

On the modular isomorphism problem for groups of class 3 and obelisks

Leo Margolis and Mima Stanojkovski*

Communicated by Bettina Eick

Abstract. We study the Modular Isomorphism Problem applying a combination of existing and new techniques. We make use of the small group algebra to give a positive answer for two classes of groups of nilpotency class 3. We also introduce a new approach to derive properties of the lower central series of a finite p -group from the structure of the associated modular group algebra. Finally, we study the class of so-called p -obelisks which are highlighted by recent computer-aided investigations of the problem.

1 Introduction

The question of how strongly the group ring RG of a group G over a commutative ring R dictates the structure of G is still far from being well-understood. The most classical version of this problem that is still open today, in its full generality, can be stated as follows.

Modular Isomorphism Problem (MIP). Let k be a field of characteristic $p > 0$, and let G be a finite p -group. Let H be another group. Does a ring isomorphism between kG and kH imply a group isomorphism between G and H ? In symbols,

$$kG \cong kH \implies G \cong H?$$

If H is a subgroup of the unit group of kG such that $kG = kH$, then H is said to be a *group base* of kG . The (MIP) can thus be reformulated as follows: are all group bases of a modular group algebra of a finite p -group isomorphic?

An explicit formulation of the (MIP) can already be found in a famous survey of Brauer [8]. Since then, the problem has been studied by many researchers; we refer to [13, 14] for an overview of most known results. New points of view and

This research has been partially supported by the FWO (Research Foundation Flanders) and CIRM-FBK Trento in connection to their Research in Pairs Program.

approaches to the problem can be found in the very recent papers [4, 9, 20, 24]. We study the (MIP) for certain classes of groups, inspired by some of these recent results and accessing the problem from different directions.

We start by recalling the construction of the so-called small group algebra of kG and its employment in the study of the (MIP); among its biggest merits are Sandling's positive solution of the (MIP) for groups with central elementary abelian derived subgroup [30] and Salim and Sandling's solution for groups of order p^5 (see [27]).

We use the small group algebra to positively solve the (MIP) for two new classes of groups, cf. Theorem 3.3 and Theorem 3.5. In particular, for p odd, our work completely covers 5 of 43 isoclinism classes of groups of order p^6 , while 10 other classes are covered by known results. We also show that the strategy of Salim and Sandling for groups of order p^5 is not directly translatable to groups of order p^6 by exhibiting a pair of non-isomorphic groups, of class 3 and with elementary abelian derived subgroups, whose small group algebras have isomorphic groups of units, cf. Example 3.11. We believe that the methods used to prove Theorems 3.3 and 3.5 can be applied to other families of groups with maximal subgroups of relatively small class.

We continue our investigation with the determination of a new invariant for certain 2-generated groups of class 3. In relation to this, we stress that, though the lower central series is a fundamental object in the study of finite p -groups, it is still quite unclear which properties of it are detected by the group algebra. For instance, it is not known in general whether group bases for the same algebra have the same nilpotency class, and even if they did, it is not known whether corresponding elements of the lower central series are isomorphic. Moreover, [4, Example 2.1] makes it clear that the ideals corresponding to the lower central series in kG are not canonical, and thus they are probably not the best candidates for recognizing the lower central series of the group. Via new quotient-in-quotient embedding techniques, we show that, for certain 2-generated groups of nilpotency class 3, the isomorphism types of the members of the lower central series of any group base are determined by kG , cf. Theorem 4.1. With the aid of computer algebra systems, it can be checked that the last theorem does not follow from known results on the (MIP), contributing to the mystery around the connection between the lower central series of the group and the Lie structure of the modular group algebra.

We conclude the present paper with the study of the (MIP) for a family of groups called p -obelisks. These groups are highlighted in computer-aided investigations for groups of order 5^6 (see [20]) and, in some sense, are among the groups of order 5^6 that are "closest" to being counterexamples to the (MIP). We show that if $kG \cong kH$ and G is a p -obelisk, then so is H , cf. Theorem 5.3.

2 Preliminaries and notation

Throughout the article, the following assumptions will hold. Let p be a prime number. We denote by G a p -group and by k the field of p elements. The (modular) group algebra of G over k is denoted by kG . Note that this provides the most general situation for the (MIP); indeed, for any field extension F/k , an isomorphism $kG \cong kH$ induces, via extension of scalars, an isomorphism $FG \cong FH$.

2.1 Group theoretical notions

We denote the order of an element $g \in G$ by $|g|$ and the order of G by $|G|$. The index of a subgroup X in G is denoted by $|G : X|$. The lower central series of G is denoted by $(\gamma_i(G))_{i \geq 1}$ and its upper central series by $(Z_i(G))_{i \geq 1}$. We write $Z(G)$ instead of $Z_1(G)$ for the center of G . We write, moreover, $\Phi(G)$ for the Frattini subgroup of G . We define

$$\mu_p(G) = \langle x \in G \mid x^p = 1 \rangle \quad \text{and} \quad G^p = \langle x^p \mid x \in G \rangle.$$

In this paper, conjugation is considered to be a *right* action, and consequently, commutators are defined and grouped in the following way. For $x, y, z \in G$, we set

$$[x, y] = x^{-1}y^{-1}xy \quad \text{and} \quad [x, y, z] = [[x, y], z].$$

For the convenience of the reader, we include the well-known commutator formulas; see for example [16, III, 1.2 Hilfssatz].

Lemma 2.1. *Let X be a group. For elements $a, b, c \in X$, the following hold:*

$$[a, bc] = [a, c][a, b]^c \quad \text{and} \quad [ab, c] = [a, c]^b[b, c].$$

Given the special role that the subgroup $Z(G) \cap \gamma_2(G)$ will play for us, we associate to it the non-standard notation $\Gamma(G) = Z(G) \cap \gamma_2(G)$.

When considering explicit examples, we will refer to the Small Groups Library in GAP [5, 34] and will denote by $SG(n, m)$ the m -th group of order n in the catalog.

2.2 Algebra notions

Until the end of Section 2.2, let \mathbb{A} be a k -algebra with fixed k -basis \mathcal{B} . An element $b \in \mathcal{B}$ is said to be *in the support of* an element $a \in \mathbb{A}$ if the image of a under the natural projection $\mathbb{A} \rightarrow kb$ is non-zero.

The algebra \mathbb{A} has a natural Lie algebra structure via defining, for all $a, b \in \mathbb{A}$, Lie brackets as $[a, b] = ab - ba$. Given any two subsets X, Y of \mathbb{A} , denote by

$[X, Y]$ the set of all elements $[x, y]$ with $x \in X$ and $y \in Y$. If \mathbb{A} is a local algebra, we denote, moreover, by $V(\mathbb{A})$ the elements of \mathbb{A} which map to the identity modulo the radical of \mathbb{A} . In case \mathbb{A} is equal to kG or one of its quotients, $V(\mathbb{A})$ is usually called the *group of normalized units* of \mathbb{A} .

For each element $g \in G$, write $\bar{g} = g - 1 \in kG$, and for each subset X of G , write \overline{X} for the set $\{\bar{x} \mid x \in X\}$. Then kG is a local algebra whose radical coincides with the *augmentation ideal*

$$I(kG) = V(kG) - 1 = \left\{ \sum_{g \in G} \lambda_g g \mid \lambda_g \in k, \sum_{g \in G} \lambda_g = 0 \right\},$$

which is easily seen to be generated, as a kG -ideal, by the elements \bar{g} as g varies in G . The augmentation ideal is a nilpotent ideal of kG , and hence, for every element $x \in I(kG)$ different from 0, there exists a minimal number w such that $x \in I(kG)^w \setminus I(kG)^{w+1}$. This minimal w is called the *weight* of x in kG , written $\text{wt}(x) = w$. We define, additionally, the *weight* of an element $g \in G$ to be the weight of \bar{g} in kG , i.e. $\text{wt}(g) = \text{wt}(\bar{g})$.

The next lemma collects some straightforward equalities holding in $I(kG)$.

Lemma 2.2. *Let $g, h \in G$. Then the following hold:*

$$\begin{aligned} \overline{gh} &= \bar{g} + \bar{h} + \bar{g}\bar{h}, \\ \bar{h}\bar{g} &= \bar{g}\bar{h} + (1 + \bar{g} + \bar{h} + \bar{g}\bar{h})\overline{[h, g]}. \end{aligned}$$

We conclude this section by observing that

$$kGI(k\gamma_2(G)) = \langle x \cdot y \mid x \in kG, y \in I(k\gamma_2(G)) \rangle_{kG},$$

the ideal of kG that is generated by the elements of $I(k\gamma_2(G))$, is minimal among the ideals J of kG such that the quotient kG/J is commutative [29, Lemma 3.5].

2.3 Jennings theory

Many attempts at tackling the (MIP) rely, in one way or the other, on the theory of Jennings [19] providing a k -basis of $I(kG)$ that is well-suited for calculations in a way that we now explain. For more detail, we refer the reader to [11, 14].

The *dimension subgroups* of G are defined, for each positive integer n , by

$$D_n(G) = G \cap (1 + I(kG)^n)$$

and filter the elements of (the group base) G according to their weights, as defined in Section 2.2. A first characterization of the dimension subgroups was provided

by Jennings himself who showed that the series of dimension subgroups coincides with the Brauer–Jennings–Zassenhaus series, i.e. that

$$D_n(G) = \begin{cases} G & \text{if } n = 1, \\ [G, D_{n-1}(G)]D_{\lceil \frac{n}{p} \rceil}(G)^p & \text{if } n \geq 2. \end{cases}$$

Another celebrated characterization of the dimension subgroups of G is given in terms of the members of the lower central series and reads

$$D_n(G) = \prod_{i p^j \geq n} \gamma_i(G)^{p^j} = D_{\lceil \frac{n}{p} \rceil}(G)^p \gamma_n(G),$$

cf. [11, Theorem 11.2, Proposition 11.12]. From the last characterization, it follows that every quotient $D_n(G)/D_{n+1}(G)$ is elementary abelian and that, for each choice of m and n , one has

$$[D_m(G), D_n(G)] \subseteq D_{m+n}(G) \quad \text{and} \quad D_n(G)^p \subseteq D_{np}(G); \quad (2.1)$$

see for instance [11, Section 11.2]. In particular, the graded k -module

$$L(G) = \bigoplus_{n \geq 1} D_n(G)/D_{n+1}(G)$$

is naturally a restricted k -Lie algebra [11, Chapter 12].

For each positive integer n , it is not difficult to see, via the obvious maps, that $D_n(G)/D_{n+1}(G)$ embeds as a k -subspace of $I(kG)^n/I(kG)^{n+1}$. We derive that, if $g_1, \dots, g_m \in D_n(G)$ are such that their images in $D_n(G)/D_{n+1}(G)$ form a basis over k , then their images $\overline{g_1}, \dots, \overline{g_m} \in I(kG)^n$ are linearly independent over k when viewed in $I(kG)^n/I(kG)^{n+1}$. Additionally, the following hold:

$$\text{wt}(\overline{g}) = w \iff \text{wt}(g) = w \iff g \in D_w(G) \setminus D_{w+1}(G),$$

and as a consequence of (2.1), for each $x, y \in G$, one also has

$$\text{wt}([x, y]) \geq \text{wt}(x) + \text{wt}(y) \quad \text{and} \quad \text{wt}(x^p) \geq p \text{wt}(x).$$

We write $d_n = \dim_k D_n(G)/D_{n+1}(G)$ and let t be minimal with the property that $D_{t+1}(G) = 1$. Set $d_0 = 0$ and $m = d_1 + \dots + d_t = \log_p |G|$. A Jennings tuple is a tuple

$$(g_1, \dots, g_{d_1} \mid g_{d_1+1}, \dots, g_{d_1+d_2} \mid \dots \mid g_{m-d_t+1}, \dots, g_m)$$

of elements of G with the property that, for all $n \geq 0$,

$$g_{d_0+\dots+d_{n+1}} D_{n+2}(G), \dots, g_{d_0+\dots+d_{n+1}} D_{n+2}(G)$$

is a basis of $D_{n+1}(G)/D_{n+2}(G)$. It follows that any element g of G can be written uniquely as a product

$$g = \prod_{i=1}^m g_i^{\alpha_i}, \quad \text{with } 0 \leq \alpha_1, \dots, \alpha_m \leq p-1.$$

If (g_1, \dots, g_m) is a Jennings tuple of G , then the set

$$\left\{ \prod_{i=1}^m \bar{g}_i^{\alpha_i} \mid 0 \leq \alpha_1, \dots, \alpha_m \leq p-1 \right\}$$

forms a k -basis of $I(kG)$ which we refer to as the *Jennings basis* on (g_1, \dots, g_m) . A *Jennings basis* of $I(kG)$ is a k -basis of $I(kG)$ that can be defined on a Jennings tuple. Observe that any Jennings basis of $I(kG)$ can be extended to a k -basis of kG by adding the element 1. The advantage of working with a Jennings basis is that calculations can be translated directly from the relations of the group elements.

Now let $g \in G$. It is possible that multiple powers of G appear in a Jennings tuple of G . For instance, if G is cyclic and $g \notin \Phi(G)$, then $(g \mid g^p \mid \dots \mid g^{\exp(G)/p})$ is a Jennings tuple of G . For a Jennings tuple (g_1, \dots, g_m) , we say that \bar{g} is a *factor* of the element

$$y = \prod_{i=1}^m \bar{g}_i^{\alpha_i}, \quad \text{with } 0 \leq \alpha_1, \dots, \alpha_m \leq p-1,$$

if there exist non-negative integers i and j such that $g^{p^j} = g_i$ and $\alpha_i \neq 0$.

Another convenient feature of Jennings bases is that, in some cases, they can be constructed to “remember” the group structure. The following fact, which readily follows from the second formula in Lemma 2.2, will be useful to us. Let (c_1, \dots, c_m) be a Jennings tuple of $\gamma_2(G)$ such that the elements c_1, \dots, c_m are also elements of a Jennings tuple \mathbf{g} of G . Then, with respect to the Jennings basis on \mathbf{g} , an element $x \in I(kG)$ lies in the ideal $kGI(k\gamma_2(G))$ if and only if each element in the support of x contains a factor from $\{\bar{c}_1, \dots, \bar{c}_m\}$.

We conclude the current section by defining a class of ideals of kG that are strictly connected to the dimension subgroups of G . We define the *Zassenhaus ideals* of kG via their characterization, given by Passi and Segal in [22]: for each positive integer n , the n -th *Zassenhaus ideal* of kG is

$$H_n(kG) = \overline{D_n(G)} + I(kG)^{n+1}.$$

The Zassenhaus ideals are canonical ideals of kG , i.e. each $H_n(kG)$ can be defined independently of the group base of kG , cf. [14, Section 1.3]. Moreover, thanks to

their definition, Zassenhaus ideals allow us to isolate, within quotients of the form $I(kG)^n/I(kG)^{n+1}$, specific contributions of the chosen Jennings basis. More precisely, if U is the subspace of kG that is spanned by all elements of a Jennings basis of $I(kG)$ not lying in $\overline{G} = G - 1$, then, for each positive integer n , one has

$$I(kG)^n/I(kG)^{n+1} = H_n(kG)/I(kG)^{n+1} \\ \oplus (U \cap I(kG)^n + I(kG)^{n+1})/I(kG)^{n+1}.$$

For more on this, see for instance [14, Section 2.4].

2.4 Group theoretical invariants

One goal in the study of the (MIP) is to determine properties of G , the so-called *group theoretical invariants*, that can be derived from the structure of kG as an algebra. More precisely, if G and H are p -groups satisfying $kG \cong kH$ and \mathcal{P} is a group theoretical invariant, then both G and H will satisfy \mathcal{P} . The order of G is an obvious invariant, being the same as the k -dimension of kG . We will usually assume this invariant implicitly. Other invariants are collected in the following list. Many of them are classical, have been known for decades, and are included in [29, Section 6]. We only provide references for the ones not included in Sandling's survey.

- (1) The isomorphism type of the quotient $G/\gamma_2(G)$.
- (2) The isomorphism type of $G/\Phi(G)$ and hence the minimal number of generators of G .
- (3) The isomorphism type of the quotient $D_n(G)/D_{n+1}(G)$ for any positive integer n .
- (4) The isomorphism type of the quotient $D_n(\gamma_2(G))/D_{n+1}(\gamma_2(G))$ for any positive integer n . In particular, if $\gamma_2(G)$ is abelian, then the isomorphism type of $\gamma_2(G)$ is an invariant.
- (5) The isomorphism type of $\Gamma(G) = \gamma_2(G) \cap Z(G)$.
- (6) The isomorphism type of the quotient $G/\gamma_2(G)^p\gamma_3(G)$ – the *Sandling quotient*.
- (7) The isomorphism type of the restricted k -Lie algebra $L(G)$ of G .
- (8) If the nilpotency class of G is equal to 2, then the nilpotency class is an invariant [3, Theorem 2].
- (9) If G is 2-generated, then the isomorphism type of $G/\gamma_2(G)^p\gamma_4(G)$ is an invariant [20].

(10) If $G/C_G(\gamma_2(G)/\Phi(\gamma_2(G)))$ is cyclic, then the isomorphism type of

$$C_G(\gamma_2(G)/\Phi(\gamma_2(G)))$$

is an invariant [1, Corollary 7].

We remark that not all authors write about group theoretic invariants; words like *determined* often serve the same purpose. The list of invariants provided above is not complete, but only contains those we will explicitly use in this article. Sometimes, in examples, we will speak of groups sharing *all known group theoretical invariants*. By this, we mean the list of invariants included in [20], which, to the best of our knowledge, covers all invariants known to this day.

2.5 The small group algebra

In this section, we define the small group algebra of kG and briefly discuss its history. We present some classical related constructions and list a number of known properties. This section mostly follows [14, Section 2.3] and [30], though the notation might differ.

Until the end of the present section, *assume* that $\gamma_2(G)^p \gamma_4(G) = 1$, and write $G^{\text{ab}} = G/\gamma_2(G)$ for the abelianization of G . The *small group algebra* of kG is $kG/I(kG)I(k\gamma_2(G))$, and its group of normalized units is

$$S = S_G = V(kG/I(kG)I(k\gamma_2(G))).$$

We then have a natural short exact sequence of groups

$$1 \rightarrow \gamma_2(G) \rightarrow S \xrightarrow{\kappa} V(kG^{\text{ab}}) \rightarrow 1 \quad (2.2)$$

with the property that $\kappa^{-1}(G^{\text{ab}})$ is a copy of G . Without loss of generality, we identify G and $\kappa^{-1}(G^{\text{ab}})$. The group $V(kG^{\text{ab}})$ being abelian, we have that G is a normal subgroup of S .

The history of the small group algebra, or small group ring in this case, dates back to Whitcomb's proof of the fact that integral group rings determine finite metabelian groups [23, Theorem 2.5]. The small group algebra gains much popularity thanks to [30] and the determination of Sandling's invariant; see also Section 2.4. The small group algebra also plays a fundamental role in the proof, by Salim and Sandling, that the (MIP) has a positive answer for groups of order p^5 (see [26–28]); for more detail, see also [25]. In the context of central Frattini extensions and with a relative definition of small group algebra, Hertweck and Soriano classify the central Frattini extensions giving rise to isomorphic small group algebras [15].

We conclude the current section by giving the construction of a complement of G in S and deriving related properties. For this, fix $x_1, \dots, x_n \in G$ (a minimal set of) generators of G with the property that

$$G^{\text{ab}} = \bigoplus_{i=1}^n \langle x_i \gamma_2(G) \rangle.$$

Denote $\mathbf{x} = (x_1, \dots, x_n)$, and for each $\delta = (\delta_1, \dots, \delta_n) \in \mathbb{Z}^n$, write

$$\mathbf{x}^\delta = \overline{x_1}^{\delta_1} \dots \overline{x_n}^{\delta_n}.$$

Set $|x_i \gamma_2(G)| = p^{\lambda_i}$. Define, additionally, $D(G)$ as

$$D(G) = \left\{ \delta = (\delta_1, \dots, \delta_n) \mid 0 \leq \delta_i < p^{\lambda_i}, \delta \not\equiv 0 \pmod p, \sum_{i=1}^n \delta_i \geq 2 \right\}. \quad (2.3)$$

Then the subgroup $A = A(G|\mathbf{x})$ of S that is generated by the elements

$$a = 1 + \mathbf{x}^\delta = 1 + \overline{x_1}^{\delta_1} \overline{x_2}^{\delta_2} \dots \overline{x_n}^{\delta_n} \quad \text{with } \delta \in D(G) \quad (2.4)$$

is a complement of G in S , equivalently $S = G \rtimes A$; see for example [14, Section 2.3]. Moreover, for $x \in G$ and a of the above form, the commutator $[x, a]$ is equal to

$$[x, a] = [\dots [x, \underbrace{x_1, \dots, x_1}_{\delta_1}], \underbrace{x_2, \dots, x_2}_{\delta_2}], \dots, x_{n-1}, \underbrace{x_n, \dots, x_n}_{\delta_n}].$$

Observe that $[G, A]$ is contained in $\gamma_3(G)$ and, since G has class at most 3, all elements a of the form (2.4) with $\sum_{i=1}^n \delta_i \geq 3$ centralize G and are thus central in S . Moreover, A is abelian and $[A, \gamma_2(G)] = 1$.

The following proposition collects some results, already presented by Salim in his PhD thesis [25]. Point (1) is a special instance of [25, Theorem 3.5], point (4) follows from [25, Theorem 3.7], while point (3) is included in [25, Corollary 3.11].

Proposition 2.3. *The following hold:*

- (1) for each $i \in \mathbb{Z}_{\geq 2}$, one has $\gamma_i(S) = \gamma_i(G)$;
- (2) $\Gamma(S) = \Gamma(G)$;
- (3) $[A^p, S] = \{1\}$;
- (4) $G \cap Z(S) = Z(G)$.

Proof. We prove (1) and (2) together. Let $x, y \in S$ and let $g, h \in G$ and $a, b \in A$ be such that $x = ga$ and $y = hb$. It follows from Lemma 2.1 and the fact that $[G, \gamma_3(G)] = 1 = [A, A\gamma_2(G)]$ that

$$\begin{aligned} [x, y] &= [ga, hb] = [ga, b][ga, h]^b \\ &= [g, b]^a [a, b]([g, h]^a [a, h])^b \\ &= [g, b][g, h][a, h] \in \gamma_3(G)\gamma_2(G)\gamma_3(G) = \gamma_2(G). \end{aligned}$$

Since $\gamma_2(G) \subseteq \gamma_2(S)$, we derive that, in fact, $\gamma_2(S) = \gamma_2(G)$.

We now show that $\Gamma(S) = \Gamma(G)$. Since $Z(S) \cap G \subseteq Z(G)$, we have that

$$Z(S) \cap \gamma_2(S) \subseteq Z(G) \cap \gamma_2(G).$$

To show the opposite inclusion, it now suffices to show that $Z(G) \cap \gamma_2(G) \subseteq Z(S)$.

To this end, let $x = ga \in S$ and let $z \in \Gamma(G)$. Then

$$[z, x] = [z, ga] = [z, a][z, g]^a = 1$$

because $[z, a] \in [\gamma_2(G), A] = 1$, $[z, g] \in [Z(G), G] = 1$, and therefore $z \in Z(S)$.

To show that $\gamma_3(S) = \gamma_3(G)$, observe that

$$\gamma_2(S)A = \gamma_2(G)A \subseteq C_S(\gamma_2(G)) = C_S(\gamma_2(S)).$$

We then get the following commutative diagram of natural maps:

$$\begin{array}{ccc} S/\gamma_2(S)A \otimes \gamma_2(S)/\Gamma(S) & \longrightarrow & \gamma_3(S) \\ \cong \downarrow & & \uparrow \subseteq \\ G/\gamma_2(G) \otimes \gamma_2(G)/\Gamma(G) & \longrightarrow & \gamma_3(G) \end{array}$$

and so the inclusion map is an equality.

We now show that $\gamma_4(S) = 1$. Since A is abelian and $S = G \rtimes A$, we have that $[A, S] \subseteq \gamma_3(S) = \gamma_3(G)$. It follows that $\gamma_3(S) \subseteq \gamma_2(G) \cap Z(G) = \gamma_2(S) \cap Z(S)$ and, in particular, $\gamma_3(S)$ is central in S , equivalently $\gamma_4(S) = [S, \gamma_3(S)] = 1$.

(3) This is a direct consequence of $\gamma_2(G)$ being elementary abelian.

(4) We clearly have that $Z(S) \cap G \subseteq Z(G)$ and so we prove the other inclusion. To this end, let $z \in Z(G)$ and $s = ga \in S$. It follows from Lemma 2.1 that $[z, ga] = [z, a][z, g]^a = [z, a]$. If we now take $a = 1 + \bar{x}_i \bar{x}_j$ as in (2.4), then $[z, a] = [[z, x_i], x_j] = 1$ and we are done. \square

Lemma 2.4. *The following hold:*

$$Z_2(S) = Z_2(G)A, \quad [Z_2(G), A] = 1, \quad Z_2(G) = Z_2(S) \cap G.$$

Moreover, $Z_2(S)$ is equal to the direct product of $Z_2(G)$ with A .

Proof. Note that, for $x = ga$ and $y = hb$ in S , the following equality holds:

$$[x, y] = [ga, hb] = [g, b][g, h][a, h]$$

and, moreover, that, by Proposition 2.3 (2), we have

$$\begin{aligned} Z_2(G) &= \{z \in G \mid \text{for all } g \in G : [z, g] \in \Gamma(G)\}, \\ Z_2(S) &= \{z \in S \mid \text{for all } s \in S : [z, s] \in \Gamma(S) = \Gamma(G)\}. \end{aligned}$$

We start by showing that $Z_2(G)A$ is contained in $Z_2(S)$. First, observe that A is contained in $Z_2(S)$ because $[S, A] = [G, A] \subseteq \gamma_3(G) \subseteq \Gamma(G)$. Moreover, if we now take $a = 1$ and $x = g \in Z_2(G)$, it follows from the above formula that $[g, hb] = [g, b][g, h] \in \gamma_3(G)\Gamma(G) = \Gamma(G)$. We now show that $Z_2(S)$ is contained in $Z_2(G)A$. To this end, assume that $x = ga \in Z_2(S)$, and we show that $g \in Z_2(G)$. Indeed, it follows from Lemma 2.1 that

$$[g, h] = [g, b]^{-1}[x, y][a, h]^{-1} \in \gamma_3(G)\Gamma(G) = \Gamma(G).$$

We now show that $[Z_2(S), A] = 1$. For this, observe that $[Z_2(S), A] = [Z_2(G), A]$. Let now $x \in Z_2(G)$ and $a = 1 + \bar{x}_i \bar{x}_j \in A$ as in (2.4). Then we have

$$[x, a] = [[x, x_i], x_j] \in [\Gamma(G), G] = 1,$$

and thus the claim is proven.

We conclude by observing that

$$Z_2(S) \cap G = (Z_2(G)A) \cap G = (G \cap A)Z_2(G) = Z_2(G). \quad \square$$

3 Applications of the small group algebra

In this section, we will push techniques of Salim and Sandling further to achieve a positive solution of the (MIP) for some families of groups, yielding in particular new results for orders p^6 and p^7 . We do this with the aid of the small group algebra, as introduced in Section 2.5.

Until the end of the present section, *assume* that $\gamma_2(G)^p \gamma_4(G) = 1$. It is not difficult to show that, under the additional assumption that p is odd, the subgroup structure of G is as in Figure 1. We remark that, in Figure 1, the only inclusion requiring p odd is $G^p \subseteq Z(G)$. In the statements in which we will require this, we will explicitly assume that p is odd.

Write $G^{\text{ab}} = G/\gamma_2(G)$ for the abelianization of G and

$$S = V(kG/I(kG)I(k\gamma_2(G)))$$

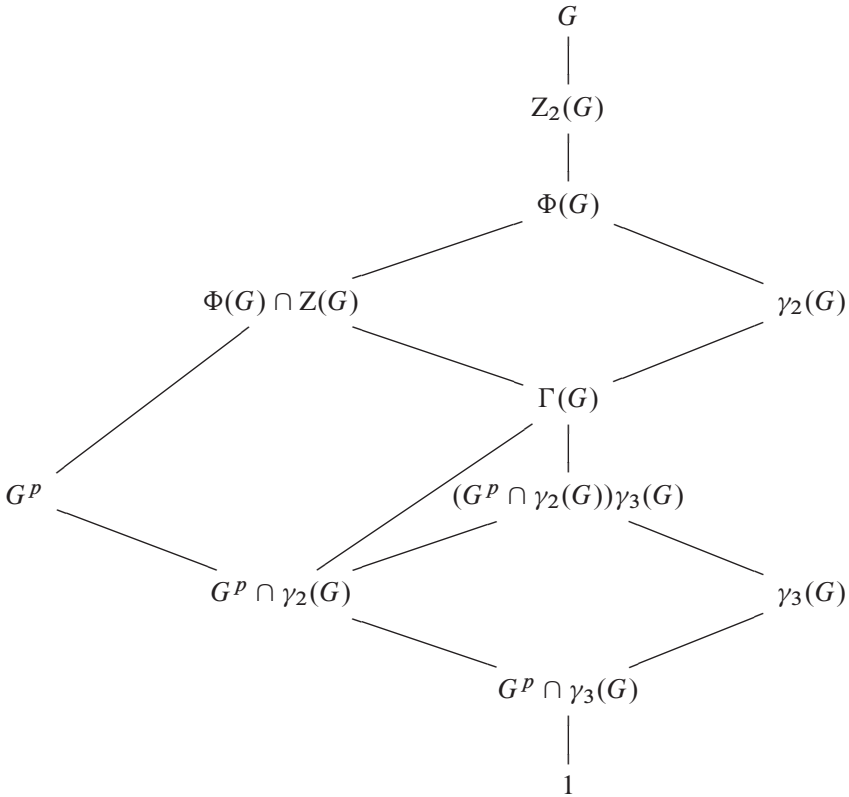


Figure 1. Subgroup structure of G in case $\gamma_2(G)^p\gamma_4(G) = 1$ and p odd

for the normalized units of the small group algebra of kG . Let $\mathbf{x} = (x_1, \dots, x_n)$ be a vector of generating elements of G satisfying $G^{\text{ab}} = \bigoplus_{i=1}^n \langle x_i \gamma_2(G) \rangle$, and denote $|x_i \gamma_2(G)| = p^{\lambda_i}$. Let $A = A(G|\mathbf{x})$ denote the complement of G in S as defined in Section 2.5. Then A satisfies the following:

$$S = G \rtimes A, \quad [G, A] \subseteq \gamma_3(G), \quad [A, A\gamma_2(G)] = 1.$$

We will show in Section 3.1 that any group base of kG can be complemented by A in S . Moreover, we will show how generating sets of two group bases can be related via translation by elements of A . Section 3.2 collects the main results of Section 3. We present implications of our main results in Section 3.3, with a particular emphasis on the case of groups of order p^6 and p^7 . Additionally, we give computational evidence aimed at depicting our contribution for the last groups and give a critical analysis of the limits of our methods for order p^6 .

3.1 Compatible complements

The aim of the current section is to relate different group bases of kG within S . We observe that, if H is another group base of kG , then $kG^{\text{ab}} = kH^{\text{ab}}$, and so, through the short exact sequence in (2.2), the group S possesses a normal subgroup that is isomorphic to H . Because of this, we can consider every group base of kG to be embedded in S as a normal subgroup.

Proposition 3.1. *Let H be a group base of kG , and consider it embedded in S . Then $S = G \rtimes A = H \rtimes A$.*

Proof. Write

$$\mathbf{y} = (y_1, \dots, y_n) = (x_1\gamma_2(G), \dots, x_n\gamma_2(G)),$$

and denote $A^{\text{ab}} = A(G^{\text{ab}}|\mathbf{y})$. Let $D(G)$ be as defined in (2.3), and define

$$\mathcal{B} = \{\mathbf{y}^\delta \mid \delta \in D(G)\}.$$

It follows from the description in Section 2.5 that A^{ab} is generated by $1 + \mathcal{B}$ and, with the notation from (2.2), that $A^{\text{ab}} = \kappa(A)$. Moreover, $V(kG^{\text{ab}})$ is the direct product of G^{ab} and A^{ab} . Now define U to be the k -linear span of \mathcal{B} in kG^{ab} ; we claim that $1 + U = A^{\text{ab}}$. For this, observe that, as we have defined it, U satisfies the following equality for all positive integers m :

$$\begin{aligned} I(kG^{\text{ab}})^m / I(kG^{\text{ab}})^{m+1} \\ &= H_m(kG^{\text{ab}}) / I(kG^{\text{ab}})^{m+1} \\ &\quad \oplus ((U \cap I(kG^{\text{ab}})^m) + I(kG^{\text{ab}})^{m+1}) / I(kG^{\text{ab}})^{m+1}. \end{aligned}$$

In particular, it holds that

$$|U| = |I(kG^{\text{ab}})| / \prod_{m \geq 1} |D_m(G^{\text{ab}}) : D_{m+1}(G^{\text{ab}})| = |I(kG^{\text{ab}})| / |G| = |A^{\text{ab}}|.$$

Since U is multiplicatively closed, $1 + U$ is a group and thus $\langle 1 + \mathcal{B} \rangle = 1 + U$. It follows from the theory of Zassenhaus ideals, cf. Section 2.3, that $A^{\text{ab}} = 1 + U$ and therefore

$$V(kG^{\text{ab}}) = H^{\text{ab}} \times A^{\text{ab}} = \kappa(H) \times \kappa(A).$$

To conclude, assume, for a contradiction, that A intersects H non-trivially. Thanks to Proposition 2.3 (1), the subgroups $\gamma_2(H)$ and $\gamma_2(G)$ coincide, and thus we have $A \cap \gamma_2(H) = 1$. It follows then that $H \cap A$ has a non-trivial image in $V(kG^{\text{ab}})$, but this contradicts the fact that $V(kG^{\text{ab}}) = H^{\text{ab}} \times \kappa(A)$. \square

Thanks to the last result, the subgroup A is a mutual complement of both G and H . It follows that, if S determines the isomorphism type of G , then so does $S/(A \cap Z(S))$. Without loss of generality, we *assume*, until the end of Section 3, that $A \cap Z(S) = 1$. It follows from Proposition 2.3 (3) that A is elementary abelian.

Lemma 3.2. *Let H be a group base of kG , and consider it embedded in S . Let g_1, \dots, g_n be a generating set of G . Then there exist $a_1, \dots, a_n \in A$ such that $g_1 a_1, \dots, g_n a_n$ is a generating set of H .*

Proof. We start by claiming that, if $\{y_i \mid 1 \leq i \leq m\}$ is a generating set of G , where each y_i is written as $y_i = z_i b_i$ with $z_i \in H$ and $b_i \in A$, then H is generated by z_1, \dots, z_m . To this end, call $Z = \langle z_i \mid 1 \leq i \leq m \rangle$; we show that $Z = H$. First observe that $\gamma_3(H) \subseteq Z$; indeed, for any choice of i, j, ℓ , one has

$$[y_i, y_j, y_\ell] = [z_i, z_j, z_\ell].$$

Now, H being a group base of kG , by Proposition 2.3 (1), the subgroups $\gamma_3(H)$ and $\gamma_3(S)$ coincide, and thus it follows that Z contains $\gamma_3(S)$. Moreover, since $[S, A]$ is contained in $\gamma_3(S)$, we derive that actually Z contains $\gamma_2(S)$. In particular, Z is normal in H , so Proposition 3.1 yields $S = HA \subseteq ZA$ and thus $Z = H$.

Now write each g_i as $g_i = h_i c_i$, where $h_i \in H$ and $c_i \in A$; this can be done thanks to Proposition 3.1. A consequence of the above claim is that h_1, \dots, h_n generate H . We conclude by defining $a_i = c_i^{-1}$. \square

3.2 Main results

In the present section, we leverage results from Section 3.1 to solve the (MIP) for certain families of groups. Recall that, without loss of generality, we have assumed in Section 3.1 that $A \cap Z(S) = 1$. The following is our first main result.

Theorem 3.3. *Assume that p is odd, $\gamma_2(G)^p \gamma_4(G) = 1$, and $C_G(\gamma_2(G))$ is a maximal subgroup of G that is abelian. Then the small group algebra of kG determines G up to isomorphism. Moreover, the (MIP) has a positive answer for G .*

Proof. Set $C = C_G(\gamma_2(G))$, and let H be another group base of kG , which we consider to be embedded in the group S of normalized units of the small group algebra of kG . Then Proposition 3.1 yields that $S = G \rtimes A = H \rtimes A$. Now, by Proposition 2.3 (1), we have $\gamma_2(G) = \gamma_2(H)$, from which we derive that

$$C_S(\gamma_2(S)) = CA = C_H(\gamma_2(H))A.$$

We will show that, for a certain family of generators g_1, \dots, g_n of G , there exist generating elements h_1, \dots, h_n of H satisfying the same relations as g_1, \dots, g_n . To this end, let g_1, \dots, g_n be a minimal generating set of G satisfying the following:

- $C = \langle g_2, \dots, g_n \rangle \gamma_2(G)$;
- for $|\gamma_2(G) : \gamma_2(G) \cap G^p| = p^{r-1}$, the elements g_2, \dots, g_r are such that

$$[g_2, g_1], \dots, [g_r, g_1]$$

form a basis of $\gamma_2(G)$ modulo $\gamma_2(G) \cap G^p$.

The following ensures the existence of such a generating set. Since C is abelian, $\gamma_2(G) = [\langle g_1 \rangle, C]$, and since $[C, \gamma_2(G)] = 1$, we have that $\gamma_3(G) = [\langle g_1 \rangle, \gamma_2(G)]$. Now let a_1, \dots, a_n be as in Lemma 3.2 and observe that $C_H = C_H(\gamma_2(H))$ is generated by $g_2 a_2, \dots, g_n a_n$ modulo $\gamma_2(H)$. Thanks to Bagiński's invariant from Section 2.4 (9), the groups C and C_H are maximal subgroups respectively in G and H , and both of them are abelian. In other words, for each $i, j \in \{2, \dots, n\}$, it holds that $[g_i a_i, g_j a_j] = [g_i, g_j] = 1$. Denote by \mathbf{g} the vector (g_1, \dots, g_n) , and for each $\delta = (\delta_1, \dots, \delta_n) \in \mathbb{Z}^n$, write $\mathbf{g}^\delta = g_1^{\delta_1} \dots g_n^{\delta_n}$. For each $i \in \{1, \dots, n\}$, we now choose $\beta_i \in \gamma_2(G) = \gamma_2(H)$ such that it satisfies

$$[\beta_i, g_1] = ([a_i, g_1][g_i, a_1])^{-1}.$$

Define, moreover, for each i , the element h_i to be $g_i \beta_i a_i$ and $\mathbf{h} = (h_1, \dots, h_n)$. Then, for $i, j, \ell \in \{1, \dots, n\}$, the following hold:

- for $i, j \geq 2$, one has

$$[h_i, h_j] = [g_i, g_j]$$

because $A\gamma_2(G)$ is abelian and $[g_i a_i, g_j a_j] = 1$;

- $[h_i, h_1] = [g_i, g_1]$ thanks to the definition of the β_i 's,

$$\begin{aligned} [h_i, h_1] &= [g_i \beta_i a_i, g_1 a_1] = [g_i \beta_i a_i, g_1][g_i, a_1] = [g_i, g_1][\beta_i a_i, g_1][g_i, a_1] \\ &= [g_i, g_1][\beta_i, g_1][a_i, g_1][g_i, a_1] = [g_i, g_1]; \end{aligned}$$

- $[h_i, h_j, h_\ell] = [g_i, g_j, g_\ell]$ because $[G, A] \subseteq \gamma_3(G) \subseteq \mathbf{Z}(G)$;
- for each $\delta \in p\mathbb{Z}^n$, one has $\mathbf{h}^\delta = \mathbf{g}^\delta$ because $[A\gamma_2(G), G]$ is central in S , $\gamma_2(G)$ is elementary abelian, and p is odd.

This shows that G and H have the same presentations in terms of g_1, \dots, g_n and h_1, \dots, h_n , respectively. So, in particular, G and H are isomorphic. \square

The small group algebra has been used to (positively) solve the (MIP) for 2-generated groups G satisfying $\gamma_2(G)^p \gamma_4(G) = 1$ (see [20]). Extending the last result to 3-generated groups is not straightforward; Theorem 3.5 is a first step in this direction.

Lemma 3.4. *Assume that G has class 3 and $|G : \Phi(G)| = |G : Z_2(G)| = p^3$. Then the following hold:*

- (1) $|\gamma_2(G) : \gamma_3(G)| \leq p^3$;
- (2) *there exists a unique subgroup K_G of G , containing $Z_2(G)$, with the property that the following sequence induced by the commutator map is exact:*

$$1 \rightarrow \wedge^2(K_G/Z_2(G)) \rightarrow \wedge^2(G/Z_2(G)) \rightarrow \gamma_2(G)/\Gamma(G) \rightarrow 1.$$

- (3) *if $|\gamma_2(G) : \Gamma(G)| = p^3$, then $K_G = Z_2(G)$;*
- (4) *if $|\gamma_2(G) : \Gamma(G)| < p^3$, then $|\gamma_2(G) : \Gamma(G)| = p^2$ and K_G is maximal in G .*

Proof. It follows from the assumptions that $\Phi(G) = Z_2(G)$. Now, to lighten the notation, we write $U = G/\Phi(G)$, which is a 3-dimensional vector space over k . Since $\gamma_2(G)$ is elementary abelian, the commutator map induces a bilinear map $U \times U \rightarrow \gamma_2(G)/\gamma_3(G)$. The last map being alternating, the universal property of wedge products induces a surjective linear map $\wedge^2 U \rightarrow \gamma_2(G)/\gamma_3(G)$, and as $\wedge^2 U$ has dimension 3, the first claim follows.

We now prove (2), (3), (4) simultaneously. For this, note that $\gamma_3(G) \subseteq \Gamma(G)$ and, since $\Phi(G) = Z_2(G)$, the commutator map induces a non-degenerate alternating map $\nu : U \times U \rightarrow \gamma_2(G)/\Gamma(G)$. In particular, the dimension of U being odd, we get that

$$p^2 \leq |\gamma_2(G) : \Gamma(G)| \leq |\gamma_2(G) : \gamma_3(G)| \leq p^3.$$

Now let W be a subspace of U such that the following short exact sequence, induced by ν , is exact:

$$1 \rightarrow \wedge^2 W \rightarrow \wedge^2 U \xrightarrow{\tilde{\nu}} \gamma_2(G)/\Gamma(G) \rightarrow 1.$$

The existence of W is guaranteed by the following considerations. The dimension of $\wedge^2 U$ being 3, one has that $|\gamma_2(G) : \Gamma(G)| = p^3$ implies that $\tilde{\nu}$ is injective and $W = 0$. In particular, in the last case, W is unique with this property and $K_G = Z_2(G)$. Assume now that $|\gamma_2(G) : \Gamma(G)| = p^2$. Then $\tilde{\nu}$ has a non-trivial kernel, and $\tilde{\nu}$ being induced by ν , there is a subspace W of U such that $\ker \tilde{\nu} = \wedge^2 W$. The map $\tilde{\nu}$ being surjective, it follows that W has dimension 2, and the fact that $|\gamma_2(G) : \Gamma(G)| = p^2$ ensures that W is unique with this property. In particular, K_G , defined by $K_G/Z_2(G) = W$, is maximal. \square

In the remaining part of Section 3, let K_G denote the characteristic subgroup from Lemma 3.4.

Theorem 3.5. *Assume that p is odd, $\gamma_2(G)^p \gamma_4(G) = 1$, and*

$$|G : \Phi(G)| = |G : Z_2(G)| = p^3.$$

If G has class 3, assume, furthermore, that $[[K_G, G], G] \subseteq [K_G, \gamma_2(G)]$. Then the isomorphism type of G is determined by the unit group of the small group algebra of kG . Moreover, the (MIP) has a positive answer for G .

Proof. If $\gamma_3(G) = 1$, then the result follows from the work of Sandling, cf. Section 2.4 (6). Assume now that $\gamma_3(G) \neq 1$, so it follows from the assumptions that $\Phi(G) = Z_2(G)$. Similarly to the proof of Theorem 3.3, let H be another group base of kG , which we consider to be embedded in the group S of normalized units of the small group algebra of kG . Then the equality $S = G \rtimes A = H \rtimes A$ holds by Proposition 3.1, and $\gamma_2(G) = \gamma_2(H)$ by Proposition 2.3 (1). We will show that, for a certain family of generators g_1, g_2, g_3 of G , there exist generating elements h_1, h_2, h_3 of H satisfying the same relations as g_1, g_2, g_3 . We will study two cases separately.

First, suppose that $|\gamma_2(G) : \Gamma(G)| = p^3$, and let g_1, g_2, g_3 be any minimal generating set of G . By Lemma 3.2, there are elements a_1, a_2, a_3 in A such that $h_i = g_i a_i$ generate H . We will show that h_1, h_2, h_3 already satisfy the same relations as g_1, g_2, g_3 . From Lemma 3.4, we know that $K_G = Z_2(G)$, $\Gamma(G) = \gamma_3(G)$, and the commutators $[g_2, g_1], [g_3, g_1], [g_3, g_2]$ form a basis of $\gamma_2(G)$ modulo $\gamma_3(G)$ and they do not lie in G^p . Notice that, for $i, j, \ell \in \{1, 2, 3\}$ and m any positive integer, we have

- $[g_i, g_j] \equiv [h_i, h_j] \pmod{\gamma_3(G)}$ because $[G, A] \subseteq \gamma_3(G)$,
- $[g_i, g_j, g_\ell] = [h_i, h_j, h_\ell]$ as $[G, A] \subseteq Z(G)$,
- $g_i^{p^m} = h_i^{p^m}$ because $A\gamma_2(G)$ is elementary abelian, $[G, A]$ is central, and p is odd.

It follows that h_1, h_2 , and h_3 satisfy the same relations as g_1, g_2 , and g_3 .

We now consider the case $|\gamma_2(G) : \Gamma(G)| = p^2$, which is the only case left in view of Lemma 3.4. By Lemma 3.4, the subgroup K_G is maximal in G . We choose a generating set g_1, g_2, g_3 of G such that $g_2, g_3 \in K_G$, and so, by Lemma 3.2, there exist $a_1, a_2, a_3 \in A$ such that $g_1 a_1, g_2 a_2, g_3 a_3$ generate H . Let β_2 and β_3 be elements of $\gamma_2(G)$ such that

$$[\beta_3, g_2][g_3, \beta_2] = ([a_3, g_2][g_3, a_2])^{-1}.$$

Note that such β_2, β_3 exist because $[a_3, g_2][g_3, a_2] \in [K_G, G, G] \subseteq [K_G, \gamma_2(G)]$ and g_2, g_3 form a basis of K_G modulo $\gamma_2(G)Z(G)$. Set $h_1 = g_1a_1, h_2 = g_2\beta_2a_2$, and $h_3 = g_3\beta_3a_3$. As $\gamma_2(G) = \gamma_2(H)$, we know that h_2 and h_3 are elements of H . Now $[g_2, g_1]$ and $[g_3, g_1]$ form a basis of $\gamma_2(G)$ modulo $\Gamma(G)$ and do not lie in G^p . So, for $i, j, \ell \in \{1, 2, 3\}$ and m any positive integer, we have

- $[g_2, g_1] \equiv [h_2, h_1]$ modulo $\gamma_3(G)$ and $[g_3, g_1] \equiv [h_3, h_1]$ modulo $\gamma_3(G)$ because $[G, A] \subseteq \gamma_3(G)$,
- $[h_3, h_2] = [g_3, g_2][\beta_3, g_2][g_3, \beta_2][a_3, g_2][g_3, a_2] = [g_3, g_2]$,
- $[g_i, g_j, g_\ell] = [h_i, h_j, h_\ell]$ since $[G, A] \subseteq Z(G)$,
- $g_i^{p^m} = h_i^{p^m}$ because $A\gamma_2(G)$ is elementary abelian, $[G, A]$ is central, and p is odd.

This shows that G and H have the same presentations in terms of respectively g_1, g_2, g_3 and h_1, h_2, h_3 , so, in particular, G and H are isomorphic. \square

3.3 Corollaries and further discussion

The upcoming series of corollaries of our results from Section 3.2 yields a number of new classes of p -groups of orders p^6 and p^7 for which the (MIP) is positively solved.

Corollary 3.6. *Assume that p is odd, $\gamma_2(G)^p\gamma_4(G) = 1$, and*

$$|G : \Phi(G)| = |G : Z_2(G)| = p^3.$$

The isomorphism type of G is determined by the normalized units of the small group algebra of kG if one of the following holds:

- (1) $|\gamma_2(G) : \Gamma(G)| = p^3$,
- (2) $|\gamma_3(G)| = p$.

Proof. We assume that $\gamma_3(G) \neq 1$ as a consequence of Section 2.4 (6). Then, by Lemma 3.4, the index $|\gamma_2(G) : \Gamma(G)|$ is either p^2 or p^3 .

If $|\gamma_2(G) : \Gamma(G)| = p^3$, then Lemma 3.4 yields $K_G = Z_2(G)$, and therefore, we have $[K_G, G] \subseteq Z(G)$ and $[[K_G, G], G] = 1$. The claim follows from Theorem 3.5.

Assume now that $|\gamma_3(G)| = p$ and that $|\gamma_2(G) : \Gamma(G)| = p^2$ as a consequence of (1). Then, by Lemma 3.4 (4), the subgroup K_G is maximal in G . Now the commutator map

$$G/C_G(\gamma_2(G)) \times \gamma_2(G)/\Gamma(G) \rightarrow \gamma_3(G)$$

is a non-degenerate alternating map and, since $\gamma_2(G)/\Gamma(G)$ is 2-dimensional, $G/C_G(\gamma_2(G))$ has dimension 2. In particular, $C_G(\gamma_2(G))$ is different from K_G , and thus $[K_G, \gamma_2(G)] \neq 1$. It follows that $[K_G, \gamma_2(G)] = \gamma_3(G)$, and so we are done by Theorem 3.5. \square

Corollary 3.7. *Assume that $|G| = p^6$, $\gamma_2(G)^p \gamma_4(G) = 1$, and $|G : Z_2(G)| = p^3$. Then the isomorphism type of G is determined by the normalized units of the small group algebra of kG .*

Proof. The work in [33] covers the case $p = 2$, and Section 2.4(6) covers the case $\gamma_3(G) = 1$. We assume that p is odd and that $\gamma_3(G) \neq 1$. We show that $\Phi(G) = Z_2(G)$. The inclusions $\gamma_2(G) \subseteq \Phi(G) \subseteq Z_2(G)$ are clear, so we show that $Z_2(G) = \gamma_2(G)$. The commutator map induces a non-degenerate map

$$G/Z_2(G) \times G/Z_2(G) \rightarrow Z(G)\gamma_2(G)/Z(G),$$

and so, the dimension of $G/Z_2(G)$ being odd, $p < |Z(G)\gamma_2(G) : Z(G)| \leq p^3$. Moreover, the class of G being 3, we have that $|\gamma_3(G)| \geq p$ and $\gamma_2(G)$ is not central. We derive that $Z(G) = \gamma_3(G)$ and $\gamma_3(G)$ has order p . In particular, we have that $\gamma_2(G)$ contains $Z(G)$ and $\gamma_2(G) = Z_2(G) = \Phi(G)$. We conclude thanks to Corollary 3.6. \square

We remark that, under the conditions that G has class 3, order p^6 , and $\gamma_2(G)$ is elementary abelian, the only possibilities for the index of $Z_2(G)$ in G are p^2 and p^3 . The latter case is settled by Corollary 3.7, while the case $|G : Z_2(G)| = p^2$ cannot be settled within the small group algebra, as Example 3.11 shows.

Remark 3.8 (Isoclinism classes). We briefly discuss here the influence of our results on the (MIP) for groups of order p^6 in terms of isoclinism classes. Following P. Hall’s definition [32, Definition 4.28], two groups X and Y are *isoclinic* if there exist isomorphisms

$$\varphi: X/Z(X) \rightarrow Y/Z(Y) \quad \text{and} \quad \psi: \gamma_2(X) \rightarrow \gamma_2(Y)$$

commuting with the commutator map, in other words such that, for each $x, x' \in X$, one has

$$\psi([x, x']) = [\varphi(x)Z(X), \varphi(x')Z(X)].$$

We rely on the classification in [17] of the 43 isoclinism classes Φ_1, \dots, Φ_{43} of groups of order at most p^6 for p odd. We note that the isomorphism types of the proper members of the lower central series of a p -group are invariants of its isoclinism classes [32, (4.30)]. In particular, Sandling’s condition $\gamma_2(G)^p \gamma_3(G) = 1$

is invariant under isoclinism and covers the classes $\Phi_2, \Phi_4, \Phi_5, \Phi_{11}, \Phi_{12}, \Phi_{13}$, and Φ_{15} . The class Φ_1 corresponds to the abelian groups and was already covered by [10]. The class Φ_{14} is covered by [9], while the class Φ_{35} is covered by [2]. To the best of our knowledge, no other class is fully covered by existing results. Theorem 3.3 yields the new classes Φ_3 and Φ_{16} , while Corollary 3.7 yields the new classes $\Phi_{31}, \Phi_{32}, \Phi_{33}$.

Corollary 3.9. *Assume that $|G| = p^7$, $\gamma_2(G)^p \gamma_4(G) = 1$, and*

$$|G : Z_2(G)| = |G : \Phi(G)| = p^3.$$

The isomorphism type of G is determined by the normalized units of the small group algebra of kG if one of the following holds:

- (1) $|\gamma_3(G)| = p$;
- (2) *if G has class 3, then $[K_G, \gamma_2(G)] = \gamma_3(G)$.*

Proof. If $p = 2$, then we are done thanks to work of Wursthorn [7]; assume thus that p is odd. If $\gamma_3(G) = 1$, then Section 2.4(6) yields the claim. Assume that $\gamma_3(G) \neq 1$. If $|\gamma_3(G)| = p$, then we are done by Corollary 3.6. To conclude, assume that $[K_G, \gamma_2(G)] = \gamma_3(G)$; then $[K_G, G, G] \subseteq [K_G, \gamma_2(G)]$, and so we are done by Theorem 3.5. \square

The groups of order p^7 are classified, cf. [18, 21]; however, to the best of our knowledge, there is no documentation available that allows us to give a precise count in this case of groups covered by our work as we do in Remark 3.8. Nonetheless, if for a fixed class c , we expect all primes larger than c to behave “in a somewhat analogous way for what concerns group counting”, cf. [21, § 1], then we can hope to learn something about the general scenario for groups of order p^7 from the groups of order 7^7 . The following remark collects computational evidence for $p = 5, 7$ in relation to this section’s results.

Remark 3.10 (Computational evidence for $p = 5, 7$). Denote by $f(p, n)$ the number of isomorphism classes of groups of order p^n and by $\tilde{f}(p, n)$ the number of such classes in which a representative has class 3 and derived subgroup of exponent p . Let, moreover, $g(p, n)$ denote the number of isomorphism classes of groups of order p^n which satisfy the assumptions of Theorems 3.3 or 3.5. Set

$$\text{perc}(p, n) = (\tilde{f}(p, n)/f(p, n), g(p, n)/\tilde{f}(p, n), g(p, n)/f(p, n)).$$

The following table collects information on these numbers for $p = 5, 7, n = 6, 7$.

p	$f(p, 6)$	$\tilde{f}(p, 6)$	$g(p, 6)$	$\text{perc}(p, 6)$
5	684	373	68	(0.545, 0.182, 0.099)
7	860	493	72	(0.573, 0.146, 0.084)

p	$f(p, 7)$	$\tilde{f}(p, 7)$	$g(p, 7)$	$\text{perc}(p, 7)$
5	34297	22436	13459	(0.654, 0.6, 0.392)
7	113147	75948	55429	(0.671, 0.73, 0.49)

Assume $p = 5$; we expand on the content of the last table. Up to isomorphism, there are 684 groups of order p^6 , of which 373 have class 3 and elementary abelian derived subgroup. Under the last assumptions, there are 50 groups G with $C_G(\gamma_2(G))$ maximal and abelian (and so covered by Theorem 3.3) and 18 groups with second center of index p^3 (covered by Corollary 3.7). On the other hand, there are 34297 groups of order p^7 , of which 22436 have class 3 and elementary abelian derived subgroup. Within this last class, 170 groups are covered by Theorem 3.3 and 13289 groups are given by Corollary 3.9, contributing to a total of 13459 groups. The interpretation for $p = 7$ is analogous.

The last result of this section is the following example of groups of order 5^6 with isomorphic small group algebras. Example 3.11 demonstrates that it is not possible to apply the same strategy adopted by Salim and Sandling for the groups of order p^5 (see [26–28]) to the groups of order p^6 , though some of the techniques from this section resemble theirs; see for example [25, Lemma 6.1]. We recall indeed that the work of Salim and Sandling builds upon three main subcases: groups that are determined by known group theoretical invariants, groups of maximal class [28], and the remaining groups, having class at most 3 and elementary abelian derived subgroup, are shown to be determined by the unit group of the small group algebra, cf. [27] and [25, Chapter 6].

Example 3.11. Let $G = \text{SG}(5^6, 553)$, $H = \text{SG}(5^6, 554)$. It can be checked using GAP that G and H share all known group theoretical invariants. We will show that the unit groups of the small group algebras of kG and kH are isomorphic. We will do so by displaying a normal subgroup of $S = V(kG/I(kG)I(k\gamma_2(G)))$ satisfying the same relations as H . It will be clear from the presentations of G and H that both groups are 4-generated of class 3 and satisfy

$$\gamma_2(G)^p \gamma_4(G) = \gamma_2(H)^p \gamma_4(H) = 1;$$

it thus makes sense to work at the level of small group algebras.

The Small Groups Library in GAP provides the following polycyclic presentations of the two groups in question, where trivial commutators are omitted:

$$G = \langle g_1, g_2, g_3, g_4, g_5, g_6 \mid g_1^5 = g_2^{25} = g_3^{25} = g_4^5 = g_5^5 = g_6^5 = 1, \\ [g_2, g_1] = g_6, [g_4, g_3] = g_5, [g_5, g_4] = g_6, \\ g_2^5 = g_3^5 = g_6^{-1} \rangle,$$

$$H = \langle h_1, h_2, h_3, h_4, h_5, h_6 \mid h_1^5 = h_2^{25} = h_3^{25} = h_4^5 = h_5^5 = h_6^5 = 1, \\ [h_2, h_1] = h_6, [h_4, h_3] = h_5, [h_5, h_4] = h_6, \\ h_2^5 = h_3^5 = h_6^{-2} \rangle.$$

Since our methods are more suitable for controlling differences between commutators rather than between p -th powers, we translate the last presentations to

$$G = \langle g_1, g_2, g_3, g_4, g_5, g_6 \mid g_1^5 = g_2^{25} = g_3^{25} = g_4^5 = g_5^5 = g_6^5 = 1, \\ [g_2, g_1] = g_6^{-1}, [g_4, g_3] = g_5, [g_5, g_4] = g_6^{-1}, \\ g_2^5 = g_3^5 = g_6 \rangle, \tag{3.1}$$

$$H = \langle h_1, h_2, h_3, h_4, h_5, h_6 \mid h_1^5 = h_2^{25} = h_3^{25} = h_4^5 = h_5^5 = h_6^5 = 1, \\ [h_2, h_1] = h_6^2, [h_4, h_3] = h_5, [h_5, h_4] = h_6^2, \\ h_2^5 = h_3^5 = h_6 \rangle.$$

We note that $A = A(G|g_1, \dots, g_4)/(A \cap Z(S))$ is generated by the elements $a = 1 + \bar{g}_3\bar{g}_4$ and $b = 1 + \bar{g}_4^2$. Moreover, one can compute that

$$C_S(b) = \langle A, \gamma_2(G), g_1, g_2, g_4 \rangle$$

and $[g_3, b] = [g_3, g_4, g_4] = [g_5^{-1}, g_4] = g_6$. Now define

$$\tilde{h}_1 = g_1^{-2}b^{-2}, \quad \tilde{h}_2 = g_2, \quad \tilde{h}_3 = g_2^{-2}g_3^{-2}, \quad \tilde{h}_4 = g_4,$$

and set $\tilde{H} = \langle \tilde{h}_1, \tilde{h}_2, \tilde{h}_3, \tilde{h}_4 \rangle$. We claim that $\tilde{H} \cap A = 1$ and $\tilde{H} \cong H$. To this end, define

$$\tilde{h}_5 = [\tilde{h}_4, \tilde{h}_3] = [g_4, g_2^{-2}g_3^{-2}] = [g_4, g_3^{-2}] = g_5^{-2} \quad \text{and} \quad \tilde{h}_6 = \tilde{h}_2^5 = g_6.$$

We will show that the relations of \tilde{H} with respect to the generators $\tilde{h}_1, \dots, \tilde{h}_6$ are exactly those from H 's presentation in (3.1). It is not difficult to show that

$$\tilde{h}_1^5 = \tilde{h}_2^{25} = \tilde{h}_3^{25} = \tilde{h}_4^5 = 1 \quad \text{and} \quad \tilde{h}_3^5 = (g_2^{-2}g_3^{-2})^5 = g_6^{-4} = g_6 = \tilde{h}_6,$$

settling the p -th powers. Moreover, we compute

$$\begin{aligned} [\tilde{h}_2, \tilde{h}_1] &= [g_2, g_1^{-2}b^{-2}] = [g_2, g_1]^{-2} = g_6^2 = \tilde{h}_6^2, \\ [\tilde{h}_3, \tilde{h}_1] &= [g_2^{-2}g_3^{-2}, g_1^{-2}b^{-2}] = [g_2^{-2}, g_1^{-2}][g_3^{-2}, b^{-2}] = g_6g_6^{-1} = 1, \\ [\tilde{h}_4, \tilde{h}_1] &= [g_4, g_1^{-2}b^{-2}] = 1, \\ [\tilde{h}_3, \tilde{h}_2] &= [g_2^{-2}g_3^{-2}, g_2] = 1, \\ [\tilde{h}_4, \tilde{h}_2] &= [g_4, g_2] = 1, \\ [\tilde{h}_5, \tilde{h}_1] &= [\tilde{h}_5, \tilde{h}_2] = [\tilde{h}_5, \tilde{h}_3] = 1, \\ [\tilde{h}_5, \tilde{h}_4] &= [g_5^{-2}, g_4] = [g_5, g_4]^{-2} = g_6^2 = \tilde{h}_6^2. \end{aligned}$$

Since \tilde{h}_6 is clearly central in \tilde{H} , all the relations from (3.1) hold. This shows that \tilde{H} is isomorphic to H , implying that the unit groups of the small group algebras of kG and kH are isomorphic. Having a closer look on the elements of \tilde{H} , we see that they are also linearly independent in $kG/I(kG)I(k\gamma_2(G))$, as so are the elements of G . So \tilde{H} is a group basis of $kG/I(kG)I(k\gamma_2(G))$. Hence the small group algebras of G and H are also isomorphic.

We close the present section with an account of the history of pairs of groups that are not told apart by the small group algebra. To the best of our knowledge, the first example appearing in the literature dates back to [1, Section 4] and concerns groups of order at least p^5 , of maximal class with an elementary abelian maximal subgroup (in particular the fourth element of the lower central series is, in this case, non-trivial). In [15], the authors display groups of order 16 and 32 with the same relative small group algebra; for all such groups, the derived subgroup is cyclic of order 4, so the considered small group algebra is different from the one from this paper. We also wish to mention two examples that are mentioned in the literature, but were never published. The first one, attributed to Kimmerle and Scott, figures in [29, Footnote 6.e after 6.25 from Chapter 6] and [15]. The second one, attributed to Wursthorn, concerns four groups of order 5^5 and maximal class that have all isomorphic small group algebras and is referred to in [28, page 1073].

4 Lower central series invariants

In [9], the (MIP) is solved for 2-generated p -groups of class 2, while in [20, Proposition 2.5], it is solved for 2-generated groups of class 3 in which the derived subgroup is elementary abelian. In this section, we consider 2-generated groups of class 3, but drop the assumption that the derived subgroup is elementary abelian. The main result of this section is the following.

Theorem 4.1. *Assume that p is odd and H is a group such that $kG \cong kH$. Assume moreover that G is 2-generated with $\gamma_3(G)$ central of exponent p . Then H has the same class as G , and for each integer $i \geq 2$, one has $\gamma_i(G) \cong \gamma_i(H)$.*

Under the assumptions of Theorem 4.1, proving that $\gamma_3(G) \cong \gamma_3(H)$ turns out to be the most challenging task. Indeed, the number $|\gamma_3(G)|$ is not a known group theoretical invariant and cannot be derived from known group theoretical invariants either, as the following example shows.

Example 4.2. For $G = \text{SG}(3^7, 19)$ and $H = \text{SG}(3^7, 43)$, a quick check using the software of [20] shows that G and H share all known group theoretical invariants, but do not satisfy $|\gamma_3(G)| = |\gamma_3(H)|$.

Lemma 4.3. *Assume that G has class 3, $\gamma_2(G)/\gamma_3(G)$ is cyclic, and $\gamma_3(G)$ is elementary abelian. Then $\Gamma(G) = \gamma_2(G)^p \gamma_3(G)$ and $\Gamma(G)$ is maximal in $\gamma_2(G)$.*

Proof. The subgroup $\gamma_3(G)$ is contained in $\Gamma(G)$, and the commutator map

$$G \times \gamma_2(G) \rightarrow \gamma_3(G)$$

is bilinear. It follows that $\gamma_2(G)^p$ is contained in $\Gamma(G)$, and so, $\gamma_2(G)/\gamma_3(G)$ being cyclic, we get that $\Gamma(G) = \gamma_2(G)^p \gamma_3(G)$ has index p in G . \square

Proposition 4.4. *Assume that G has class 3, $\gamma_2(G)/\gamma_3(G)$ is cyclic, and $\gamma_3(G)$ is elementary abelian. Let, moreover, H be a group such that $kG \cong kH$. Then H has class 3, the quotient $\gamma_2(H)/\gamma_3(H)$ is cyclic, $\gamma_2(G) \cong \gamma_2(H)$, and $\gamma_3(H)$ is elementary abelian.*

Proof. Thanks to the list in Section 2.4, we know that

- (1) $G/\gamma_2(G) \cong H/\gamma_2(H)$,
- (2) $\Gamma(G) \cong \Gamma(H)$,
- (3) for each n , $D_n(\gamma_2(G))/D_{n+1}(\gamma_2(G)) \cong D_n(\gamma_2(H))/D_{n+1}(\gamma_2(H))$.

From (1) and (2) combined with Lemma 4.3, we derive that $\Gamma(H)$ is maximal in $\gamma_2(H)$, and in particular, H has class at least 2 and $\gamma_2(H)$ is abelian. We next show that $\gamma_3(H)$ is contained in $\Gamma(H)$; for a contradiction, we assume that this is not the case. It follows that $\gamma_2(H) = \Gamma(H)\gamma_3(H)$, and so, $\Gamma(H)$ being central in H , we get that

$$\gamma_3(H) = [H, \gamma_2(H)] = [H, \Gamma(H)\gamma_3(H)] = [H, \gamma_3(H)] = \gamma_4(H).$$

In particular, H has class 2, contradicting Section 2.4 (8). This proves that H has class 3. The fact that the abelian groups $\gamma_2(G)$ and $\gamma_2(H)$ are isomorphic follows from (3).

We now claim that $\Gamma(H) = \gamma_2(H)^p \gamma_3(H)$. For this, assume first that $\gamma_2(H)$ does not have exponent p . We remark that, by Lemma 4.3, we have that

$$\Gamma(G) = \gamma_2(G)^p \gamma_3(G),$$

and $\gamma_2(G)/\gamma_3(G)$ being cyclic, we also have that $\Gamma(G) = \mu_{\exp(\gamma_2(G))/p}(\gamma_2(G))$. Given the isomorphism type of $\gamma_2(G)$, this is the only subgroup of $\gamma_2(G)$ that is isomorphic to $\Gamma(G)$. It follows from (2) that

$$\Gamma(H) = \mu_{\exp(\gamma_2(H))/p}(\gamma_2(H)) = \gamma_2(H)^p \gamma_3(H)$$

and thus that $\gamma_2(H)/\gamma_3(H)$ is cyclic. Now, $\gamma_2(H)^p$ and $\gamma_3(H)$ being central, we have that

$$\gamma_3(H)^p = [H, \gamma_2(H)]^p = [H, \gamma_2(H)^p] = 1,$$

equivalently $\gamma_3(H)$ has exponent p .

Assume now that $\gamma_2(G)^p = 1$. Then $\gamma_2(G)$ is elementary abelian and so is $\gamma_2(H)$. In particular, $\gamma_3(H)$ is elementary abelian. Now, relying on Section 2.4 (6), the (Sandling) quotients $G/\gamma_3(G)$ and $H/\gamma_3(H)$ are isomorphic, and so we have $|\gamma_3(G)| = |\gamma_3(H)|$. Since $\gamma_2(G)/\gamma_3(G)$ is cyclic, the equalities

$$|\gamma_2(G) : \gamma_3(G)| = p = |\gamma_2(H) : \gamma_3(H)|$$

hold, proving that $\gamma_2(H)/\gamma_3(H)$ is cyclic. □

Lemma 4.5. *Let X be a 2-generated p -group of class 3 such that $\gamma_3(X)$ is elementary abelian. Let, moreover, J_X be a subgroup of X containing*

$$T = \Phi(\gamma_2(X)) \cap \gamma_3(X)$$

such that $J_X/T = C_{X/T}(\gamma_2(X)/T)$. Then the following hold:

- (1) $p \leq |\gamma_3(X)| \leq p^2$;
- (2) $|X : J_X| = p$;
- (3) if $|\gamma_3(X)| = p^2$, then $\Phi(X) \neq X^p \gamma_3(X)$.

Proof. Since X is 2-generated, the quotient $\gamma_2(X)/\gamma_3(X)$ is cyclic, and thus the commutator map induces a surjective homomorphism

$$X/\Phi(X) \otimes \gamma_2(X)/\Gamma(X) \rightarrow \gamma_3(X).$$

As a consequence of Lemma 4.3, the index $|\gamma_2(X) : \Gamma(X)|$ is p , and thus we have $|\gamma_3(X)| \leq |X/\Phi(X)| = p^2$. Since X is assumed to have class 3, we also have $|\gamma_3(X)| \geq p$. Let $\varphi: X \rightarrow X/T$ be the natural projection. It follows from (1) and the fact that $\gamma_2(X)/\gamma_3(X)$ is cyclic that $\gamma_3(\varphi(X))$ has order p . Now, the commutator map induces a non-degenerate bilinear map

$$\varphi(X)/\varphi(J_X) \times \gamma_2(\varphi(X))/\Gamma(\varphi(X)) \rightarrow \gamma_3(\varphi(X)),$$

and so, $\gamma_3(\varphi(X))$ having order p , we derive $|X : J_X| = |\gamma_2(X) : \Gamma(X)| = p$. To conclude, assume that $|\gamma_3(X)| = p^2$ and, for a contradiction, $\Phi(X) = X^p\gamma_3(X)$. Then the commutator map induces a bilinear map

$$X/\Phi(X) \times X^p\gamma_3(X)/\Gamma(X) \rightarrow \gamma_3(X)$$

whose image generates $\gamma_3(X)$. From the fact that $\gamma_3(X)$ is elementary abelian, we get that the last bilinear map has a non-trivial right kernel, and thus $|\gamma_3(X)|$ has order at most $p^{1 \cdot \log_p |X^p\gamma_3(X) : \Gamma(X)|} = p$, a contradiction. \square

The remaining part of this section will be devoted to the proof of Theorem 4.1. To this end, the following *assumptions* will hold until the end of Section 4. Assume p is odd, and let H be a p -group such that $kG \cong kH$. Assume, additionally, that G is 2-generated with $\gamma_3(G)$ central of exponent p . Without loss of generality, we assume that $kG = kH$, and so we view G and H as group bases of the same modular group algebra. If the class of G is smaller than 3, then it follows from [9] that $G \cong H$ and in particular Theorem 4.1 holds. We assume that G has class 3.

From group theoretical invariants and Proposition 4.4, we know that H is 2-generated of class 3, $\gamma_2(G) \cong \gamma_2(H)$, and $\gamma_3(H)$ is elementary abelian. We will show that $|\gamma_3(G)| = |\gamma_3(H)|$. For a contradiction, we *assume* that $|\gamma_3(G)| < |\gamma_3(H)|$.

We fix the notation. Let g_G, h_G and g_H, h_H be generators of G and H , respectively. In case it is clear which group we are considering, we will omit indices. As a consequence of Lemma 4.5 (2), we assume without loss of generality that h_G and h_H are elements of J_G and J_H , respectively. Set $c = [g, h]$, and let p^{t+1} denote the order of c . Observe that, thanks to Lemma 4.5 (1), we have that $|\gamma_3(G)| = p$ and $|\gamma_3(H)| = p^2$. Summarizing, in both groups, we have

$$c = [g, h], \quad |c| = p^{t+1}, \quad [c, g] = d \neq 1, \quad d^p = 1,$$

while, up to possible rescaling (namely up to possibly replacing g_H with a power), the following hold independently:

$$\begin{aligned} [c_G, h_G] &= 1, & \gamma_3(G) &= \langle [c_G, g_G] \rangle = \langle d_G \rangle, \\ [c_H, h_H] &= c_H^{p^t}, & \gamma_3(H) &= \langle [c_H, h_H], [c_H, g_H] \rangle = \langle c_H^{p^t} \rangle \times \langle d_H \rangle. \end{aligned}$$

From the fact that $\gamma_2(G)$ and $\gamma_2(H)$ are isomorphic, it follows that

$$\gamma_2(G) = \langle c_G \rangle \times \langle d_G \rangle \quad \text{and} \quad \gamma_2(H) = \langle c_H \rangle \times \langle d_H \rangle.$$

Moreover, from Lemma 2.1, we derive that $[G^{p^{t+1}}, G] = [H^{p^{t+1}}, H] = 1$, while, for any integer i , the following hold:

$$[h^i g^{p^t}, h] \neq 1 \quad \text{and} \quad [g, h^{p^t} g^i] \neq 1.$$

Let $G^{\text{ab}} = G/\gamma_2(G)$ denote the abelianization of G , as in Section 2.5, and let

$$\pi: G \rightarrow G/G^{p^{t+1}} \gamma_2(G) \cong G^{\text{ab}}/(G^{\text{ab}})^{p^{t+1}}$$

denote the natural projection. Then $\pi(g_G)$ and $\pi(h_G)$ both have order p^{t+1} and $\pi(G) = \langle \pi(g_G) \rangle \oplus \langle \pi(h_G) \rangle$. It follows, for every $\ell \leq t + 1$, that

$$(G^{p^\ell} \setminus G^{p^{t+1}}) \cap \gamma_2(G) \subseteq \langle c_G^{p^\ell} \rangle,$$

and an analogous statement can be derived for H by looking at $H/H^{p^{t+1}} \gamma_2(H)$. Note that, if $t = 0$, then Section 2.4 (6) yields that $G \cong H$, and so Theorem 4.1 follows. We assume that $t \geq 1$. We fix, moreover, r to be an integer such that, for any other integer r_0 , one has $\text{wt}(c_G^r d_G) \geq \text{wt}(c_G^{r_0} d_G)$.

Lemma 4.6. *The following hold:*

- (1) $\text{wt}(c_G) = \text{wt}(c_H) = 2$;
- (2) for each $\ell \leq t$, one has $\text{wt}(g_G^{p^\ell}) = \text{wt}(h_G^{p^\ell}) = \text{wt}(g_H^{p^\ell}) = \text{wt}(h_H^{p^\ell}) = p^\ell$;
- (3) for $X \in \{G, H\}$, there exists a Jennings tuple $\mathcal{J} = (g_1, \dots, g_m)$ of X satisfying

$$\{g_1, \dots, g_m\} \supseteq \{g, g^p, \dots, g^{p^t}, h, h^p, \dots, h^{p^t}, c, c^p, \dots, c^{p^t}\} \cup \begin{cases} \emptyset & \text{if } X = H, \\ \{c^r d\} & \text{if } X = G, \end{cases}$$

and, if $i, j \in \{1, \dots, m\}$ and $\ell \leq t$ are such that $g_i = h^{p^\ell}$ and $g_j = g^{p^\ell}$, then $i < j$.

Proof. To lighten the notation, we will avoid the use of indices in this proof.

(1) Thanks to Lemma 4.5 (3), the element c is not a product of p -th powers and has thus weight 2.

(2) Since g^{p^t} and h^{p^t} are not elements of the derived subgroup, we have, for all $\ell \leq t$, that $\text{wt}(g^{p^\ell}) = \text{wt}(h^{p^\ell}) = p^\ell$.

(3) We will prove the existence of \mathcal{J} for $X = G$; similar arguments apply to H . We define

$$\tau = \{g, g^p, \dots, g^{p^t}, h, h^p, \dots, h^{p^t}, c, c^p, \dots, c^{p^t}\}.$$

To show that the elements of τ figure as entries of a Jennings tuple of G , we shall show that elements of τ with the same weight i in G are linearly independent modulo $D_{i+1}(G)$. For non-negative integers $i, j < t$, it follows from the properties of the dimension subgroups that $\text{wt}(g^{p^i}) = \text{wt}(g^{p^j})$ if and only if $i = j$; analogously, it holds that

$$\text{wt}(h^{p^i}) = \text{wt}(h^{p^j}) \quad \text{or} \quad \text{wt}(c^{p^i}) = \text{wt}(c^{p^j})$$

if and only if $i = j$.

We proceed by showing that, for any $\ell \leq t$, the weight of c^{p^ℓ} is different from the weight of any other element in τ . If $\text{wt}(c^{p^\ell}) = 2p^\ell$, the same argument as above yields the claim. Assume now that, for some $\ell \leq t$, one has

$$\text{wt}(c^{p^\ell}) \neq 2p^\ell,$$

equivalently that $c^{p^\ell} \in D_{2p^\ell+1}(G) = G^{p^{\ell+1}}$. From the inclusion

$$(G^{p^{\ell+1}} \setminus G^{p^{\ell+1}}) \cap \gamma_2(G) \subseteq \langle c^{p^{\ell+1}} \rangle,$$

we conclude that $c^{p^\ell} \in G^{p^{\ell+1}}$, and so c^{p^ℓ} has weight larger than that of any element in the set $\{g, g^p, \dots, g^{p^t}, h, h^p, \dots, h^{p^t}\}$.

We have proven that the only elements in τ having the same weight come in pairs (g^{p^ℓ}, h^{p^ℓ}) for $\ell \leq t$. Moreover, two elements g^{p^ℓ} and h^{p^ℓ} are linearly independent in $D_{p^\ell}(G)/D_{p^\ell+1}(G)$ as they span the 2-dimensional k -vector space $(G^{\text{ab}})^{p^\ell}/(G^{\text{ab}})^{p^{\ell+1}}$. In the choice of the Jennings tuple \mathcal{J} , we take without loss of generality h^{p^ℓ} to precede g^{p^ℓ} .

We finally assume, for a contradiction, that $c^r d$ has the same weight as some other element of τ . Note that, as $d \in \gamma_3(G)$, we have $\text{wt}(c^r d) \geq 3$. If $\text{wt}(c^r d) = 3$, we are reduced to considering the case $p = 3$ and showing that g^3, h^3 , and $c^r d$ are linearly independent in $D_3(G)/D_4(G) = G^3\gamma_2(G)^3\gamma_3(G)/G^9\gamma_2(G)^3$. Now, if g^3, h^3 , and $c^r d$ are linearly dependent, then there exist integers $0 \leq i_1, i_2, i_3 \leq 2$, of which at least two are non-zero modulo 3, such that

$$(h^3)^{i_1} (g^3)^{i_2} (c^r d)^{i_3} \in G^9\gamma_2(G)^3.$$

It then follows that $\pi((h^3)^{i_1} (g^3)^{i_2}) \in (G^{\text{ab}})^9$, contradicting the structure of $\pi(G)$.

Assume now, for some integer s , that $\text{wt}(c^r d) = p^s > 3$. It follows that

$$c^r d \in G^{p^s} \setminus G^{p^{s+1}}.$$

If $s \leq t$, then the inclusion

$$(G^{p^{s+1}} \setminus G^{p^{t+1}}) \cap \gamma_2(G) \subseteq \langle c^{p^{s+1}} \rangle$$

provides a contradiction. So $s \geq t + 1$, and in particular, $c^r d$ has weight different from the weights of any g^{p^ℓ}, h^{p^ℓ} with $\ell \leq t$. In conclusion, if, for some $\ell \leq t$, the elements $\overline{c^r d}$ and c^{p^ℓ} are linearly dependent modulo $D_{\text{wt}(c^r d)+1}(G)$, there is an integer m such that $\text{wt}(c^r d(c^{p^\ell})^m) > \text{wt}(c^r d)$, contradicting the choice of r . \square

We fix Jennings tuples of G and H and assume them to satisfy the properties listed in Lemma 4.6. Let, moreover, m be an integer such that, for any integer m_0 , one has

$$\text{wt}(c_G^{p^t} d_G^m) \geq \text{wt}(c_G^{p^t} d_G^{m_0}).$$

Set $w = \text{wt}(c_G^{p^t} d_G^m)$, and observe that

$$\text{wt}(c_G) > \text{wt}(c_G^p) > \dots > \text{wt}(c_G^{p^t}) \geq \text{wt}(c^{p^t} d^m) = w.$$

In particular, no element among $c_G, c_G^p, \dots, c_G^{p^t}$ has weight bigger than w .

Until the end of this section, let \mathcal{K} be the smallest ideal of kG containing $\overline{d_G}$ and $I(kG)^{2w}$. We define

$$Z = Z(kG) + \mathcal{K}/\mathcal{K} \quad \text{and} \quad \mu_p^0(Z) = \{a \in Z \mid a^p = 0\}.$$

By abuse of notation, we will denote the elements of Z as they were elements of kG . Then $\mu_p^0(Z)$ is a k -vector space containing

$$\overline{c_G^{p^t}}, \quad \overline{c_H^{p^t}}, \quad \text{and} \quad \overline{d_H}$$

in which, by definition of \mathcal{K} , the image of $\overline{c_G^{p^t}}$ is non-trivial (see also (4.1) below). We fix a subspace L of $\mu_p^0(Z)$ such that

$$\mu_p^0(Z) = \overline{\langle c_G^{p^t} \rangle} \oplus L$$

and let \mathcal{L} be the ideal of kG containing \mathcal{K} such that $\mathcal{L}/\mathcal{K} = L$. There then exist α and β in k such that

$$\overline{d_H} \equiv \alpha \overline{c_G^{p^t}} \pmod{\mathcal{L}} \quad \text{and} \quad \overline{c_H^{p^t}} \equiv \beta \overline{c_G^{p^t}} \pmod{\mathcal{L}}.$$

Moreover, modulo \mathcal{L} , the following equalities hold:

$$\begin{aligned} 0 \not\equiv \overline{c_G^{p^t} d^m} &= \overline{c_G^{p^t}} + \overline{d^m} + \overline{c_G^{p^t} d^m} \equiv \overline{c_G^{p^t}} \pmod{\mathcal{L}}, \\ \text{and therefore} \quad 0 &\equiv \overline{c_G^{p^t} d^{m^2}} \equiv \overline{c_G^{p^t} d^2} \pmod{\mathcal{L}}. \end{aligned} \tag{4.1}$$

We let $\varphi_L: kG \rightarrow kG/\mathcal{L}$ be the canonical projection.

Lemma 4.7. *One has $\beta \neq 0$.*

Proof. Write $|G| = p^m$, and denote by $\mathcal{J} = (g_1, \dots, g_m)$ the chosen Jennings tuple of G . As remarked in Section 2.3, any element of G can be written as

$$\prod_{i=1}^m g_i^{\alpha_i} \quad \text{with } 0 \leq \alpha_i \leq p - 1.$$

Let \tilde{w} be the weight of $\overline{c_H^{p^t}}$ and note that, by the theory of Zassenhaus ideals, cf. Section 2.3, we can write

$$\overline{c_H^{p^t}} = \bar{a} + y, \quad \text{where } a \in D_{\tilde{w}}(G), \ y \in I(kG)^{\tilde{w}+1}.$$

Let $0 \leq \alpha_1, \dots, \alpha_m \leq p - 1$ be such that $a = \prod_{i=1}^m g_i^{\alpha_i}$. Thanks to Lemma 2.2, we have

$$\bar{a} = \sum_{i=1}^m \alpha_i \overline{g_i} + r,$$

where the Jennings basis elements in the support of r are products of at least two elements from $\overline{\mathcal{J}}$ and are linearly independent from the elements in $\overline{\mathcal{J}}$. Note that the weight of \bar{a} is the smallest weight among the weights of $\overline{g_i}$'s satisfying $\alpha_i \neq 0$. As the weight of \bar{a} is equal to \tilde{w} , we conclude that $\alpha_i = 0$ whenever the weight of $\overline{g_i}$ is smaller than \tilde{w} and there must exist an i such that $\overline{g_i}$ has weight \tilde{w} and $\alpha_i \neq 0$.

Observe now that

$$\overline{c_H^{p^t}} \in kGI(k\gamma_2(G)),$$

as the ideal $kGI(k\gamma_2(G))$ is canonical. It follows that, in the expression of $\overline{c_H^{p^t}}$ as linear combination of elements in the Jennings basis on \mathcal{J} , each support element features a factor from $\gamma_2(G)$, cf. Section 2.3. In particular, if the weight of $\overline{g_i}$ is \tilde{w} and $\alpha_i \neq 0$, then $g_i \in \gamma_2(G)$.

We write $\overline{c_H} \in kGI(k\gamma_2(G))$ since $\overline{c_H} = \delta_1 \overline{c_G} + \delta_2 \overline{d_G}$ for some $\delta_1, \delta_2 \in kG$. As $\gamma_2(G)$ is abelian and $\overline{d_G^p} = 0$, Lemma 2.2 yields elements $\varepsilon_0, \dots, \varepsilon_{p-1} \in kG$ such that

$$\overline{c_H^{p^t}} = \overline{c_H}^{p^t} = (\delta_1 \overline{c_G} + \delta_2 \overline{d_G})^{p^t} = \sum_{j=0}^{p-1} \varepsilon_j \overline{c_G}^{p^t-j} \overline{d_G}^j.$$

As d_G is central in G and $[\overline{c_G}, kG] \subseteq kG\overline{d_G}$, the elements of \mathcal{J} in the support of $\varepsilon_j \overline{c_G}^{p^t-j} \overline{d_G}^j$ have at least p^t factors from $\{\overline{c_G}, \overline{d_G}\}$. However, at the same

time, there is an element $\overline{g_i}$ in the support of \bar{a} such that $g_i \in \gamma_2(G)$, i.e. $\overline{g_i}$ is an element from

$$\{\overline{c_G}, \dots, \overline{c_G^{p^t}}, \overline{c_G^r d_G}\}.$$

It follows that, if $g_i = c_G^{p^t}$, then $\alpha_i \neq 0$ and in particular $\beta \neq 0$. □

Lemma 4.8. *There exists $\delta \in k$ such that $d_H(c_H^{p^t})^\delta \equiv 1 \pmod{\mathcal{L}}$.*

Proof. Define $\delta = -\alpha\beta^{-1}$ and observe that δ is well-defined thanks to Lemma 4.7. As a consequence of (4.1), one has

$$\overline{c_H^{p^t}{}^2} \equiv 0 \pmod{\mathcal{L}},$$

and so we compute

$$\begin{aligned} \overline{d_H(c_H)^{\delta p^t}} &\equiv \overline{d_H} + \delta \overline{c_H^{p^t}} + \delta \overline{d_H} \cdot \overline{c_H^{p^t}} \\ &\equiv \alpha \overline{c_G^{p^t}} + \delta \beta \overline{c_G^{p^t}} + \alpha \beta \delta \overline{c_G^{p^t}{}^2} \equiv 0 \pmod{\mathcal{L}}. \end{aligned}$$

Removing bars yields the claim. □

For the remaining part of Section 4, let \mathbb{A} denote the algebra

$$\mathbb{A} = kG/\mathcal{L} = kH/\mathcal{L}.$$

If $\overline{d_H} \notin \mathcal{L}$, then we replace g_H by $g_H h_H^\delta$, where δ is chosen as in Lemma 4.8. This choice has no influence on the results from this section; nonetheless, it guarantees that $\overline{d_H} \in \mathcal{L}$. In particular, the images of $\overline{g_H}$ and $\overline{c_H}$ in \mathbb{A} commute. Our strategy is to show that the ideal $[\mathbb{A}, \mathbb{A}]\mathbb{A} \cap Z(\mathbb{A})$ has conflicting properties, when viewed as an ideal of kG/\mathcal{L} or kH/\mathcal{L} , respectively. The choice of the ideal is inspired by Sandling’s argument [29, Lemma 6.10] relying on the ideal

$$[kX, kX]kX \cap Z(kX)$$

of kX to show that the isomorphism type of $\Gamma(X)$ is an invariant of kX ; cf. Section 2.4 (5). We point out that, under our assumptions, we have indeed that

$$\Gamma(\varphi_L(G)) \not\cong \Gamma(\varphi_L(H)).$$

Compared to [29, Lemma 6.10], however, we do not have a well-understood basis of the center of \mathbb{A} resulting in more complicated calculations on our side.

Lemma 4.9. *There exists $x \in I(kG)^3 \cap kGI(\gamma_2(kG))$ such that*

$$\varphi_L(\overline{c_H} + x) \in [\mathbb{A}, \mathbb{A}]\mathbb{A} \cap Z(\mathbb{A})$$

and $[x, \overline{c_G}] \equiv [x, \overline{c_H}] \equiv [x, \overline{g_H}] \equiv 0 \pmod{\mathcal{L}}$ hold.

Proof. The elements $\overline{c_G}$ and $\overline{c_H}$ both belong to the canonical ideal $kGI(k\gamma_2(G))$ and have weight 2; moreover, modulo $I(kG)^3$, they are, up to invertible scalars, unique with this property. It follows that there exist elements

$$x \in I(kG)^3 \cap kGI(\gamma_2(kG)) \quad \text{and} \quad \lambda \in k^*$$

such that

$$\varphi_L(\overline{c_H} + x) = \varphi_L(\lambda \overline{c_G}) \in [\mathbb{A}, \mathbb{A}]\mathbb{A} \cap Z(\mathbb{A}).$$

For such an x , we use the facts that $\varphi_L(\overline{c_G})$ is central and $[\varphi_L(\overline{c_H}), \varphi_L(\overline{g_H})] = 0$ to derive that

$$0 = [\varphi_L(x), \varphi_L(\overline{c_G})] = [\varphi_L(x), \varphi_L(\overline{c_H})] = [\varphi_L(x), \varphi_L(\overline{g_H})]. \quad \square$$

Proof of Theorem 4.1. We will show that the element x introduced in Lemma 4.9 cannot exist, which will provide a contradiction to $kG = kH$.

As a generating set of \mathbb{A} as a vector space, we will use the image under φ_L of the Jennings basis of $kG = kH$ obtained from the Jennings tuple of H . To lighten the notation, we will drop the index H in our calculations. Moreover, we will abuse notation and denote the elements of \mathbb{A} in the same way we denote elements in kH , e.g. we will write $\overline{d} = 0$. As $x \in [\mathbb{A}, \mathbb{A}]\mathbb{A}$, any base element in the support of x features a factor \overline{c} and has weight at least 3. Moreover, as a consequence of Lemma 4.9, the element $\overline{c} + x$ is central, so in particular $(\overline{c} + x)^h = \overline{c} + x$. From the equalities $[c, h] = c^{p^t}$ and $[g, h] = c$ and Lemma 2.2, we derive

$$\overline{c}^h = \overline{c} + \overline{c}^{p^t} + \overline{c} \overline{c}^{p^t} \quad \text{and} \quad \overline{g}^h = \overline{g} + \overline{c} + \overline{g} \overline{c}, \tag{4.2}$$

from which it follows that

$$x^h - x = \overline{c} - \overline{c}^h = -\overline{c}^{p^t} - \overline{c} \overline{c}^{p^t}. \tag{4.3}$$

We will show that (4.3) cannot hold. We start by showing that, to this aim, we can restrict our computations to a specific subset of the support elements of x . We can ignore central base elements because they do not contribute to $x^h - x$. Moreover, if a support element y contains a factor from $\{\overline{h}, \overline{h}^p, \dots, \overline{h}^{p^t}\}$, then, as a consequence of (4.2) and the choice of the Jennings basis, this factor will also be present in any support element of y^h . Finally, assume that y is in the support of x and contains a central factor from $H^{p^{t+1}}$ which does not lie in $\gamma_2(H)$. Then the projection of $y^h - y$ onto the linear subspace spanned by

$$\overline{c}^{p^t} \quad \text{and} \quad \overline{c} \overline{c}^{p^t}$$

is 0 as this central factor cannot be eliminated by conjugation. So considering y cannot influence the satisfiability of (4.3).

To show that x cannot satisfy (4.3), we assume without loss of generality that each element y in the support of x is of the form $\bar{g}^i \bar{c}^j$, where i and j are non-negative integers with $j > 0$. The positivity of j follows from x being in $[\mathbb{A}, \mathbb{A}]\mathbb{A}$, and we have used the intercommutativity of \bar{g} and \bar{c} to simplify the notation. Each such support element y can be written as

$$y = \bar{g}^{i_0} \overline{g^{p^{i_1}}} \dots \overline{g^{p^t i_t}} \bar{c}^{j_0} \overline{c^{p^{j_1}}} \dots \overline{c^{p^t j_t}},$$

where $0 \leq i_0, \dots, i_t, j_0, \dots, j_t < p$ and

$$i_0 + pi_1 + \dots + p^t i_t = i \quad \text{and} \quad j_0 + pj_1 + \dots + p^t j_t = j$$

are the p -adic expansions of i and j . Following this notation, we compute

$$y^h = (\bar{g} + \bar{c} + \overline{g\bar{c}})^{i_0} \dots (\overline{g^{p^t} + c^{p^t}} + \overline{g^{p^t} c^{p^t}})^{i_t} (\bar{c} + c^{p^t} + \overline{c c^{p^t}})^{j_0} \overline{c^{p^{j_1}}} \dots \overline{c^{p^t j_t}}. \tag{4.4}$$

Now, if a certain $y = \bar{g}^i \bar{c}^j$ is in the support of x and the support of $y^h - y$ contains an element \tilde{y} different from c^{p^t} and $\bar{c}c^{p^t}$, then there must be another support element y' in x such that $(y')^h - y'$ also contains \tilde{y} in its support. Relying on the last observation, we will show that y is not in the support of x for $1 \leq i, j \leq p^t - 1$. Note that it is sufficient to show that no y satisfying these conditions on i and j is an element in the support of x as only in these cases $y^h - y$ can contain c^{p^t} as an element in the support and c^{p^t} is an element necessary for (4.3) to hold. Our restrictions, in particular, imply $i_t = j_t = 0$ in (4.4).

We will prove the impossibility of any such y coming up in the support of x by induction on triples of the form (ℓ, j, r) , where $i = p^\ell(sp - r)$ for some integer s , ordered lexicographically. Observe that the entries of such triples range over

$$0 \leq \ell \leq t - 1, \quad 1 \leq j \leq p^t - 1, \quad 1 \leq r \leq p - 1.$$

When considering $y^h - y$, note that the elements in the support are those which can be gotten from multiplying explicitly in (4.4) with the exception of the element

$$\bar{g}^{i_0} \dots \overline{g^{p^t i_t}} \bar{c}^{j_0} \dots \overline{c^{p^t j_t}} = y.$$

In particular, working with the factor $(\bar{c} + c^{p^t} + \overline{c c^{p^t}})^{j_0} \overline{c^{p^{j_1}}} \dots \overline{c^{p^t j_t}}$ in (4.4), we derive the following trick.

Trick. If $y^h - y$ contains an element $\bar{g}^{i'} \bar{c}^{j'}$ in its support with $j' < j + p^t - 1$, then at least one of the factors in $\bar{c}^{j'}$ comes from the product

$$(\bar{g} + \bar{c} + \overline{g\bar{c}})^{i_0} \dots (\overline{g^{p^t} + c^{p^t}} + \overline{g^{p^t} c^{p^t}})^{i_t}.$$

Note that, if j' is of the form $j' \leq j + p^\ell$ for some ℓ belonging to the induction range, then the trick is always applicable.

For the induction base, assume $(\ell, j, r) = (0, 1, 1)$. Then, for some s , we have $i = sp - 1$ and the element $\bar{g}^{sp-1}\bar{c}^2$ is in the support of $y^h - y$ and y is the only element with this property. Indeed, let $y' = \bar{g}^{i'}\bar{c}^{j'}$ be such that $\bar{g}^{sp-1}\bar{c}^2$ is in the support of $y'^h - y'$, and compute

$$(y')^h = (\bar{g} + \bar{c} + \bar{g}\bar{c})^{i'_0} \dots (\overline{g^{p^t} + c^{p^t}} + \overline{g^{p^t} c^{p^t}})^{i'_t} (\bar{c} + c^{p^t} + \bar{c}c^{p^t})^{j'_0} \overline{c^{p^t}}^{j'_1} \dots c^{p^t j'_t}. \tag{4.5}$$

As the support of $(y')^h - y'$ contains an element featuring the factor \bar{c} exactly twice, we deduce that $1 \leq j' \leq 2$. Moreover, the factor

$$(\overline{g^{p^t} + c^{p^t}} + \overline{g^{p^t} c^{p^t}})^{i'_1} \dots (\overline{g^{p^t} + c^{p^t}} + \overline{g^{p^t} c^{p^t}})^{i'_t}$$

does not contribute a factor \bar{c} , as the smallest available factor is \bar{c}^p . The factor \bar{g}^{sp-1} can only be obtained from the subproduct

$$(\bar{g} + \bar{c} + \bar{g}\bar{c})^{i'_0} \dots (\overline{g^{p^t} + c^{p^t}} + \overline{g^{p^t} c^{p^t}})^{i'_t},$$

and $(\bar{g} + \bar{c} + \bar{g}\bar{c})^{i'_0}$ being the only candidate able to contribute a factor \bar{c} , the index i' must equal $ps - 1$. Combining the trick with the fact that one factor \bar{c} is contributed by

$$(\bar{c} + c^{p^t} + \bar{c}c^{p^t})^{j'_0} \overline{c^{p^t}}^{j'_1} \dots c^{p^t j'_t},$$

we conclude that $j' = 1$.

We proceed with the induction step. Write $i = p^\ell(sp - r)$, and assume that the triples satisfying $(\ell', j', r') < (\ell, j, r)$ have been excluded. We claim that the element $\bar{g}^{p^\ell(sp-r)}\bar{c}^{j+p^\ell}$ is in the support of $y^h - y$ and assume that this element also appears in the support of $y'^h - y'$ for some y' , presented as in (4.5) and associated to the triple (ℓ', j', r') . It follows from the induction hypothesis that $i'_0 = \dots = i'_{\ell-1} = 0$. We note that, for the factor $\bar{g}^{p^\ell(sp-r)}$ to be realizable, it is necessary that $i'_\ell \neq 0$ and $\ell' = \ell$. The induction hypothesis yields $j' \geq j$, and the factor

$$(\overline{g^{p^{\ell+1}} + c^{p^{\ell+1}}} + \overline{g^{p^{\ell+1}} c^{p^{\ell+1}}})^{i'_{\ell+1}} \dots (\overline{g^{p^t} + c^{p^t}} + \overline{g^{p^t} c^{p^t}})^{i'_t}$$

cannot contribute to the factor $\bar{c}^{j'}$ as its minimum contribution would be $\bar{c}^{p^{\ell+1}}$. On the other hand, since $j' \leq j + p^\ell$, the trick ensures that the product

$$(\bar{g} + \bar{c} + \bar{g}\bar{c})^{i'_0} \dots (\overline{g^{p^t} + c^{p^t}} + \overline{g^{p^t} c^{p^t}})^{i'_t}$$

contributes the factor $\bar{c}^{j'}$. The minimum contribution is \bar{c}^{p^ℓ} , as

$$i'_0 = \dots = i'_{\ell-1} = 0.$$

The maximal possible contribution being \bar{c}^{j+p^ℓ} , we conclude that $j = j'$. It follows from the induction hypothesis that $r' \geq r$. In particular, to obtain the factor $\bar{g}^{p^\ell(s-p-r)}$, the product

$$(\bar{g} + \bar{c} + \bar{g}\bar{c})^{i'_0} \dots (\bar{g}^{p^t} + \bar{c}^{p^t} + \bar{g}^{p^t} \bar{c}^{p^t})^{i'_t}$$

has to contribute the maximal amount of possible factors \bar{g} at the same time, i.e. contributing only p^ℓ times the factor \bar{c} . We deduce that $r' = r$.

In order to conclude the proof, we shall make sure that the elements of the form $\bar{g}^{p^\ell(s-p-r)}\bar{c}^{j+p^\ell}$ used in the arguments above are not congruent to 0 modulo \mathcal{L} . None of such elements is central as an element of kG , as $p^\ell(s-p-r) < p^t$, and so they do not lie in $\mu_p^0(Z)$, if they do not lie in \mathcal{K} itself. We will consider their weights to determine if they lie in \mathcal{K} , taking into account that an element c^{p^ℓ} might have smaller weight than $c^{p^\ell}d^u$ for some integer u ; even these two elements are congruent modulo \mathcal{K} .

Among the elements in consideration, the ones of shape $\bar{g}^{p^\ell(s-p-1)}\bar{c}^{j+p^\ell}$ have biggest weight, so we will ignore the case $r > 1$. As we have $p^\ell(s-p-1) < p^{t+1}$, Lemma 4.6 implies that

$$\text{wt}(\bar{g}^{p^\ell(s-p-1)}) = p^\ell(s-p-1).$$

Moreover, the weight of \bar{c} being 2, the maximal possible weight of an element $\bar{g}^{p^\ell(s-p-1)}\bar{c}^{j+p^\ell}$ is realized when $\ell = t-1$ and $j = p^t - 1$. We define

$$z = \bar{g}^{p^t-p^{t-1}}\bar{c}^{p^t+p^{t-1}-1},$$

which comes up when, in the induction process, we exclude $\bar{g}^{p^t-p^{t-1}}\bar{c}^{p^t-1}$. We claim that $\text{wt}(z) < 2w$. Erasing the factor c^{p^t} of weight not larger than w , Lemma 4.7 yields the translation of the claim into $\text{wt}(\bar{g}^{p^t-p^{t-1}}\bar{c}^{p^t-1-1}) < w$. As noted above, the weight of $\bar{g}^{p^t-p^{t-1}}$ is $p^t - p^{t-1}$. Now let u be an integer such that, for any integer u_0 , one has

$$w' = \text{wt}(c^{p^{t-1}}d^u) \geq \text{wt}(c^{p^{t-1}}d^{u_0}).$$

It follows that $w \geq pw'$ and, the weight of \bar{c} being 2, that $w' \geq 2p^{t-1}$. From the last observations, we derive

$$\begin{aligned} \text{wt}(\bar{g}^{p^t-p^{t-1}}\bar{c}^{p^t-1-1}) &\leq \text{wt}(\bar{g}^{p^t-p^{t-1}}\bar{c}^{p^t-1}) \\ &\leq \text{wt}(\bar{g}^{p^t-p^{t-1}}\overline{c^{p^{t-1}}d^u}) = p^t - p^{t-1} + w' \end{aligned}$$

$$\begin{aligned}
&\leq p^t - p^{t-1} + w - (p-1)w' \\
&\leq p^t - p^{t-1} + w - (p-1)2p^{t-1} \\
&\leq w - (p^t - p^{t-1}) < w,
\end{aligned}$$

and so the claim is proven. \square

Remark 4.10. Theorem 4.1 can be used to solve the (MIP) in some cases that cannot be handled by the known group theoretical invariants. For instance, if $G = \text{SG}(3^7, 19)$ and H is a group not isomorphic to G but sharing all group theoretical invariants with G , then $H \cong \text{SG}(3^7, 43)$. One finds that $|\gamma_3(G)| = 3$, while $|\gamma_3(H)| = 3^2$, so Theorem 4.1 yields $kG \not\cong kH$. Other examples of groups for which group theoretical invariants are not sufficient to solve the (MIP), but are when upgraded with Theorem 4.1, are

$$\begin{aligned}
&\text{SG}(3^7, 23), \text{SG}(3^7, 45), \text{SG}(3^7, 27), \text{SG}(3^7, 47), \\
&\text{SG}(5^7, 19), \text{SG}(5^7, 21), \text{SG}(5^7, 77), \text{SG}(5^7, 87), \text{SG}(5^7, 30086), \\
&\text{SG}(7^7, 23), \text{SG}(7^7, 25), \text{SG}(7^7, 111), \text{SG}(7^7, 125), \text{SG}(7^7, 104602).
\end{aligned}$$

It seems like still some work will be required to understand this evidence in a generic sense. Some of the groups listed above for which the third terms in their lower central series have the same size can only be distinguished using the so-called Roggenkamp parameter $\sum_{g \in G} \log_p(|C_G(g)/\Phi(C_G(g))|)$, where the sum runs over conjugacy classes of G . This invariant is far from easy to compute by hand in a general situation.

5 The class of obelisks

In computer-aided investigations of the (MIP) such as [12, 20, 33], one is interested in determining the smallest number m such that, given two non-isomorphic groups G and H , one has $I(kG)/I(kG)^m \not\cong I(kH)/I(kH)^m$. It follows directly from the theory of Jennings that

$$G/D_\ell(G) \cong H/D_\ell(H) \implies I(kG)/I(kG)^\ell \cong I(kH)/I(kH)^\ell.$$

The following questions are based on computational evidence.

Question 5.1. Let H be a p -group not isomorphic to G satisfying $|H| = |G|$, and let ℓ be the maximal integer such that $G/D_\ell(G) \cong H/D_\ell(H)$. Are the following statements true?

- (1) It holds that $I(kG)/I(kG)^{2\ell+1} \not\cong I(kH)/I(kH)^{2\ell+1}$ (see [7]).
- (2) If p is odd and $m = \max\{\ell, 2\ell - \frac{p-1}{2}\}$, then (see [20])

$$I(kG)/I(kG)^{m+1} \not\cong I(kH)/I(kH)^{m+1}.$$

Question 5.1 (1) has been answered negatively in [20] for groups of order 2^8 . Question 5.1 (2) is open. There are very few bins of groups of order 5^6 , which share all known group theoretical invariants and for which the upper bound given in Question 5.1 (2) is sharp [20, Section 3.3]. A family that is highlighted in this process is that of the so-called p -obelisks (see Definition 5.2 below). These groups were first investigated in [6] and later in [31]. As a first step towards understanding the modular group algebras of p -obelisks and solving the (MIP) for this class of groups, we show in this section that the property of being a p -obelisk is an invariant of the group algebra. Until the end of the present section, assume that $p > 3$.

Definition 5.2. A p -obelisk is a finite non-abelian p -group \mathcal{O} with

$$|\mathcal{O} : \gamma_2(\mathcal{O})| = p^2 \quad \text{and} \quad \mathcal{O}^p = \gamma_3(\mathcal{O}).$$

The next theorem is the main result of this section, which will be proven after Lemma 5.5.

Theorem 5.3. Let \mathcal{O} be a p -obelisk such that $kG \cong k\mathcal{O}$. Then G is a p -obelisk.

The following proposition collects known properties of p -obelisks; see for example [31, Lemmas 322-3] or [6, Theorem 4.3 and its proof] (this is also to be found in [16, III, Satz 17.9]).

Proposition 5.4. Let G be a p -obelisk of class c and i a positive integer. Then the following hold:

- (1) the quotient $\gamma_i(G)/\gamma_{i+1}(G)$ is elementary abelian of rank

$$\dim_k(\gamma_i(G)/\gamma_{i+1}(G)) = \begin{cases} 2 & \text{if } i \leq c - 1 \text{ and } i \text{ odd,} \\ 1 & \text{if } i \leq c \text{ and } i \text{ even;} \end{cases}$$

- (2) one has $\gamma_i(G)^p = \gamma_{i+2}(G)$.

Lemma 5.5. Let \mathcal{O} be a p -obelisk. Assume that n is a positive integer, and write $n = ap^\ell + b$, where $\ell \geq 0$, $1 \leq a \leq p - 1$, and $0 \leq b < p^\ell$. Then we have that $D_n(\mathcal{O}) = \gamma_{m(n)}(\mathcal{O})$, where

$$m(n) = \begin{cases} 2\ell + 1 & \text{if } a = 1 \text{ and } b = 0, \\ 2\ell + 3 & \text{if } a > 2 \text{ or } a = 2 \text{ and } b \geq 1, \\ 2\ell + 2 & \text{otherwise.} \end{cases}$$

Proof. We work by induction on n and using the iterative formula for dimension subgroups. We clearly have $D_1(\mathcal{O}) = \gamma_1(\mathcal{O})$. Moreover, from $p \geq 5$, we compute $D_2(\mathcal{O}) = \gamma_2(\mathcal{O})\mathcal{O}^p$ and $D_3(\mathcal{O}) = \gamma_3(\mathcal{O})\mathcal{O}^p$. The group \mathcal{O} being a p -obelisk, we deduce $D_2(\mathcal{O}) = \gamma_2(\mathcal{O})$ and $D_3(\mathcal{O}) = \gamma_3(\mathcal{O})$. We have proven the claim when n is equal to 1, 2, or 3.

Assume now that $n \geq 4$ and, for each $n' < n$, the equality $D_{n'}(\mathcal{O}) = \gamma_{m(n')}(\mathcal{O})$ holds. We write

$$n = ap^\ell + b \quad \text{with } \ell \geq 0, 1 \leq a \leq p-1, 0 \leq b < p^\ell.$$

Let first $a = 1$ and $b = 0$; then $n \geq 4$ implies $\ell \neq 0$, and in particular, we have $2\ell + 1 \leq p^\ell = n$. Note that, by Proposition 5.4 (2), we have

$$\gamma_{2\ell-1}(\mathcal{O})^p = \gamma_{2\ell+1}(\mathcal{O}).$$

Thanks to the inductive formula for the dimension subgroups, cf. Section 2.3, the induction hypothesis yields

$$D_n(\mathcal{O}) = D_{ap^{\ell-1}}(\mathcal{O})^p \gamma_n(\mathcal{O}) = \gamma_{2(\ell-1)+1}(\mathcal{O})^p \gamma_n(\mathcal{O}) = \gamma_{2\ell+1}(\mathcal{O}).$$

Now let $a > 2$ or $a = 2$ and $b \geq 1$. The inductive formula for the dimension subgroups combined with Proposition 5.4 and the fact that $n \geq 4$ yields

$$D_n(\mathcal{O}) = D_{ap^{\ell-1} + \lceil \frac{b}{p} \rceil}(\mathcal{O})^p \gamma_n(\mathcal{O}) = \gamma_{2(\ell-1)+3}(\mathcal{O})^p \gamma_n(\mathcal{O}) = \gamma_{2\ell+3}(\mathcal{O}).$$

We next assume that $a = 1$ and $b \geq 1$ or $a = 2$ and $b = 0$. The combination of Proposition 5.4, the induction hypothesis, and the fact that $p \geq 5$ yields

$$D_n(\mathcal{O}) = D_{ap^{\ell-1} + \lceil \frac{b}{p} \rceil}(\mathcal{O})^p \gamma_n(\mathcal{O}) = \gamma_{2(\ell-1)+2}(\mathcal{O})^p \gamma_n(\mathcal{O}) = \gamma_{2\ell+2}(\mathcal{O}). \quad \square$$

We give here the proof of Theorem 5.3. To this end and until the end of the proof, let \mathcal{O} be a p -obelisk such that $kG \cong k\mathcal{O}$. We show that G is a p -obelisk.

The (MIP) is solved for orders dividing p^5 (see [27]), so we assume without loss of generality that $|G| = |\mathcal{O}| \geq p^6$. Then, by Proposition 5.4 (1), the nilpotency class of \mathcal{O} is at least 4. From Section 2.4, we know that G and \mathcal{O} have the same order and also that $G/\gamma_2(G) \cong \mathcal{O}/\gamma_2(\mathcal{O})$; the last quotients are elementary abelian of order p^2 by Proposition 5.4 (1). In particular, $\gamma_2(G)/\gamma_3(G)$ and $\gamma_2(\mathcal{O})/\gamma_3(\mathcal{O})$ are cyclic of order p , and hence $|\gamma_2(G) : \gamma_3(G)| = |\gamma_2(\mathcal{O}) : \gamma_3(\mathcal{O})|$. Now, by Section 2.4 (4) and Lemma 5.5, we have

$$D_1(G)/D_2(G) \cong D_1(\mathcal{O})/D_2(\mathcal{O}) = \mathcal{O}/\gamma_2(\mathcal{O}).$$

From $D_2(G) = \gamma_2(G)G^p$, we then obtain $G^p \leq \gamma_2(G)$ and $D_2(G) = \gamma_2(G)$. In the same way, we get

$$D_2(G)/D_3(G) \cong D_2(\mathcal{O})/D_3(\mathcal{O}) = \gamma_2(\mathcal{O})/\gamma_3(\mathcal{O}).$$

Both

$$D_3(G) = \gamma_3(G)G^p \quad \text{and} \quad \gamma_3(G)$$

being subgroups of index p of $D_2(G) = \gamma_2(G)$, we get $G^p \subseteq \gamma_3(G)$ and, in particular, that $D_3(G) = \gamma_3(G)$. We claim that, for each integer $n \geq 3$, the following holds:

- (i) $\gamma_3(G) = G^p \gamma_n(G)$;
- (ii) $\gamma_i(G) = D_j(G)$ for all $1 \leq i \leq n$ and any j satisfying $\gamma_i(\mathcal{O}) = D_j(\mathcal{O})$.

To prove the last claim, we will work by induction on n . For *this proof only*, we will use the bar notation with a different meaning from that introduced in Section 2.2.

Assume $n = 3$. We have already proven (i), so we show (ii). By Lemma 5.5, one has $\gamma_3(\mathcal{O}) = D_j(\mathcal{O})$ if and only if $3 \leq j \leq p$. When $i \in \{1, \dots, p\}$, we get from Section 2.4 (4) that

$$D_i(\mathcal{O})/D_{i+1}(\mathcal{O}) \cong D_i(G)/D_{i+1}(G),$$

and so $\gamma_3(G) = D_j(G)$ if and only if $3 \leq j \leq p$. This proves the base case. We now assume that the claim holds for $n \geq 3$ and prove it for $n + 1$.

Assume that n is even. Set $\overline{G} = G/\gamma_{n+1}(G)$. We claim that \overline{G} is a p -obelisk. Indeed, applying in this order the induction hypothesis on (i), then on (ii), the formula for dimension subgroups, and then again (ii), one gets

$$\begin{aligned} \gamma_3(\overline{G}) &= \overline{G}^p \gamma_n(\overline{G}) = \overline{G}^p D_{2p}^{u_{\overline{2}^2}}(\overline{G}) \\ &= \overline{G}^p (D_{2p}^{u_{\overline{2}^4}}(\overline{G}))^p \gamma_{2p}^{u_{\overline{2}^2}}(\overline{G}) = \overline{G}^p \gamma_{n-2}(\overline{G})^p = \overline{G}^p. \end{aligned}$$

We have proven that \overline{G} is a p -obelisk, equivalently $\gamma_3(G) = G^p \gamma_{n+1}(G)$ and (i) holds. We continue with (ii). By Lemma 5.5, we have $D_{p\frac{n}{2}}(\mathcal{O}) = \gamma_{n+1}(\mathcal{O})$, and so the induction hypothesis on (ii) yields

$$D_{p\frac{n}{2}}(G) = D_{p\frac{n-2}{2}}(G)^p \gamma_{p\frac{n}{2}}(G) = \gamma_{n-1}(G)^p \gamma_{p\frac{n}{2}}(G).$$

Note that, by Lemma 5.5, we have that

$$\gamma_n(\mathcal{O}) = D_{2p\frac{n}{2}-1}(\mathcal{O})$$

and, for each $2p^{\frac{n}{2}-1} + 1 \leq j \leq p^{\frac{n}{2}}$, that $\gamma_{n+1}(\mathcal{O}) = D_j(\mathcal{O})$. It follows from the combination of Section 2.4 (3) with the induction hypothesis on (ii) that

$$\gamma_n(G) = D_{2p^{\frac{n}{2}-1}}(G)$$

and, for each $2p^{\frac{n}{2}-1} + 1 \leq j, j' \leq p^{\frac{n}{2}}$, that $D_j(G) = D_{j'}(G)$. Hence we get

$$\begin{aligned} \gamma_n(G)/\gamma_{n-1}(G)^p \gamma_{p^{\frac{n}{2}}}(G) &= D_{2p^{\frac{n}{2}-1}}(G)/D_{p^{\frac{n}{2}}}(G) \\ &\cong D_{2p^{\frac{n}{2}-1}}(\mathcal{O})/D_{p^{\frac{n}{2}}}(\mathcal{O}) = \gamma_n(\mathcal{O})/\gamma_{n+1}(\mathcal{O}) \end{aligned} \quad (5.1)$$

with $|\gamma_n(\mathcal{O}) : \gamma_{n+1}(\mathcal{O})| \leq p$. As \overline{G} is an obelisk, Proposition 5.4 yields

$$\gamma_{n-1}(\overline{G})^p \subseteq \gamma_{n+1}(\overline{G}) = 1,$$

from which it follows that

$$\gamma_{n-1}(G)^p \gamma_{p^{\frac{n}{2}}}(G) \subseteq \gamma_{n+1}(G) \subseteq \gamma_n(G).$$

As a consequence of (5.1), we have that $|\gamma_n(G) : \gamma_{n-1}(G)^p \gamma_{p^{\frac{n}{2}}}(G)| \leq p$, and so either $\gamma_n(G) = \gamma_{n+1}(G)$ or $\gamma_{n+1}(G) = \gamma_{n-1}(G)^p \gamma_{p^{\frac{n}{2}}}(G)$. If $\gamma_n(G) = \gamma_{n+1}(G)$, then $\gamma_n(G) = 1$, and as by induction $\gamma_3(G) = G^p \gamma_n(G)$, we obtain that G is an obelisk. Assume, on the other hand that $\gamma_{n-1}(G)^p \gamma_{p^{\frac{n}{2}}}(G) = \gamma_{n+1}(G)$. Then $\gamma_{n+1}(G) = D_{p^{\frac{n}{2}}}(G)$ together with the reasoning above implies (ii) for $n + 1$.

Assume now that n is odd. Set $\overline{G} = G/\gamma_{n+1}(G)$, which we can show to be an obelisk via computing

$$\begin{aligned} \gamma_3(\overline{G}) &= \overline{G}^p \gamma_n(\overline{G}) = \overline{G}^p D_{p^{\frac{n-1}{2}}}(\overline{G}) \\ &= \overline{G}^p (D_{p^{\frac{n-3}{2}}}(\overline{G}))^p \gamma_{p^{\frac{n-1}{2}}}(\overline{G}) = \overline{G}^p \gamma_{n-2}(\overline{G})^p = \overline{G}^p. \end{aligned} \quad (5.2)$$

In particular, the equality $\gamma_3(G) = G^p \gamma_{n+1}(G)$ holds. Now, by Lemma 5.5, we have $D_{2p^{\frac{n-1}{2}}}(\mathcal{O}) = \gamma_{n+1}(\mathcal{O})$. Then, by the iterative formula for dimension subgroups and induction hypothesis on (ii), we have

$$D_{2p^{\frac{n-1}{2}}}(G) = D_{2p^{\frac{n-3}{2}}}(G)^p \gamma_{2p^{\frac{n-1}{2}}}(G) = \gamma_{n-1}(G)^p \gamma_{2p^{\frac{n-1}{2}}}(G).$$

It follows from Lemma 5.5 that

$$\gamma_n(\mathcal{O}) = D_{p^{\frac{n-1}{2}}}(\mathcal{O})$$

and, for each $p^{\frac{n-1}{2}} + 1 \leq j \leq 2p^{\frac{n-1}{2}}$, that $\gamma_{n+1}(\mathcal{O}) = D_j(\mathcal{O})$. Section 2.4 (4) and the induction hypothesis on (ii) then yield that $\gamma_n(G) = D_{p^{\frac{n-1}{2}}}(G)$ and, for each $p^{\frac{n-1}{2}} + 1 \leq j, j' \leq 2p^{\frac{n-1}{2}}$, that $D_j(G) = D_{j'}(G)$. The following hold:

$$\begin{aligned} \gamma_n(G)/\gamma_{n-1}(G)^p \gamma_{2p^{\frac{n-1}{2}}}(G) &= D_{p^{\frac{n-1}{2}}}(G)/D_{2p^{\frac{n-1}{2}}}(G) \\ &\cong D_{p^{\frac{n-1}{2}}}(\mathcal{O})/D_{2p^{\frac{n-1}{2}}}(\mathcal{O}) = \gamma_n(\mathcal{O})/\gamma_{n+1}(\mathcal{O}), \end{aligned}$$

where $\gamma_n(\mathcal{O})/\gamma_{n+1}(\mathcal{O})$ is elementary abelian of rank at most 2. Since \overline{G} is a p -obelisk, we have $\gamma_{n-1}(\overline{G})^p = \gamma_{n+1}(\overline{G}) = 1$, and so

$$\gamma_{n-1}(G)^p \gamma_{2p}^{\frac{n-1}{2}}(G) \subseteq \gamma_{n+1}(G) \subseteq \gamma_n(G).$$

If $\gamma_n(G) = \gamma_{n+1}(G)$, then $\gamma_3(G) = G^p$ and G is a p -obelisk. If

$$p = |\gamma_n(G) : \gamma_{n+1}(G)| = |\gamma_n(G) : \gamma_{n-1}(G)^p \gamma_{2p}^{\frac{n-1}{2}}(G)|,$$

then $|\gamma_n(\mathcal{O}) : \gamma_{n+1}(\mathcal{O})| = p$ which, together with Proposition 5.4, implies that $\gamma_{n+1}(\mathcal{O}) = 1$. As G and \mathcal{O} have the same order, we get that $\gamma_{n+1}(G) = 1$, and the equality $\gamma_3(G) = G^p \gamma_{n+1}(G) = G^p$ yields that G is a p -obelisk. Assume now that $|\gamma_n(G) : \gamma_{n-1}(G)^p \gamma_{2p}^{\frac{n-1}{2}}(G)| = p^2$. If also $|\gamma_n(G) : \gamma_{n+1}(G)| = p^2$, then $D_{2p}^{\frac{n-1}{2}}(G) = \gamma_{n-1}(G)^p \gamma_{2p}^{\frac{n-1}{2}}(G) = \gamma_{n+1}(G)$ and (ii) follows from a similar argument as before. So the only possibility left is $|\gamma_n(G) : \gamma_{n+1}(G)| = p$. Set $\overline{G} = G/\gamma_{n-1}(G)^p \gamma_{2p}^{\frac{n-1}{2}}(G)$. As $\gamma_{n+1}(\overline{G})$ has order p , we get $\gamma_{n+2}(\overline{G}) = 1$. Moreover, for each $p \geq 5$ and $n \geq 3$, we have $n + 2 \leq p^{\frac{n-1}{2}}$, and so, imitating the arguments in (5.2), we get that $\gamma_3(\overline{G}) = \overline{G}^p \gamma_n(\overline{G}) = \overline{G}^p$. In particular, \overline{G} is a p -obelisk satisfying

$$p = |\gamma_{n-1}(\overline{G}) : \gamma_n(\overline{G})| = |\gamma_n(\overline{G}) : \gamma_{n+1}(\overline{G})| = |\gamma_{n+1}(\overline{G}) : \gamma_{n+2}(\overline{G})|,$$

a contradiction to Proposition 5.4 (1). The claim is now proven.

We conclude by observing that, when n is such that $\gamma_n(G) = 1$, then (i) yields $\gamma_3(G) = G^p$, and since such an n always exists, we are done. \square

Within the family of p -obelisks, there is a natural separation that is dictated by the collection of sizes of minimal generating sets of maximal subgroups.

Definition 5.6. Let \mathcal{O} be a p -obelisk. Then \mathcal{O} is *framed* if all maximal subgroups of \mathcal{O} are 2-generated.

Though not referred to with the name “framed p -obelisks”, these groups are the reason Blackburn became interested in p -obelisks in the first place [6, Theorem 4.2]. However, not all obelisks are framed [31, Lemma 437], and in non-framed obelisks, there are exactly 2 maximal subgroups that are not 2-generated (but 3-generated) [31, Lemma 335]. The following result [31, Proposition 336] makes it clear how the restricted k -Lie algebra of an obelisk determines whether the obelisk is framed or not.

Lemma 5.7. *Let \mathcal{O} be a p -obelisk. The following are equivalent:*

- (1) *the obelisk \mathcal{O} is framed;*
- (2) *the images of M^p and $[M, M]$ in $\gamma_3(\mathcal{O})/\gamma_4(\mathcal{O})$ for each maximal subgroup M of \mathcal{O} are distinct subgroups of order p .*

Theorem 5.8. *Let \mathcal{O} be a framed p -obelisk with $kG \cong k\mathcal{O}$. Then G is a framed p -obelisk.*

Proof. Thanks to Theorem 5.3, the group G is an obelisk if and only if \mathcal{O} is. Now, from Lemma 5.5, we know that

$$\gamma_3(G)/\gamma_4(G) = D_p(G)/D_{p+1}(G) \quad \text{and} \quad \gamma_3(\mathcal{O})/\gamma_4(\mathcal{O}) = D_p(\mathcal{O})/D_{p+1}(\mathcal{O}).$$

The combination of Lemma 5.7 with Section 2.4 (7) yields that G is framed if and only if \mathcal{O} is. □

Acknowledgments. The research in this paper has been conducted at various institutions with different sponsors to whom we wish to express our gratitude. We thank Eric Jespers from the Vrije Universiteit Brussel, Christopher Voll from the Universität Bielefeld, and Bernd Sturmfels from the Max-Planck-Institute for Mathematics in the Sciences. We wish to thank CIRM-FBK Trento for the financial support and hospitality during our Research in Pairs visit in February 2019. Moreover, we are thankful to the referees for their suggestions, which led to improvements on the exposition of this paper.

Bibliography

- [1] C. Bagiński, On the isomorphism problem for modular group algebras of elementary abelian-by-cyclic p -groups, *Colloq. Math.* **82** (1999), no. 1, 125–136.
- [2] C. Bagiński and A. Caranti, The modular group algebras of p -groups of maximal class, *Canad. J. Math.* **40** (1988), no. 6, 1422–1435.
- [3] C. Bagiński and A. Konovalov, The modular isomorphism problem for finite p -groups with a cyclic subgroup of index p^2 , in: *Groups St. Andrews 2005. Vol. 1*, London Math. Soc. Lecture Note Ser. 339, Cambridge University, Cambridge (2007), 186–193.
- [4] C. Bagiński and J. Kurdics, The modular group algebras of p -groups of maximal class II, *Comm. Algebra* **47** (2019), no. 2, 761–771.
- [5] H. U. Besche, B. Eick and E. O’Brien, SmallGrp: The GAP Small Groups Library, version 1.4.1, <https://gap-packages.github.io/smallgrp/>, 2019.
- [6] N. Blackburn, Generalizations of certain elementary theorems on p -groups, *Proc. Lond. Math. Soc. (3)* **11** (1961), 1–22.
- [7] F. M. Bleher, W. Kimmerle, K. W. Roggenkamp and M. Wursthorn, Computational aspects of the isomorphism problem, in: *Algorithmic Algebra and Number Theory* (Heidelberg 1997), Springer, Berlin (1999), 313–329.

-
- [8] R. Brauer, Representations of finite groups, in: *Lectures on Modern Mathematics, Vol. I*, Wiley, New York (1963), 133–175.
- [9] O. Broche and Á. del Río, The modular isomorphism problem for two generated groups of class two, preprint 2020, <https://arxiv.org/abs/2003.13281>.
- [10] W.E. Deskins, Finite Abelian groups with isomorphic group algebras, *Duke Math. J.* **23** (1956), 35–40.
- [11] J.D. Dixon, M.P.F. du Sautoy, A. Mann and D. Segal, *Analytic Pro- p Groups*, 2nd ed., Cambridge Stud. Adv. Math. 61, Cambridge University, Cambridge, 1999.
- [12] B. Eick, Computing automorphism groups and testing isomorphisms for modular group algebras, *J. Algebra* **320** (2008), no. 11, 3895–3910.
- [13] B. Eick and A. Konovalov, The modular isomorphism problem for the groups of order 512, in: *Groups St Andrews 2009 in Bath. Volume 2*, London Math. Soc. Lecture Note Ser. 388, Cambridge University, Cambridge (2011), 375–383.
- [14] M. Hertweck and M. Soriano, On the modular isomorphism problem: Groups of order 2^6 , in: *Groups, Rings and Algebras*, Contemp. Math. 420, American Mathematical Society, Providence (2006), 177–213.
- [15] M. Hertweck and M. Soriano, Parametrization of central Frattini extensions and isomorphisms of small group rings, *Israel J. Math.* **157** (2007), 63–102.
- [16] B. Huppert, *Endliche Gruppen. I*, Grundlehren Math. Wiss. 134, Springer, Berlin, 1967.
- [17] R. James, The groups of order p^6 (p an odd prime), *Math. Comp.* **34** (1980), no. 150, 613–637.
- [18] R. James, M. F. Newman and E. A. O’Brien, The groups of order 128, *J. Algebra* **129** (1990), no. 1, 136–158.
- [19] S. A. Jennings, The structure of the group ring of a p -group over a modular field, *Trans. Amer. Math. Soc.* **50** (1941), 175–185.
- [20] L. Margolis and T. Moede, The modular isomorphism problem for small groups – revisiting Eick’s algorithm, preprint (2020), <https://arxiv.org/abs/2010.07030>.
- [21] E. A. O’Brien and M. R. Vaughan-Lee, The groups with order p^7 for odd prime p , *J. Algebra* **292** (2005), no. 1, 243–258.
- [22] I. B. S. Passi and S. K. Sehgal, Isomorphism of modular group algebras, *Math. Z.* **129** (1972), 65–73.
- [23] D. S. Passman, *The Algebraic Structure of Group Rings*, Pure Appl. Math., John Wiley & Sons, New York, 1977.
- [24] T. Sakurai, The isomorphism problem for group algebras: a criterion, *J. Group Theory* **23** (2020), no. 3, 435–445.

- [25] M. A. M. Salim, *The isomorphism problem for the modular group algebras of groups of order p^5* , Ph.D. thesis, Department of Mathematics, University of Manchester, 1993.
- [26] M. A. M. Salim and R. Sandling, The unit group of the modular small group algebra, *Math. J. Okayama Univ.* **37** (1995), 15–25.
- [27] M. A. M. Salim and R. Sandling, The modular group algebra problem for groups of order p^5 , *J. Aust. Math. Soc. Ser. A* **61** (1996), no. 2, 229–237.
- [28] M. A. M. Salim and R. Sandling, The modular group algebra problem for small p -groups of maximal class, *Canad. J. Math.* **48** (1996), no. 5, 1064–1078.
- [29] R. Sandling, The isomorphism problem for group rings: A survey, in: *Orders and Their Applications* (Oberwolfach 1984), Lecture Notes in Math. 1142, Springer, Berlin (1985), 256–288.
- [30] R. Sandling, The modular group algebra of a central-elementary-by-abelian p -group, *Arch. Math. (Basel)* **52** (1989), no. 1, 22–27.
- [31] M. Stanojkovski, Intense automorphisms of finite groups, preprint (2017), <https://arxiv.org/abs/1710.08979>; to appear in *Mem. Amer. Math. Soc.*
- [32] M. Suzuki, *Group Theory. II*, Grundlehren Math. Wiss. 248, Springer, New York, 1986.
- [33] M. Wursthorn, Isomorphisms of modular group algebras: An algorithm and its application to groups of order 2^6 , *J. Symbolic Comput.* **15** (1993), no. 2, 211–227.
- [34] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.10.2, 2019, <http://www.gap-system.org>.

Received November 10, 2020; revised July 27, 2021.

Author information

Leo Margolis, Department of Mathematics, Vrije Universiteit Brussel,
Pleinlaan 2, 1050 Brussels, Belgium.
E-mail: leo.margolis@vub.be

Corresponding author:

Mima Stanojkovski, Max-Planck-Institut für Mathematik in den Naturwissenschaften,
Inselstraße 22, 04103 Leipzig, Germany.
E-mail: mima.stanojkovski@mis.mpg.de