only on $p, m, n_1, n_2, o_1, o_2, o_1', o_2'$ and e, where $p^e = |\mathrm{D}_{p^{n_1 - o_1 + o_2}}(\mathrm{C}_\Gamma(\Gamma'))|$, and show that $\mathrm{C}_\Gamma(\Gamma') \cong \Delta$ for $\Gamma \in \{G, H\}$. We rely on the description of $C_\Gamma(\Gamma')$ given in Lemma 3.8(2) and analyze the different cases listed in Theorem 3.1(3).

Assume first that $o_1 = 0$. Then $\mathrm{C}_\Gamma(\Gamma') = \left\langle b_1, b_2^{p^{o_2}}, a \right\rangle$, and by Eq. 3.8 and Lemma 2.1(2) we have $[b_2^{u_1^\Gamma p^{o_2}}, b_1] = a^{u_1^\Gamma p^{o_2}}$. Defining

$$\Delta = \left\langle x, y, z \mid [y, x] = z^{p^{o_2}}, [z, x] = [z, y] = 1, x^{p^{n_1}} = z^{p^{m-o'_1}}, y^{p^{n_2-o_2}} = z^{p^{m-o'_2}}, z^{p^m} = 1 \right\rangle,$$

the assignment $(x, y, z) \mapsto (b_1^{u_2^\Gamma}, b_2^{u_1^\Gamma p^{o_2}}, a^{u_1^\Gamma u_2^\Gamma})$ extend to an isomorphism $\Delta \to \mathrm{C}_\Gamma(\Gamma')$.

Next assume that $o_2 = 0 < o_1$, so that $\mathrm{C}_\Gamma(\Gamma') = \left\langle b_1^{p^{o_1}}, b_2, a \right\rangle$. Set

$$\Delta = \left\langle x, y, z \mid [y, x] = z^{p^{o_1}}, [z, x] = [z, y] = 1, x^{p^{n_1-o_1}} = z^{p^{m-o'_1}}, y^{p^{n_2}} = z^{p^{m-o'_2}}, z^{p^m} = 1 \right\rangle.$$

Then the assignment $(x, y, z) \mapsto (b_1^{u_2^\Gamma p^{o_1}}, b_2^{u_1^\Gamma}, a^{u_1^\Gamma u_2^\Gamma})$ induces an isomorphism $\Delta \to \mathrm{C}_\Gamma(\Gamma')$.

Finally assume that $o_1 o_2 > 0$. Then $o_2 < o_1 < o_2 + n_1 - n_2$ and $o'_1 \leq o'_2 \leq o'_1 + n_1 - n_2$, and we also have

$$\mathrm{C}_\Gamma(\Gamma') = \left\langle b_1^{p^{o_1}}, b_1^{p^{o_1-o_2}} b_2^{-1}, a \right\rangle = \left\langle b_1^{p^{o_1-o_2}} b_2^{-1}, b_2^{p^{o_2}}, a \right\rangle.$$

Let r' be an integer such that $r_2 r' \equiv 1 \mod p^m$. By the definition of r_2 in Eq. 3.1 we have $r' \equiv 1 \mod p^{m-o_2}$ and, as $o_1 > o_2$, we also have $r' \equiv 1 \mod p^{m-o_1}$. Applying Eq. 3.9 we get $[b_2, b_1^{p^{o_1-o_2}} b_2^{-1}] = a^{r' \mathcal{S}(r_1 | p^{o_1-o_2})}$ and, as a consequence, that $[b_2^{p^{o_2}}, b_1^{p^{o_1-o_2}} b_2^{-1}] = a^{r' \mathcal{S}(r_1 | p^{o_1-o_2}) \mathcal{S}(r_2 | p^{o_2})}$. From Lemma 2.1(1)-(2) and $r' \equiv 1 \mod p^{m-o_1}$ we derive $r' \mathcal{S}\left(r_1 \mid p^{o_1-o_2}\right) \mathcal{S}\left(r_2 \mid p^{o_2}\right) \equiv r' p^{o_1} \equiv p^{o_1} \mod p^m$, from which it follows that $[b_2^{p^{o_2}}, b_1^{p^{o_1-o_2}} b_2^{-1}] = a^{p^{o_1}}$. As $C_G(G')$ is of class at most 2, we have moreover that

$$[b_2^{d p^{o_2}}, (b_1^{p^{o_1-o_2}} b_2^{-1})^e] = a^{p^{o_1} de}, \quad \text{for every } d, e \in \mathbb{Z}. \tag{4.4}$$

We construct different Δ's depending on whether $s = n_1 + o'_1 - n_2 - o'_2 - o_1 + o_2$ is positive, negative or zero.

Suppose $s > 0$ and take $\alpha^\Gamma = u_1^\Gamma - u_2^\Gamma p^s$ and

$$\Delta = \left\langle x, y, z \mid [y, x] = z^{p^{o_1}}, [z, x] = [z, y] = 1, x^{p^{n_1-o_1+o_2}} = z^{p^{m-o'_1}}, y^{p^{n_2-o_2}} = z^{p^{m-o'_2}}, z^{p^m} = 1 \right\rangle.$$

Define additionally We claim that the homomorphism $f_\Gamma : \Delta \to \mathrm{C}_\Gamma(\Gamma')$ that is defined by

$$x \mapsto x_1 := (b_1^{p^{o_1-o_2}} b_2^{-1})^{u_2^\Gamma}, \quad y \mapsto y_1 := b_2^{\alpha^\Gamma p^{o_2}}, \quad z \mapsto z_1 := a^{\alpha^\Gamma u_2^\Gamma}$$

is in fact an isomorphism. Indeed, both a and z have order p^m and $\mathrm{C}_\Gamma(\Gamma') / \langle a \rangle \cong \Delta / \langle z \rangle \cong C_{p^{n_1-o_1+o_2}} \times C_{p^{n_2-o_2}}$, so to prove that f_Γ is an isomorphism we check that x_1, y_1 and z_1 satisfy the relations of Δ. It is clear that $[z_1, x_1] = [z_1, y_1] = 1$ and regularity grants that $x_1^{p^{n_1-o_1+o_2}} = z_1^{p^{m-o'_1}}$ and $y_1^{p^{n_2-o_2}} = z_1^{p^{m-o'_2}}$. The last relation follows from Eq. 4.4.

In case $s < 0$ we take $\alpha^\Gamma = u_1^\Gamma p^s - u_2^\Gamma$,

$$\Delta = \left\langle x, y, z \mid [y, x] = z^{p^{o_1}}, [z, x] = [z, y] = 1, x^{p^{n_1-o_1+o_2}} = z^{p^{m-o'_1+s}}, y^{p^{n_2-o_2}} = z^{p^{m-o'_2}}, z^{p^m} = 1 \right\rangle,$$

and f_Γ defined as in the previous paragraph. The same argument shows that f_Γ is a group isomorphism.

Finally suppose that $s = 0$ and factorize $u_1^\Gamma - u_2^\Gamma = w^\Gamma p^{\ell^\Gamma}$ with w^Γ coprime to p. Observe that (w^G, ℓ^G) and (w^H, ℓ^H) might be different, nonetheless the following hold:

$$p^e = |\mathrm{D}_{p^{n_1-o_1+o_2}}(\mathrm{C}_\Gamma(\Gamma'))| = |\mho_{n_1-o_1+o_2}(\mathrm{C}_\Gamma(\Gamma'))| = \left|\left\langle a^{p^{\min\{m-o_1'+\ell^\Gamma, m-o_1'+o_2, n_1-o_1+o_2\}}}\right\rangle\right|.$$

As a result, $e = \max\{o_1' - \ell^\Gamma, o_1' - o_2, m - n_1 + o_1 - o_2, 0\}$ is independent of $\Gamma \in \{G, H\}$. We now give contructions of Δ depending on the value of e.

Assume that $e = \max\{o_1' - o_2, m - n_1 + o_1 - o_2, 0\}$. We set

$$\Delta = \left\langle x, y, z \mid [y, x] = z^{p^{o_1}}, [z, x] = [z, y] = 1, x^{p^{n_1-o_1+o_2}} = 1, y^{p^{n_2-o_2}} = z^{p^{m-o_2'}}, z^{p^m} = 1\right\rangle$$

and select an integer v such that $vu_2^\Gamma \equiv 1 \mod p^m$. Then we obtain an isomorphism $\Delta \to \mathrm{C}_\Gamma(\Gamma')$ by assigning $y \mapsto b_2^{u_1^\Gamma p^{o_2}}$, $z \mapsto a^{u_1^\Gamma u_2^\Gamma}$ and

$$x \mapsto \begin{cases} (b_1^{p^{o_1-o_2}} b_2^{-1})^{u_2^\Gamma}, & \text{if } e = 0; \\ (b_1^{p^{o_1-o_2}} b_2^{-1} a^{-w^\Gamma p^{m-o_1'-n_1+\ell^\Gamma+o_1-o_2}})^{u_2^\Gamma}, & \text{if } e = m - n_1 + o_1 - o_2; \\ (b_1^{p^{o_1-o_2}} b_2^{-1+(u_2^\Gamma - u_1^\Gamma)v})^{u_2^\Gamma}, & \text{if } e = o_1' - o_2. \end{cases}$$

Otherwise assume $e = o_1' - \ell^\Gamma > \max\{o_1' - o_2, m - n_1 + o_1 - o_2, 0\}$ and we take

$$\Delta = \left\langle x, y, z \mid [y, x] = z^{p^{o_1}}, [z, x] = [z, y] = 1, x^{p^{n_1-o_1+o_2}} = z^{p^{m-e}}, y^{p^{n_2-o_2}} = z^{p^{m-o_2'}}, z^{p^m} = 1\right\rangle.$$

Slightly modifying the arguments from the previous paragraph, one easily shows that

$$x \mapsto (b_1^{p^{o_1-o_2}} b_2^{-1})^{u_2^\Gamma}, \quad y \mapsto b_2^{w^\Gamma p^{o_2}}, \quad \text{and} \quad z \mapsto a^{w^\Gamma u_2^\Gamma}$$

determines an isomorphism $\Delta \to \mathrm{C}_\Gamma(\Gamma')$. □

The following result is the same as Corollary E.

Corollary 4.6 *The groups G and H have the same type invariants.*

Proof We will express the type invariants solely in terms of $(p, m, n_1, n_2, o_1, o_2, o_1', o_2')$. The corollary then will follow from Theorem C. The discussion after [44, Theorem 3.1] guarantees, for $\Gamma \in \{G, H\}$, that $\omega(\Gamma) \in \{2, 3\}$ and, moreover, $\omega(\Gamma) = 2$ if and only if Γ is metacyclic, that is if $\max\{o_1', o_2'\} = m$. In view of Proposition 2.3(3)(b) we assume without loss of generality that $\omega(\Gamma) = 3$. In this situation, as indicated in [44], the type invariants satisfy the following properties:

$$\exp(\Gamma) = p^{e_1^\Gamma}, \quad |\Gamma| = p^{e_1^\Gamma + e_2^\Gamma + e_3^\Gamma} \quad \text{and} \quad p^{e_3^\Gamma} = \min\{|g| : g \in \Phi(\Gamma) \setminus \mho_1(\Gamma)\}. \quad (4.5)$$

where $\Phi(\Gamma) = \langle b_1^p, b_2^p, a \rangle$ is the Frattini subgroup of Γ and e_i^Γ denotes the i-th type invariant of Γ. We claim that the type invariants are given by the following formulae:

$$\begin{aligned} e_1^\Gamma &= \max(n_1 + o_1', n_2 + o_2'), \\ e_2^\Gamma &= n_1 + n_2 + \max(o_1', o_2') - \max(n_1 + o_1', n_2 + o_2'), \\ e_3^\Gamma &= m - \max(o_1', o_2'). \end{aligned} \tag{4.6}$$

Indeed, by Lemma 3.5(2) the exponent of G is $p^{\max(n_1+o_1',n_2+o_2')}$, so Eq. 4.5 yields the first equality. Moreover the order of G is both $p^{e_1^\Gamma+e_2^\Gamma+e_3^\Gamma}$ and $p^{m+n_1+n_2}$. Therefore it is enough to prove that $e_3^\Gamma = m - \max(o_1', o_2')$. For this, let g in $\Phi(\Gamma) \setminus \mho_1(\Gamma)$. Then $g = b_1^{xp^{s_1}} b_2^{yp^{s_2}} a^z$, with $1 \leq \min\{s_1, s_2\}$ and p does not divide zxy. Conversely, every element of such form belongs to $\Phi(\Gamma) \setminus \mho_1(\Gamma)$. Thanks to Eq. 3.6, if $p^N \geq |g|$ then

$$1 = (b_1^{xp^{s_1}} b_2^{yp^{s_2}} a^z)^{p^N} = b_1^{xp^{s_1+N}} b_2^{yp^{s_2+N}} a^{\mathcal{S}(r_1|xp^{s_1})\mathcal{S}(r_2|yp^{s_2})\mathcal{T}\left(r_1^{xp^{s_1}},r_2^{yp^{s_2}}|p^N\right)+z\mathcal{S}\left(r_1^{xp^{s_1}}r_2^{yp^{s_2}}|p^N\right)}. \tag{4.7}$$

Then $s_i + N \geq n_i$ for $i = 1, 2$ and, as $n_1 \geq m$, Lemma 2.1(1)-(3) yields

$$v_p\left(\mathcal{S}\left(r_1 \mid xp^{s_1}\right)\mathcal{T}\left(r_1^{xp^{s_1}}, r_2^{yp^{s_2}} \mid p^N\right)\right) \geq s_1 + N \geq n_1 \geq m \quad \text{and} \quad v_p\left(z\mathcal{S}\left(r_1^{xp^{s_1}} r_2^{yp^{s_2}} \mid p^N\right)\right) = N.$$

So $\mathcal{S}\left(r_1^{xp^{s_1}} r_2^{yp^{s_2}} \mid p^N\right) = Ap^N$, for some integer $A = A(x, y, s_1, s_2)$, with p not dividing A. Hence Eq. 4.7 can be rewritten as

$$1 = a^{xu_1^\Gamma p^{s_1+N-n_1+m-o'_1}+yu_2^\Gamma p^{s_2+N-n_2+m-o'_2}+zAp^N}$$

and e_3^Γ is the minimum value of N such that there are integers x, y, z, s_1 and s_2 satisfying

$$\begin{aligned} &p \nmid xyz, \quad 1 \leq s_i \quad s_i + N \geq n_i, \quad \text{and} \\ &xu_1^\Gamma p^{s_1+N-n_1+m-o_1'} + yu_2^\Gamma p^{s_2+N-n_2+m-o_2'} + zAp^N \equiv 0 \mod p^m. \end{aligned} \tag{4.8}$$

If $N \geq m$ then the conditions hold trivially taking s_1 and s_2 large enough, so we look for values $N < m$. Then $zAp^N \not\equiv 0 \mod p^m$ and hence s_1 and s_2 should be taken satisfying one of the following conditions:

$$(1)\, s_1 = n_1 + o_1' - m, \quad (2)\, s_2 = n_2 + o_2' - m, \quad (3)\, m < n_1 + o_1' - s_1 = n_2 + o_2' - s_2.$$

In the three cases $n_i \leq s_i + N \leq n_i + o_i' - m + N$ and hence $N \geq m - o_i'$. This shows that

$$N \geq \min(m - o_1', m - o_2') = m - \max(o_1', o_2')$$

and hence, in view of the above we assume that $\max(o_1', o_2') > 0$. It now suffices to prove that, for $N = m - \max(o_1', o_2')$, there exists integers x, y, z, s_1 and s_2 satisfying Eq. 4.8. From $N < m$ we conclude that $\max(o_1', o_2') > 0$. We note, moreover that $n_i + o_i' \geq m$. Indeed, if this weren't the case, we would have $n_i < m$ and, applying Theorem 3.1(2)-(4), that $i = 2$ and $n_2 = 2m - o_1 - o_2' > m - o_2'$. If $o_1' \geq o_2'$ then the following integers satisfy Eq. 4.8:

$$N = m - o_1', \quad s_1 = n_1 + o_1' - m = n_i - N > 0, \quad s_2 = n_2 + o_2' \geq m, \quad x = -1, \quad y = 1, \quad z = Bu_1$$

with B an integer such that $AB \equiv 1 \mod p^m$. Otherwise $o_2' > o_1'$ and a symmetric argument shows that for $N = m - o_2'$ the integers

$$x = 1, \quad y = -1, \quad s_1 = n_1 + o_1' \geq m, \quad s_2 = n_2 - m + o_2' = n_2 - N > 0, \quad z = Bu_2$$

satisfy Eq. 4.8. This finishes the proof of Eq. 4.6 and hence also of the corollary. □

Author Contributions All the authors contributed evenly to the paper.

Funding Open Access funding provided thanks to the CRUE-CSIC agreement with Springer Nature. The first two authors are partially supported by Grant PID2020-113206GB-I00 funded by MCIN/AEI/10.13039/501100011033. The third author is supported by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – Project-ID 286237555 – TRR 195.

Availability of data and materials Not applicable.

Declarations

Ethical Approval Not applicable.

Competing interests No financial or personal competing interest.

References

1. Bagiński, C.: The isomorphism question for modular group algebras of metacyclic p-groups. Proc. Amer. Math. Soc. **104**(1), 39–42 (1988)
2. Bagiński, C.: On the isomorphism problem for modular group algebras of elementary abelian-by-cyclic p-groups. Colloq. Math. **82**(1), 125–136 (1999)
3. Bagiński, C., Caranti, A.: The modular group algebras of p-groups of maximal class. Canad. J. Math. **40**(6), 1422–1435 (1988)
4. Broche, O., del Río, Á.: The Modular Isomorphism Problem for two generated groups of class two. Indian J. Pure Appl. Math. **52**, 721–728 (2021)
5. Broche, O., García-Lucas, D., del Río, Á.: A classification of the finite two-generated cyclic-by-abelian groups of prime power order, arXiv:2106.06449
6. Bagiński, C., Konovalov, A.: The modular isomorphism problem for finite p-groups with a cyclic subgroup of index p^2, Groups St. Andrews2005. Vol. 1, London Math. Soc. Lecture Note Ser., vol. 339, Cambridge Univ. Press, Cambridge, pp. 186–193 (2007)
7. Bleher, F.M., Kimmerle, W., Roggenkamp, K.W., Wursthorn, M.: Computational Aspects of the Isomorphism Problem, Algorithmic Algebra and Number Theory (Heidelberg, 1997), pp. 313–329. Springer, Berlin (1999)
8. Brauer, R.: Representations of Finite Groups, Lectures on Modern Mathematics, vol. I, pp. 133–175. Wiley, N. Y. (1963)
9. Cheng, Y.: On finite p-groups with cyclic commutator subgroup. Arch. Math. **39**(4), 295–298 (1982)
10. Curtis, C.h.W., Reiner, I.: Methods of Representation Theory, vol. I. Wiley, New York (1981). With applications to finite groups and orders, Pure and Applied Mathematics, A Wiley-Interscience Publication. MR 632548 (82i:20001)
11. Curtis, C.h.W., Reiner, I.: Methods of Representation Theory, vol. II. Pure and Applied Mathematics (New York). Wiley, New York (1987). With applications to finite groups and orders, A Wiley-Interscience Publication, MR 892316 (88f:20002)
12. Dade, E.: Deux groupes finis distincts ayant la même algèbre de groupe sur tout corps. Math. Z. **119**, 345–348 (1971)
13. Deskins, W.E.: Finite Abelian groups with isomorphic group algebras. Duke Math. J. **23**, 35–40 (1956). MR 77535

14. Eick, B.: Computing automorphism groups and testing isomorphisms for modular group algebras. J. Algebra **320**(11), 3895–3910 (2008)
15. Eick, B., Konovalov, A.: The modular isomorphism problem for the groups of order 512, Groups St Andrews 2009 in Bath. Volume 2, London, Math. Soc. Lecture Note Ser., vol. 388, Cambridge Univ. Press, Cambridge, pp. 375–383 (2011)
16. García-Lucas, D., Margolis, L., del Río, Á.: Non-isomorphic 2-groups with isomorphic modular group algebras. J. Reine Angew. Math. **154**(783), 269–274 (2022)
17. Hertweck, M.: A counterexample to the isomorphism problem for integral group rings. Ann. Math. (2) **154**(1), 115–138 (2001)
18. Higman, G.: The units of group-rings. Proc. London Math. Soc. (2) **46**, 231–248 (1940)
19. Hertweck, M., Soriano, M.: On the modular isomorphism problem: Groups of order 2^6. Groups, rings and algebras. Contemp. Math., vol. 420, pp. 177–213. Amer. Math. Soc., Providence (2006)
20. Hertweck, M., Soriano, M.: Parametrization of central Frattini extensions and isomorphisms of small group rings. Israel J. Math. **157**, 63–102 (2007)
21. Huppert, B.: Endliche Gruppen I. Die Grundlehren der Mathematischen Wissenschaften Band, vol. 134. Springer, Berlin (1967)
22. Jennings, S.A.: The structure of the group ring of a p-group over a modular field. Trans. Amer. Math. Soc. **50**, 175–185 (1941)
23. Külshammer, B.: Bemerkungen über die Gruppenalgebra als symmetrische Algebra II. J. Algebra **75**(1), 59–69 (1982)
24. Kimmerle, W.: Beiträge zur ganzzahligen Darstellungstheorie endlicher Gruppen. Bayreuth Math. Schr. **36**, 139 (1991)
25. Makasikis, A.: Sur l'isomorphie d'algèbres de groupes sur un champ modulaire. Bull. Soc. Math. Belg. **28**(2), 91–109 (1976). MR 561324
26. Margolis, L.: The Modular Isomorphism Problem: A Survey, Jahresber. Dtsch. Math Ver (2022)
27. Margolis, L., Moede, T.: The Modular Isomorphism Problem for small groups – revisiting Eick's algorithm. arXiv:2010.07030
28. Margolis, L., Stanojkovski, M.: On the modular isomorphism problem for groups of class 3 and obelisks. J. Group Theory **25**(1), 163–206 (2022)
29. Margolis, L., Stanojkovski, M., Sakurai, T.: Abelian invariants and a reduction theorem for the modular isomorphism problem, arXiv:2110.10025
30. Navarro, G., Sambale, B.: On the blockwise modular isomorphism problem. Manuscripta Math. **157**(1–2), 263–278 (2018)
31. Passman, D.S.: Isomorphic groups and group rings. Pacific J. Math. **15**, 561–583 (1965)
32. Passman, D.S.: The Algebraic Structure of Group Rings, Pure and Applied Mathematics. Wiley-Interscience [John Wiley & Sons], New York-London-Sydney (1977)
33. Perlis, S., Walker, G.L.: Abelian group algebras of finite order. Trans. Amer. Math. Soc. **68**, 420–426 (1950)
34. Quillen, D.G.: On the associated graded ring of a group ring. J. Algebra **10**, 411–418 (1968)
35. Roggenkamp, K.W., Scott, L.: Isomorphisms of p-adic group rings. Ann. of Math. (2) **126**(3), 593–647 (1987)
36. Sakurai, T.: The isomorphism problem for group algebras: A criterion. J. Group Theory **23**(3), 435–445 (2020)
37. Salim, A.M.M.: The Isomorphism Problem for the Modular Group Algebras of Groups of Order p^5. ProQuest LLC, Ann Arbor (1993). Thesis (Ph.D.)–University of Manchester
38. Sandling, R.: Units in the modular group algebra of a finite abelian p-group. J. Pure Appl. Algebra **33**(3), 337–346 (1984)
39. Sandling, R.: The Isomorphism Problem for Group Rings: A survey, Orders and their Applications (Oberwolfach, 1984), Lecture Notes in Math., vol. 1142, pp. 256–288. Springer, Berlin (1985)
40. Sandling, R.: The modular group algebra of a central-elementary-by-abelian p-group. Arch. Math. (Basel) **52**(1), 22–27 (1989)
41. Sandling, R.: The modular group algebra problem for metacyclic p-groups. Proc. Amer. Math. Soc. **124**(5), 1347–1350 (1996)
42. Sehgal, S.K.: On the isomorphism of group algebras. Math. Z. **95**, 71–75 (1967)
43. Sehgal, S.K.: Topics in group rings. Monographs and Textbooks in Pure and Applied Math., vol. 50. Marcel Dekker, Inc., New York (1978)
44. Song, Q.: Finite two-generator p-subgrous with cyclic derived group. Comm. Algebra **41**(4), 1499–1513 (2013)
45. Salim, M.A.M., Sandling, R.: The unit group of the modular small group algebra. Math. J. Okayama Univ. **37**(1995), 15–25 (1996)

46. Salim, M.A.M., Sandling, R.: The modular group algebra problem for groups of order p^5. J. Austral. Math. Soc. Ser. A **61**(2), 229–237 (1996)
47. Ward, H.N.: Some results on the group algebra of a p-group over a prime field, Seminar on finite groups and related topics., Mimeographed notes, Harvard Univ., pp. 13–19 (1960)
48. Whitcomb, A.: The Group Ring Problem. Thesis (Ph.D.)–The University of Chicago, Ann Arbor (1968)
49. Wursthorn, M.: Isomorphisms of modular group algebras: An algorithm and its application to groups of order 2^6. J. Symbolic Comput. **15**(2), 211–227 (1993). MR 1218760

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.