Rev. Mat. Iberoam. (Online first)
DOI 10.4171/RMI/1531

Published by EMS Press

Identification of non-isomorphic 2-groups with dihedral central quotient and isomorphic modular group algebras

Leo Margolis and Taro Sakurai

Abstract. The question whether non-isomorphic finite p-groups can have isomorphic modular group algebras was recently answered in the negative by García-Lucas, Margolis and del Río [J. Reine Angew. Math. 783 (2022), 269–274]. We embed these negative solutions in the class of two-generated finite 2-groups with dihedral central quotient, and solve the original question for all groups within this class. As a result, we discover new negative solutions and simple algebra isomorphisms.

Introduction

The *modular isomorphism problem* asks whether non-isomorphic finite p-groups can have isomorphic group algebras over a field of positive characteristic p. It seems to have first been raised in the 1950s and appears in an influential survey by Brauer (Problem 2 and Section 9 of Supplements in [3]). Over the following decades, positive results for many classes of finite p-groups were published, cf. [18] for an overview. However, a few years ago, García-Lucas, Margolis and del Río [11] discovered the first non-isomorphic finite 2-groups that have isomorphic group algebras over an arbitrary field of characteristic 2.

Nevertheless, the problem remains poorly understood in general and open for odd primes, for instance. Our goal in this article is to understand better how the negative solutions presented in [11] come to be. These groups were discovered during an effort to solve the modular isomorphism problem for two-generated finite p-groups with cyclic derived subgroup, after these had been classified by Broche, García-Lucas and del Río [4]. Although considerable effort has been devoted to solving the problem in this wide class, it has not been achieved completely so far [9, 10]. We consider the negative solutions from another viewpoint and embed them in a natural class of groups for which we can completely solve the modular isomorphism problem.

We call a non-abelian group that is generated by two elements of order 2 *dihedral*. For a group G, we call the quotient by its center the *central quotient* of G. In this article, we study the modular isomorphism problem for two-generated finite 2-groups with dihedral central quotient. This class of groups includes the negative solutions presented

Mathematics Subject Classification 2020: 20C05 (primary); 16S34, 20D15, 16U60 (secondary).
Keywords: modular isomorphism problem, group algebra, counterexamples, finite 2-groups, classification.

in [11], and we are able to identify all negative solutions to the problem –including new counterexamples– within this class of groups.

Theorem A. *Let G and H be finite 2-groups and $\mathbb{F}$ a field of characteristic 2. Suppose that G is two-generated and the central quotient of G is dihedral. Then $\mathbb{F}G \cong \mathbb{F}H$ but $G \not\cong H$ if and only if for some integers $n > m > \ell \geq 2$, up to exchange,*

$$G \cong \langle x, y, z \mid x^{2^n} = 1, y^{2^m} = 1, \quad z^{2^\ell} = 1, [y, x] = z, [z, x] = z^{-2}, [z, y] = z^{-2} \rangle,$$
$$H \cong \langle a, b, c \mid a^{2^n} = 1, b^{2^m} = a^{2^m}, c^{2^\ell} = 1, [b, a] = c, [c, a] = c^{-2}, [c, b] = c^{-2} \rangle.$$

The known counterexamples to the modular isomorphism problem presented in [11] correspond to the case $\ell = 2$. It should be emphasized, however, that our algebra isomorphisms are simpler than the original ones and it makes the proof cleaner. This is largely due to the change of presentations of the groups, which is natural in our class.

For the proof of Theorem A, we first give presentations of the groups in our target class. We then establish an isomorphism between the algebras of the above groups in Theorem 3.1. The proof of this isomorphism can be read independently of the rest of this article, as it only needs the presentations of the groups. We remark that the proof cannot be carried over to odd primes, or at least not in the most naive way (cf. Remark 3.5). Finally, we prove that no more negative solutions exist within the class of two-generated finite 2-groups with dihedral central quotient. This is the most challenging part of the article, and what can be considered standard methods to attack the problem turn out to be insufficient to prove this. We hence introduce a procedure that could be called a “group base approximation”. It allows us, after considerable effort, to solve the modular isomorphism problem completely within our class. This procedure could also be used for other classes of groups with some adjustments. These positive solutions for most groups in the studied class give some insights why minimal changes to the defining relations of the negative solutions break down the isomorphism between the group algebras.

As a byproduct of identifying negative solutions, we obtain the classification of two-generated finite 2-groups with dihedral central quotient. Since such a classification of groups might be also of independent interest, we provide a direct proof in Appendix A.

1. Preliminaries

We use standard group-theoretical notation. We always write G and H for finite p-groups for some prime p. In most cases, $p = 2$ holds. The center of G is denoted by $\mathbf{Z}(G)$, the derived subgroup by G' and the Frattini subgroup by $\Phi(G)$. By $\Omega(G)$ we mean the subgroup of G generated by the elements of order p. For a non-negative integer r, we write $\mho_r(G)$ for the subgroup of G generated by g^{p^r}, $g \in G$. For $g, h \in G$, we let $[g, h] = g^{-1}h^{-1}gh$ denote the commutator. Accordingly, we conjugate as $g^h = h^{-1}gh$. We write a cyclic group of order n as C_n.

Let $\mathbb{F}$ denote a field of characteristic p and $\mathbb{F}G$ the group algebra of G over $\mathbb{F}$. We write $\Delta(G)$ for the augmentation ideal in the group algebra $\mathbb{F}G$. Note that $\Delta(G)$ is nilpotent and equal to the Jacobson radical of $\mathbb{F}G$. In particular, the complement of $\Delta(G)$ equals the set of units in $\mathbb{F}G$. The center of an algebra Λ over $\mathbb{F}$ is denoted by $\mathbf{Z}(\Lambda)$, and the linear subspace spanned by the Lie commutators is denoted by $[\Lambda, \Lambda]$. We note that $\Delta(G')\mathbb{F}G$ is the relative augmentation ideal of the derived subgroup and equal to the smallest ideal $[\mathbb{F}G, \mathbb{F}G]\mathbb{F}G$ of $\mathbb{F}G$ with commutative quotient. Moreover, we let $\mho_r(\Lambda)$ be the subalgebra of Λ generated by T^{p^r}, $T \in \Lambda$.

The center of $\mathbb{F}G$ has a special decomposition which we will use frequently. Namely, $\mathbf{Z}(\mathbb{F}G) = \mathbb{F}\mathbf{Z}(G) \oplus (\mathbf{Z}(\mathbb{F}G) \cap [\mathbb{F}G, \mathbb{F}G])$. Moreover, $\mathbf{Z}(\mathbb{F}G) \cap [\mathbb{F}G, \mathbb{F}G]$ coincides with the linear subspace of $\mathbf{Z}(\mathbb{F}G)$ spanned by the class sums of non-central elements of G. We refer to Section III.6 of [25] for more details and proofs. We will allude to these facts in Section 4 without further mention.

A property of G is an *invariant* if $\mathbb{F}G \cong \mathbb{F}H$ implies the same property for H. A subset of $\mathbb{F}G$ is called *canonical* if it is stable under all algebra automorphisms.

2. Presentations of groups

In this section, we give presentations of two-generated finite 2-groups with dihedral central quotient. Compared to many other classes of finite p-groups, this class turns out to be rather accessible.

Theorem 2.1. *Let G be a two-generated finite 2-group with dihedral central quotient. Then $G/G' \cong C_{2^n} \times C_{2^m}$ and $G' \cong C_{2^\ell}$ for some positive integers n, m and ℓ with $n \geq m$ and $\ell \geq 2$, and G is isomorphic to a group generated by x, y and z, with one of the following defining relations*:

$$
\begin{aligned}
&\text{⚀} : x^{2^n} = 1, && y^{2^m} = 1, && z^{2^\ell} = 1, [y,x] = z, [z,x] = z^{-2}, [z,y] = z^{-2};\\
&\text{⚁} : x^{2^n} = 1, && y^{2^m} = x^{2^m}, && z^{2^\ell} = 1, [y,x] = z, [z,x] = z^{-2}, [z,y] = z^{-2};\\
&\text{⚂} : x^{2^n} = 1, && y^{2^m} = z^{2^{\ell-1}}, && z^{2^\ell} = 1, [y,x] = z, [z,x] = z^{-2}, [z,y] = z^{-2};\\
&\text{⚃} : x^{2^n} = 1, && y^{2^m} = x^{2^m} z^{2^{\ell-1}}, && z^{2^\ell} = 1, [y,x] = z, [z,x] = z^{-2}, [z,y] = z^{-2};\\
&\text{⚄} : x^{2^n} = z^{2^{\ell-1}}, && y^{2^m} = 1, && z^{2^\ell} = 1, [y,x] = z, [z,x] = z^{-2}, [z,y] = z^{-2};\\
&\text{⚅} : x^{2^n} = z^{2^{\ell-1}}, && y^{2^m} = x^{2^m}, && z^{2^\ell} = 1, [y,x] = z, [z,x] = z^{-2}, [z,y] = z^{-2}.
\end{aligned}
$$

We write

$$G_{\text{⚀}}, G_{\text{⚁}}, \ldots, G_{\text{⚅}} \tag{2.1}$$

for the groups of order $2^{n+m+\ell}$ in Theorem 2.1 and always use the generators satisfying the above relations, which are written x, y, z or a, b, c. Although the definitions of the groups depend on the parameters n, m and ℓ, we do not include these in the notation as different parameters are never considered simultaneously, except in the appendix where the parameters are hence included.

Evidently, if $n = m$, then

$$G_{\text{⚀}} \cong G_{\text{⚁}} \quad \text{and} \quad G_{\text{⚂}} \cong G_{\text{⚃}} \cong G_{\text{⚄}}. \tag{2.2}$$

We will see in the end that all other pairs of groups are non-isomorphic through investigation of their modular group algebras. Even though such indirect arguments suffice to prove Theorem A, a more direct proof is also of interest. See Appendix A.

We also note that the groups (2.1) include finite 2-groups of maximal class: the dihedral, semidihedral and generalized quaternion groups (Proposition A.5).

To help the reader we summarize some of the basic properties which the groups have in common. We will frequently use these properties in the following without explicit mention. Let $G = G_{\boxed{?}}$ with $\boxed{?} \in \{\text{⚀}, \dots, \text{⚅}\}$. Then:

(1) the order of G is $2^{n+m+\ell}$,

(2) we have $G/G' \cong C_{2^n} \times C_{2^m}$ and $G' \cong C_{2^\ell}$,

(3) the center of G is generated by x^2, y^2 and $z^{2^{\ell-1}}$ and has order 2^{n+m-1} (cf. Lemma 4.1 for the different isomorphism types of the center),

(4) xy commutes with z,

(5) the nilpotency class of G is $\ell + 1$ and the coclass is $n + m - 1$.

We next prove several auxiliary results before proving Theorem 2.1.

Lemma 2.2. *Let G be a two-generated finite 2-group with dihedral central quotient. Then $G/G' \cong C_{2^n} \times C_{2^m}$ and $G' \cong C_{2^\ell}$ for some positive integers n, m and ℓ with $n \geq m$ and $\ell \geq 2$, and G is isomorphic to the group*

$$G_\theta = \left\langle x, y, z \;\middle|\; \begin{array}{l} x^{2^n} = z^{r2^{\ell-1}},\ y^{2^m} = x^{s2^m} z^{t2^{\ell-1}},\ z^{2^\ell} = 1, \\ \quad [y, x] = z,\ [z, x] = z^{-2},\ [z, y] = z^{-2} \end{array} \right\rangle$$

for some $\theta = (r, s, t)$ belonging to

$$\Theta = \{(r, s, t) \mid 0 \leq r \leq 1,\ 0 \leq s \leq 2^{n-m} - 1,\ 0 \leq t \leq 1\}.$$

Proof. First, suppose that the central quotient $G/\mathbf{Z}(G)$ is isomorphic to the dihedral group of order $2^{\ell+1}$ with $\ell \geq 2$. Then the quotient $G'\mathbf{Z}(G)/\mathbf{Z}(G)$, which is the derived subgroup of $G/\mathbf{Z}(G)$, has order $2^{\ell-1}$. There are two elements x and y of G such that x^2, y^2 and $(yx)^{2^\ell}$ are trivial modulo the center $\mathbf{Z}(G)$. Moreover, x and y together with the center of G generate the whole group G. We write z for the commutator $[y, x]$. Since y^2 is central, we have

$$1 = [y^2, x] = [y, x]^y [y, x] = z^y z,$$

and the action of y on z by conjugation equals the inversion. The same is true for x. Then a direct calculation of commutators shows that the derived subgroup G' is a cyclic group generated by z. Since z is congruent to $(yx)^2$ modulo the center $\mathbf{Z}(G)$, the power $z^{2^{\ell-1}}$ is central. Then $z^{2^{\ell-1}}$ is equal to its inverse by conjugation. This shows that $G' \cap \mathbf{Z}(G)$ has order 2 and hence G' has order 2^ℓ. In summary, three elements x, y and z of G satisfy the last four relations:

$$z^{2^\ell} = 1, \quad [y, x] = z, \quad [z, x] = z^{-2}, \quad [z, y] = z^{-2}.$$

Next, suppose that $G/G' \cong C_{2^n} \times C_{2^m}$ with $n \geq m$ as G is two-generated. Since $G/G'\mathbf{Z}(G)$, the abelianization of $G/\mathbf{Z}(G)$, is elementary abelian of rank two, $\Phi(G) = G'\mathbf{Z}(G)$. Hence, x and y generate G. We may assume that x^{2^n} belongs to G', while $x^{2^{n-1}}$ does not. (Otherwise replace x, y and z by y, x and z^{-1}). Since x^2 is central, we see that x^{2^n} belongs to $G' \cap \mathbf{Z}(G)$ which is a cyclic group of order 2 generated by $z^{2^{\ell-1}}$. Hence,

$$x^{2^n} = z^{r2^{\ell-1}} \quad \text{for some } 0 \leq r \leq 1.$$

Let $\bar{G}$ denote the abelianization G/G'. From Theorem 7.12 in [14], there is an element w of G with $\bar{G} = \langle \bar{x} \rangle \times \langle \bar{w} \rangle$, in particular, $\bar{w}$ has order 2^m. Then $\bar{y}^{2^m} = \bar{x}^{s2^m}$ for some $0 \le s \le 2^{n-m} - 1$. Since $y^{-2^m} x^{s2^m}$ belongs to $G' \cap \mathbf{Z}(G)$, we obtain

$$y^{2^m} = x^{s2^m} z^{t2^{\ell-1}} \quad \text{for some } 0 \le t \le 1.$$

The six relations above define a finite group of order $2^{n+m+\ell}$ and yield a presentation of G. ■

We consider a partition of the parameter space introduced in Lemma 2.2 as

$$\Theta = \Theta_{\text{⚀}} \cup \cdots \cup \Theta_{\text{⚅}}$$

defined by the following:

$$\begin{aligned}
\Theta_{\text{⚀}} &= \{(r,s,t) \in \Theta \mid r = 0,\ t = 0,\ s \equiv 0 \mod 2\},\\
\Theta_{\text{⚁}} &= \{(r,s,t) \in \Theta \mid r = 0,\ t = 0,\ s \equiv 1 \mod 2\},\\
\Theta_{\text{⚂}} &= \{(r,s,t) \in \Theta \mid r = 0,\ t = 1,\ s \equiv 0 \mod 2\},\\
\Theta_{\text{⚃}} &= \{(r,s,t) \in \Theta \mid r = 0,\ t = 1,\ s \equiv 1 \mod 2\},\\
\Theta_{\text{⚄}} &= \begin{cases} \{(r,s,t) \in \Theta \mid r = 1,\ s \equiv 0 \mod 2\} & (n > m),\\ \{(r,s,t) \in \Theta \mid r = 1,\ s \equiv 0 \mod 2\} \setminus \{(1,0,1)\} & (n = m),\end{cases}\\
\Theta_{\text{⚅}} &= \begin{cases} \{(r,s,t) \in \Theta \mid r = 1,\ s \equiv 1 \mod 2\} & (n > m),\\ \{(r,s,t) \in \Theta \mid r = 1,\ s \equiv 1 \mod 2\} \cup \{(1,0,1)\} & (n = m).\end{cases}
\end{aligned}$$

The introduction of this partition is justified by the next lemma; note that in the corner case $n = m$, slight changes are required to ensure that $\Theta_{\text{⚅}}$ is non-empty.

Lemma 2.3. *Let n, m and ℓ be positive integers with $n \ge m$ and $\ell \ge 2$, and let $\theta = (r,s,t) \in \Theta$. Let $s_0 \equiv s \mod 2$ with $s_0 \in \{0,1\}$. Then*

$$G_\theta \cong G_{(r,s_0,(1-r)t)}$$

except the case $n = m$ and $\theta = (1,0,1)$. In the exceptional case,

$$G_\theta \cong G_{(1,1,0)}.$$

In particular, we have $G_{\boxed{?}} \cong G_\theta$ if $\theta \in \Theta_{\boxed{?}}$ for $\boxed{?} \in \{\text{⚀}, \dots, \text{⚅}\}$.

Proof. Assume that $n > m$ or $\theta \ne (1,0,1)$ so that $r(2-t)2^{n-m}$ is even. Note here that $n = m$ implies $s = 0$.

Take an even number u such that $s + u = s_0 + r(2-t)2^{n-m}$. Then x^u is central and

$$\begin{aligned}
(x^u y)^{2^m} &= x^{u2^m} y^{2^m} = x^{u2^m} x^{s2^m} z^{t2^{\ell-1}} = x^{(s+u)2^m} z^{t2^{\ell-1}}\\
&= x^{s_0 2^m} x^{r(2-t)2^n} z^{t2^{\ell-1}} = x^{s_0 2^m} z^{r^2(2-t)2^{\ell-1}} z^{t2^{\ell-1}}\\
&= x^{s_0 2^m} z^{r(2-t)2^{\ell-1}} z^{t2^{\ell-1}} = x^{s_0 2^m} z^{(1-r)t2^{\ell-1}}.
\end{aligned}$$

Hence, $G_\theta = \langle x, x^u y, z \rangle$ enjoys the defining relations of $G_{(r,s_0,(1-r)t)}$.

If $n = m$ and $\theta = (1,0,1)$, then $y^{2^m} = z^{2^{\ell-1}} = x^{2^n} = x^{2^m}$ and $G_\theta = \langle x, y, z\rangle$ enjoys the defining relations of $G_{(1,1,0)}$. ■

Proof of Theorem 2.1. It follows from Lemmas 2.2 and 2.3. ■

3. Isomorphic modular group algebras

This section is devoted to proving that groups $G_{\text{⚀}}$ and $G_{\text{⚁}}$ with $n > m > \ell \geq 2$ have isomorphic group algebras over an arbitrary field of characteristic 2, but are non-isomorphic groups. In the next section, we will see that these are the only counterexamples to the modular isomorphism problem within the class of two-generated finite 2-groups with dihedral central quotient.

Arguably the most interesting part of this article is the following, which generalizes the negative solutions to the modular isomorphism problem presented in [11].

Theorem 3.1. *Let $n \geq m > \ell \geq 2$ and $\mathbb{F}$ a field of characteristic 2. Then $\mathbb{F}G_{\text{⚀}} \cong \mathbb{F}G_{\text{⚁}}$.*

Proof. Let $G = G_{\text{⚀}}$ and $H = G_{\text{⚁}} = \langle a, b, c\rangle$. We construct an algebra homomorphism from $\mathbb{F}G$ to $\mathbb{F}H$ and then show that it is bijective. Given a group homomorphism from G to the unit group of $\mathbb{F}H$, we can extend it and obtain an algebra homomorphism from $\mathbb{F}G$ to $\mathbb{F}H$ by Lemma 1.1.7 in [23]. To obtain such a group homomorphism, it suffices to show that the units

$$x = a, \quad y = b + a + 1, \quad z = [y, x] \in \mathbb{F}H \setminus \Delta(H)$$

satisfy the defining relations for G by Proposition 4.3 in [16].

We first verify the commutator relations. Evidently, $[y, x] = z$. As x^2 is central in $\mathbb{F}H$, the basic commutator identity $[y, x^2] = [y, x][y, x]^x$ yields $[z, x] = z^{-2}$. Now use $ba = abc$ to see

$$y^2 = b^2 + a^2 + ab + abc + 1.$$

Observe that $(ab)^a = abc = (ab)^b$ and $(abc)^a = ab = (abc)^b$. Hence, $\{ab, abc\}$ is a conjugacy class of H and the class sum $ab + abc$ is central in $\mathbb{F}H$. Thus, so is y^2 which yields $[z, y] = z^{-2}$ as before.

We proceed to the power relations. Clearly, $x^{2^n} = 1$. As ab commutes with c, it is also easy to raise y to a power:

$$y^{2^m} = (b^2 + a^2 + ab + abc + 1)^{2^{m-1}} = b^{2^m} + a^{2^m} + (ab)^{2^{m-1}}(1 + c^{2^{m-1}}) + 1.$$

The first two terms vanish as $b^{2^m} = a^{2^m}$, and the third term vanishes as $c^{2^\ell} = 1$ and $m > \ell$. Thus, $y^{2^m} = 1$. Finally, use $yx = xyz$ and $ba = abc$ to see

$$xy(1 + z) = xy + yx = ab + ba = ab(1 + c).$$

We raise both sides to the power of 2^ℓ. Since ab commutes with c, the right-hand side becomes $(ab)^{2^\ell}(1 + c^{2^\ell}) = 0$. On the other hand, xy commutes with z as

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

Hence, the left-hand side becomes $(xy)^{2^\ell}(1+z^{2^\ell})$. As xy is a unit, we obtain $z^{2^\ell}=1$. Therefore, all relations are satisfied and we obtain a suitable algebra homomorphism.

Since $a=x$ and $b=y+x+1$ belong to the image of our algebra homomorphism, it is surjective. As G and H have the same order, it is bijective. ■

Lemma 3.2. *Let $n>m>\ell\geq 2$. Then $G_{\text{⚀}}\not\cong G_{\text{⚁}}$.*

Proof. Let $G=G_{\text{⚀}}=\langle x,y,z\rangle$ and $H=G_{\text{⚁}}=\langle a,b,c\rangle$. The centralizers of the derived subgroups can distinguish these groups. First we calculate the exponent of $\mathbf{C}_H(H')$.

Recall that the Frattini subgroup $\Phi(H)$ is generated by a^2, b^2 and c. As a^2 and b^2 are central, we have $\Phi(H)\leq\mathbf{C}_H(H')$. Moreover, as $ab\in\mathbf{C}_H(H')$ but $ab\notin\Phi(H)$ we have that $\langle a^2,ab,b^2,c\rangle$ is an abelian maximal subgroup of H and hence equals $\mathbf{C}_H(H')$. The orders of a^2, b^2 and c are 2^{n-1}, 2^{n-1} and 2^ℓ, respectively. From $(ab)^2=a^2bcb=a^2b^2c^{-1}$ and $b^{2^m}=a^{2^m}$, we obtain

$$(ab)^{2^{n-1}}=a^{2^{n-1}}b^{2^{n-1}}c^{-2^{n-2}}=c^{-2^{n-2}}.$$

Since $n>m>\ell\geq 2$, we have $(ab)^{2^{n-1}}=1$ and the exponent of $\mathbf{C}_H(H')$ is 2^{n-1}.

Similar arguments show that $\mathbf{C}_G(G')$ is abelian and generated by x^2, xy, y^2 and z. Then the exponent of $\mathbf{C}_G(G')$ is equal to 2^n, which is the order of xy. Hence, these groups are not isomorphic. ■

The negative solutions to the modular isomorphism problem presented in [11] correspond to the groups $G_{\text{⚀}}$ and $G_{\text{⚁}}$ for $n>m>\ell=2$ in our notation. In fact, the isomorphisms from $G_{\text{⚀}}=\langle x,y,z\rangle$ and $G_{\text{⚁}}=\langle a,b,c\rangle$ to the original groups

$$\mathsf{G}=\left\langle \mathsf{x},\mathsf{y},\mathsf{z}\mid \mathsf{x}^{2^n}=1,\mathsf{y}^{2^m}=1,\mathsf{z}^{2^\ell}=1,\ [\mathsf{y},\mathsf{x}]=\mathsf{z},\mathsf{z}^{\mathsf{x}}=\mathsf{z}^{-1},\mathsf{z}^{\mathsf{y}}=\mathsf{z}^{-1}\right\rangle,$$
$$\mathsf{H}=\left\langle \mathsf{a},\mathsf{b},\mathsf{c}\mid \mathsf{a}^{2^n}=1,\mathsf{b}^{2^m}=1,\mathsf{c}^{2^\ell}=1,\ [\mathsf{b},\mathsf{a}]=\mathsf{c},\mathsf{c}^{\mathsf{a}}=\mathsf{c}^{-1},\mathsf{c}^{\mathsf{b}}=\mathsf{c}\right\rangle$$

are given by

$$G_{\text{⚀}}\to\mathsf{G},\quad x\mapsto\mathsf{x},\quad y\mapsto\mathsf{y},\quad z\mapsto\mathsf{z},$$
$$G_{\text{⚁}}\to\mathsf{H},\quad a\mapsto\mathsf{a},\quad b\mapsto\mathsf{ab},\quad c\mapsto\mathsf{c}.$$

Remark 3.3. For a finite p-group G with cyclic derived subgroup G', García-Lucas, del Río and Stanojkovski (Theorem A in [10]) proved that the exponent of the centralizer $\mathbf{C}_G(G')$ is an invariant of its modular group algebra, provided that the prime p is odd. This shows that the above pairs of groups, including the original ones presented in [11], are distinctive for $p=2$.

The groups $G_{\text{⚀}}$ and $G_{\text{⚁}}$ are in fact isomorphic if $n=m$. We summarize explicitly the negative solutions to the modular isomorphism problem that we obtain by the previous theorem and lemma.

Corollary 3.4. *Let $n>m>\ell\geq 2$. Then the groups*

$$\left\langle x,y,z\mid x^{2^n}=1,y^{2^m}=1,\quad z^{2^\ell}=1,[y,x]=z,[z,x]=z^{-2},[z,y]=z^{-2}\right\rangle,$$
$$\left\langle a,b,c\mid a^{2^n}=1,b^{2^m}=a^{2^m},c^{2^\ell}=1,\ [b,a]=c,\ [c,a]=c^{-2},\ [c,b]=c^{-2}\right\rangle$$

are not isomorphic, but have isomorphic group algebras over an arbitrary field of characteristic 2.

Remark 3.5. Given the simple proof of the negative solutions to the modular isomorphism problem for $p = 2$, it is natural to ask whether this strategy might be imitated for groups of odd order. While we currently have no clue, at least the isomorphism we exhibit and the proof we use cannot be imitated directly, as we will quickly show. Analyzing what facilitates the proof so much, one important thing is that no actual commutator between any non-trivial units in the group algebra must be computed: The action of the generators of the group on the derived subgroup follows from the fact that their squares are central, and the correct structure of the whole derived subgroup essentially from its cyclicity. To imitate the proof, it would be necessary to find a finite non-abelian p-group G generated by two elements, say x and y, such that x^p and y^p are central and G' is cyclic. We show that in this case $G/\mathbf{Z}(G)$ is elementary abelian of rank two. For such groups, a positive answer to the modular isomorphism problem over an arbitrary field is obtained by Drensky [7].

So, assume p is odd, $G = \langle x, y\rangle$ is a finite non-abelian p-group such that x^p, y^p are central in G and $G' = \langle z\rangle$ is cyclic. We assume $z = [y, x]$ and let p^ℓ be the order of z. Then G is regular by Satz 10.2 (c) in Kapitel III of [13]. Hence, $1 = [z, x^p] = [z, x]^p$ by Satz 10.6 (b) in Kapitel III of [13]. As $\Omega(G') = \langle z^{p^{\ell-1}}\rangle$, there exists an $0 \leq r \leq p-1$ such that $[z, x] = z^{rp^{\ell-1}}$. This implies $z^{x^i} = z^{1+irp^{\ell-1}}$. We conclude by the standard commutator identity that $[y, x^p] = [y, x][y, x]^x \cdots [y, x]^{x^{p-1}} = z^k$, where

$$k = \sum_{i=0}^{p-1}(1 + irp^{\ell-1}) = p + \frac{1}{2}r(p-1)p^\ell \equiv p \mod p^\ell.$$

As $[y, x^p] = 1$, we conclude that $\ell = 1$. Hence, x centralizes z, and so does y. This implies that z is central. As x^p and y^p are also central, we get $\Phi(G) = \mathbf{Z}(G)$, which shows that $G/\mathbf{Z}(G)$ is indeed elementary abelian of rank two.

We add one bibliography remark for readers interested in generalizing the groups from Theorem 3.1 to odd primes: In several generalizations we have tried and which were proposed to us the invariants from [2] turned out to solve the problem in the positive.

For the choice of our isomorphisms in Theorem 3.1, see also Remark 4.21.

4. Non-isomorphic modular group algebras

The rest of this article is devoted to showing that the groups $G_{⚀}$ and $G_{⚁}$ with $n > m > \ell \geq 2$ are indeed the only negative solutions within our class, thereby completing the proof of Theorem A. Throughout this section, we fix a field $\mathbb{F}$ of characteristic p and assume $p = 2$ unless otherwise stated.

We first apply known group-theoretical invariants and then utilize a well-known argument on power maps to distinguish algebras. However, this turns out to be insufficient, and in the last part, we apply a procedure that could be called a "group base approximation". This could also be used for other classes of groups with some adjustments.

For the proof, we examine all the pairs of groups with $n \geq m$ and $\ell \geq 2$. Basically, we divide it into five cases:

(1) $n > m > \ell$,

(2) $n > m \geq 2$ and $m \leq \ell$,

(3) $n > m = 1$,

(4) $n = m \geq 2$,

(5) $n = m = 1$.

We observe first that the coclass of the groups is $n + m - 1$, and the last case $n = m = 1$ corresponds to the finite 2-groups of maximal class for which a positive answer to the modular isomorphism problem has been known for decades [1, 5]. Therefore, we may assume $n \geq 2$.

The case $n = m \geq 2$ can be dealt with using a classic invariant, the center of a group, except the pair that corresponds to ⚄⚅. We will use a group base approximation for this case (Lemmas 4.17 to 4.19). What will be used to distinguish modular group algebras for the rest of the cases is summarized in Table 1.

	$n > m > \ell$	$n > m \geq 2$ and $m \leq \ell$	$n > m = 1$
⚀⚁	X	P	P
⚀⚂	C	C	Q
⚀⚃	C	C	P
⚀⚄	C	C	C
⚀⚅	C	C	C
⚁⚂	C	C	P
⚁⚃	C	C	K
⚁⚄	C	C	C
⚁⚅	C	C	C
⚂⚃	A	P	P
⚂⚄	C	C	C
⚂⚅	C	C	C
⚃⚄	C	C	C
⚃⚅	C	C	C
⚄⚅	A	P	P

Table 1. Summary of how modular group algebras will be distinguished for $n > m$. [X] counterexample (Theorem 3.1), [C] center of group (Lemma 4.1), [P] kernel size of power map (Lemma 4.8), [Q] Quillen's theorem (Proposition 4.4), [K] Külshammer's theorem (Proposition 4.3), [A] group base approximation (Section 4.3).

4.1. Group-theoretical invariants

The first invariant we will use is the isomorphism type of the center of a group. This is a well-known invariant, and a proof can be found in Theorem 6.6 of Chapter III in [25].

Lemma 4.1. *Let $G = \langle x, y, z \rangle$ be one of the groups $G_{\text{⚀}}, \ldots, G_{\text{⚅}}$. Then the center of G is generated by x^2, y^2 and $z^{2^{\ell-1}}$. Consequently,*

$$\mathbf{Z}(G_{\text{⚀}}) = \langle x^2 \rangle \times \langle y^2 \rangle \times \langle z^{2^{\ell-1}} \rangle \qquad \cong C_{2^{n-1}} \times C_{2^{m-1}} \times C_2,$$

$$\begin{aligned}
\mathbf{Z}(G_{\text{⚁}}) &= \langle x^2\rangle \times \langle x^{-2}y^2\rangle \times \langle z^{2^{\ell-1}}\rangle && \cong C_{2^{n-1}} \times C_{2^{m-1}} \times C_2,\\
\mathbf{Z}(G_{\text{⚂}}) &= \langle x^2\rangle \times \langle y^2\rangle && \cong C_{2^{n-1}} \times C_{2^m},\\
\mathbf{Z}(G_{\text{⚃}}) &= \langle x^2\rangle \times \langle x^{-2}y^2\rangle && \cong C_{2^{n-1}} \times C_{2^m},\\
\mathbf{Z}(G_{\text{⚄}}) &= \langle x^2\rangle \times \langle y^2\rangle && \cong C_{2^n} \times C_{2^{m-1}},\\
\mathbf{Z}(G_{\text{⚅}}) &= \langle x^2\rangle \times \langle x^{-2}y^2\rangle && \cong C_{2^n} \times C_{2^{m-1}}.
\end{aligned}$$

Proof. From the relations, we directly get $x^2, y^2 \in \mathbf{Z}(G)$. As $G/\langle x^2, y^2\rangle$ is dihedral with the center generated by the image of $z^{2^{\ell-1}}$, it follows that $\mathbf{Z}(G) = \langle x^2, y^2, z^{2^{\ell-1}}\rangle$. The concrete descriptions of the centers are then easy to read off from the relations. ∎

Proposition 4.2. *Let $n = m$. If G and H are two of the groups $G_{\text{⚀}}, \dots, G_{\text{⚅}}$ with $\mathbb{F}G \cong \mathbb{F}H$ but $G \not\cong H$, then G and H are, up to exchange, isomorphic to the groups $G_{\text{⚄}}$ and $G_{\text{⚅}}$ with $n = m \geq 2$.*

Proof. We observe first that the coclass of the groups is $n + m - 1$ in general. Hence, the case $n = m = 1$ corresponds to the finite 2-groups of maximal class for which a positive answer to the modular isomorphism problem is obtained by Carlson [5], p. 434, and Bagínski [1].

Thus, we may assume that $n = m \geq 2$. Recall that $G_{\text{⚀}} \cong G_{\text{⚁}}$ and $G_{\text{⚂}} \cong G_{\text{⚃}} \cong G_{\text{⚄}}$ by (2.2). Since $\mathbf{Z}(G_{\text{⚀}}) \cong C_{2^{n-1}} \times C_{2^{m-1}} \times C_2$ and $\mathbf{Z}(G_{\text{⚄}}) \cong \mathbf{Z}(G_{\text{⚅}}) \cong C_{2^n} \times C_{2^{m-1}}$ from Lemma 4.1, the assertion follows. ∎

We will see in Lemmas 4.17 to 4.19 that the remaining cases cannot happen and hence $n > m$. The corner case $n > m = 1$ requires some extra work as the direct factor $C_{2^{m-1}}$ in Lemma 4.1 becomes trivial and the isomorphism type of the center is not sufficient to distinguish the groups as in cases where $m > 1$. Nevertheless, known group theoretical invariants give further information as we show now.

Proposition 4.3. *Let $n > m = 1$. Then $\mathbb{F}G_{\text{⚁}} \not\cong \mathbb{F}G_{\text{⚃}}$.*

Proof. We will calculate the number of conjugacy classes that consist of squares for each group. This is an invariant of the group algebra due to the work of Külshammer in Section 1 of [17], cf. Section 2.2 of [12] for a short proof. To see that these numbers are different for $G_{\text{⚁}}$ and $G_{\text{⚃}}$, consider a generic element $x^r y^s z^t$ with $0 \leq r \leq 2^n - 1, 0 \leq s \leq 1$ and $0 \leq t \leq 2^\ell - 1$. Then, independently of the group,

$$(x^r y^s z^t)^2 = \begin{cases} x^{2r} z^{2t} & (r \equiv 0 \mod 2,\ s = 0),\\ x^{2r} & (r \equiv 1 \mod 2,\ s = 0),\\ x^{2r} y^2 z^{2t-1} & (r \equiv 1 \mod 2,\ s = 1),\\ x^{2r} y^2 & (r \equiv 0 \mod 2,\ s = 1). \end{cases}$$

Note that if a square is not central, then its centralizer is given by the maximal subgroup $\langle x^2, y^2, z, xy\rangle$, the centralizer of the derived subgroup $\langle z\rangle$. So each conjugacy class containing squares has either one or two elements; this can be seen from the generic form of an element. The case $r \equiv 0 \mod 2$ and $s = 0$ covers all elements of shape $x^u z^v$ with $u \equiv 0 \mod 4$ and $v \equiv 0 \mod 2$. These elements are formally reading the same in $G_{\text{⚁}}$ and $G_{\text{⚃}}$

and they also give the same number of classes, as the centrality of an element of this shape does not depend on which group we choose. In the case $r \equiv 1 \mod 2$ and $s = 0$, we get elements of shape x^u with $u \equiv 2 \mod 4$. Again this is the same for $G_{⚁}$ and $G_{⚃}$. Next we consider the case $r \equiv 1 \mod 2$ and $s = 1$. In $G_{⚁}$, we have $x^{2r}y^2z^{2t-1} = x^{2r+2}z^{2t-1}$, so these are the elements of shape $x^u z^v$ with $u \equiv 0 \mod 4$ and $v \equiv 1 \mod 2$. In $G_{⚃}$, we have $x^{2r}y^2z^{2t-1} = x^{2r+2}z^{2t-1+2^{\ell-1}}$, which gives the same kind of elements.

Finally, we consider the case where there is a difference: $r \equiv 0 \mod 2$ and $s = 1$. In $G_{⚁}$, we have $x^{2r}y^2 = x^{2r+2}$, which are elements of shape x^u with $u \equiv 2 \mod 4$. These elements are not new as they already appeared in the second case (i.e., $r \equiv 1 \mod 2$ and $s = 0$). While in $G_{⚃}$, we have $x^{2r}y^2 = x^{2r+2}z^{2^{\ell-1}}$, which are elements of shape $x^u z^{2^{\ell-1}}$ for $u \equiv 2 \mod 4$. These elements are new, so in particular there are 2^{n-2} more conjugacy classes of squares in $G_{⚃}$ than in $G_{⚁}$. ■

Proposition 4.4. *Let $n > m = 1$. Then $\mathbb{F}G_{⚀} \not\cong \mathbb{F}G_{⚂}$.*

Proof. Note that $G_{⚀}$ contains an elementary abelian subgroup of rank three, namely, the group $\langle x^{2^{n-1}}, y, z^{2^{\ell-1}} \rangle$. By contrast, $G_{⚂}$ does not since the only involutions are $x^{2^{n-1}}, z^{2^{\ell-1}}$ and $x^{2^{n-1}}z^{2^{\ell-1}}$. As the maximal rank of an elementary abelian subgroup is known to be an invariant of the group algebra due to the work of Quillen (Theorem 6.28 in [24]), we conclude that $\mathbb{F}G_{⚀} \not\cong \mathbb{F}G_{⚂}$. ■

Proposition 4.5. *Let $n > m$. If G and H are two of the groups $G_{⚀}, \ldots, G_{⚅}$ with $\mathbb{F}G \cong \mathbb{F}H$ but $G \not\cong H$, then G and H are, up to exchange, isomorphic to one of the following groups:*

1. *$G_{⚀}$ and $G_{⚁}$,*
2. *$G_{⚂}$ and $G_{⚃}$,*
3. *$G_{⚄}$ and $G_{⚅}$.*

Proof. This follows from Lemma 4.1 and Propositions 4.3 and 4.4. See also Table 1. ■

We note that computer experiments for the remaining cases in Propositions 4.2 and 4.5 show that the group-theoretical invariants contained in the GAP package ModIsomExt [19, 20] do not give new information on whether the algebras in question are isomorphic. (These invariants can now also be computed using the version 3.0.0 of the ModIsom package [8].)

4.2. Kernel sizes

We will write Δ for the augmentation ideal $\Delta(G)$ of $\mathbb{F}G$ for brevity. The next argument we will apply is well known and consists in computing the sizes of the kernels of certain maps. It can be traced back to an idea of Brauer (Section 9 of Supplements in [3]), and was applied in practice for the first time by Passman [22]. For a positive integer s, we define the standard 2^s-power map

$$\varphi_s : \Delta/\Delta^2 \to \Delta^{2^s}/\Delta^{1+2^s}. \tag{4.1}$$

The kernel of a power map φ_s is defined to be

$$K_s(G) = \{R + \Delta^2 \in \Delta/\Delta^2 \mid \varphi_s(R + \Delta^2) = 0 + \Delta^{1+2^s}\}.$$

Note that this kernel is not an ideal of Δ in general, but still a well-defined set stable under automorphisms of the algebra.

A basis for Δ makes concrete calculations of the kernels feasible, and we use what is called a Jennings basis, which behaves well with a filtration $\Delta \supseteq \Delta^2 \supseteq \cdots$. We will work with a basis that looks formally the same in each case. We assume some familiarity with Jennings' theory for the proof of the next lemma. If the reader is willing to accept it, then one can safely skip its proof because we will not use Jennings' theory explicitly elsewhere.

We write capital letters for elements of the augmentation ideal corresponding to group elements, e.g., $X = x + 1 \in \Delta$ for $x \in G$.

Lemma 4.6. *Let $G = \langle x, y, z\rangle$ be one of the groups $G_{\text{⚀}}, \dots, G_{\text{⚅}}$ and k a non-negative integer. Set*

$$w = z^{2^{\ell-1}} \quad \textit{and} \quad q = \begin{cases} 2^{\ell} & (G = G_{\text{⚀}} \textit{ or } G = G_{\text{⚁}}), \\ 2^{\max\{m,\ell\}} & (G = G_{\text{⚂}} \textit{ or } G = G_{\text{⚃}}), \\ 2^{\max\{n,\ell\}} & (G = G_{\text{⚄}} \textit{ or } G = G_{\text{⚅}}). \end{cases} \tag{4.2}$$

Then

$$\mathfrak{D}_k = \left\{ X^r Y^s Z^t W^u \;\middle|\; \begin{array}{c} 0 \le r \le 2^n - 1,\ 0 \le s \le 2^m - 1, \\ 0 \le t \le 2^{\ell-1} - 1,\ 0 \le u \le 1, \\ r + s + 2t + qu \ge k \end{array} \right\} \tag{4.3}$$

is a basis of Δ^k. In particular, the image of $\mathfrak{D}_k \setminus \mathfrak{D}_{k+1}$ under the natural projection $\Delta^k \to \Delta^k/\Delta^{k+1}$ is a basis of Δ^k/Δ^{k+1}.

Proof. Let $M_k = G \cap (1 + \Delta^k)$, the kth dimension subgroup of G, for $k \ge 1$. Observe first that $G' = \langle z\rangle$ and $\Phi(G) = \langle x^2, y^2, z\rangle$ are abelian. It follows from Theorems 11.2 and 12.9 in [6] that $M_1 = \langle x, y\rangle$ and

$$2^{e-1} < k \le 2^e \implies M_k = \mho_e(G)\,\mho_{e-1}(G') = \langle x^{2^e}, y^{2^e}, z^{2^{e-1}}\rangle$$

for $e \ge 1$. In particular, we have

$$\begin{aligned} 0 \le e \le n-1 &\implies & x^{2^e} &\in M_{2^e} \setminus M_{1+2^e}, \\ 0 \le e \le m-1 &\implies & y^{2^e} &\in M_{2^e} \setminus M_{1+2^e}, \\ 1 \le e \le \ell-1 &\implies & z^{2^{e-1}} &\in M_{2^e} \setminus M_{1+2^e}, \end{aligned}$$

and by the relations of G, one has

$$w \in M_q \setminus M_{1+q}.$$

Since x^2 and y^2 are central, an element of the Jennings basis can be written in the form

$$\begin{aligned}
&(x+1)^{r_0}(y+1)^{s_0}(x^2+1)^{r_1}(y^2+1)^{s_1}(z+1)^{t_0}\cdots(w+1)^u\cdots\\
&\quad=(x+1)^{r_0}(x^2+1)^{r_1}\cdots(y+1)^{s_0}(y^2+1)^{s_1}\cdots(z+1)^{t_0}\cdots(w+1)^u\\
&\quad=(x+1)^{r_0}(x+1)^{r_1 2}\cdots(y+1)^{s_0}(y+1)^{s_1 2}\cdots(z+1)^{t_0}\cdots(w+1)^u\\
&\quad=(x+1)^{r_0+\cdots+r_{n-1}2^{n-1}}(y+1)^{s_0+\cdots+s_{m-1}2^{m-1}}(z+1)^{t_0+\cdots+t_{\ell-2}2^{\ell-2}}(w+1)^u\\
&\quad=(x+1)^r(y+1)^s(z+1)^t(w+1)^u\\
&\quad=X^rY^sZ^tW^u
\end{aligned}$$

for

$$0\le r_0,r_1,\dots,r_{n-1},s_0,s_1,\dots,s_{m-1},t_0,\dots,t_{\ell-2},u\le 1$$

where $r=r_0+\cdots+r_{n-1}2^{n-1}$, $s=s_0+\cdots+s_{m-1}2^{m-1}$ and $t=t_0+\cdots+t_{\ell-2}2^{\ell-2}$. Hence, the assertion follows from Jennings' theorem (Theorem 3.2 in [15]). ■

The *weight* of an element of $\mathfrak{D}_k\setminus\mathfrak{D}_{k+1}$ is defined to be k.

To aid the reader in the following calculations, we explicitly state the bases of the first few layers of the subsequent quotients of the augmentation ideal power series when $n\ge m\ge 2$:

$$\begin{aligned}
\Delta^1/\Delta^2 &: \mathfrak{D}_1\setminus\mathfrak{D}_2=\{X,Y\},\\
\Delta^2/\Delta^3 &: \mathfrak{D}_2\setminus\mathfrak{D}_3=\{X^2,XY,Y^2,Z\},\\
\Delta^3/\Delta^4 &: \mathfrak{D}_3\setminus\mathfrak{D}_4=\{X^3,X^2Y,XY^2,XZ,Y^3,YZ\}.
\end{aligned}$$

We will collect some elementary relations between the elements of the basis, which we will use without further mention:

$$\begin{aligned}
XY+YX&=Z+XZ+YZ+XYZ,\\
XY+YX&\equiv Z \mod \Delta^3.
\end{aligned}$$

Now a more concrete expression of the power map (4.1) can be obtained.

Lemma 4.7. *Let $G=\langle x,y,z\rangle$ be one of the groups $G_{\text{⚀}},\dots,G_{\text{⚅}}$ and $\alpha,\beta\in\mathbb{F}$. Then*

$$\varphi_m(\alpha X+\beta Y+\Delta^2)=\alpha^{2^m}X^{2^m}+\beta^{2^m}Y^{2^m}+(\alpha\beta)^{2^{m-1}}Z^{2^{m-1}}+\Delta^{1+2^m}.$$

Proof. In general, we have

$$\begin{aligned}
(\alpha X+\beta Y)^2&=\alpha^2X^2+\beta^2Y^2+(\alpha\beta)(XY+YX)\\
&\equiv\alpha^2X^2+\beta^2Y^2+(\alpha\beta)Z \mod \Delta^3.
\end{aligned}$$

Since X^2 and Y^2 are central in $\mathbb{F}G$, we obtain

$$\varphi_m(\alpha X+\beta Y+\Delta^2)=\alpha^{2^m}X^{2^m}+\beta^{2^m}Y^{2^m}+(\alpha\beta)^{2^{m-1}}Z^{2^{m-1}}+\Delta^{1+2^m}.$$ ■

Lemma 4.8. *Assume $n>m$ and let G be one of the groups $G_{\text{⚀}},\dots,G_{\text{⚅}}$. Then the kernel $K_m(G)$ of the power map φ_m has the cardinality shown in Table 2.*

	$m > \ell$	$m = \ell$	$m < \ell$
⚀	$\lvert\mathbb{F}\rvert$	$\lvert\mathbb{F}\rvert$	$\lvert\mathbb{F}\rvert$
⚁	$\lvert\mathbb{F}\rvert$	1	1
⚂	1	1	$\lvert\mathbb{F}\rvert$
⚃	1	$\lvert\mathbb{F}\rvert$	1
⚄	$\lvert\mathbb{F}\rvert$	$\lvert\mathbb{F}\rvert$	$\lvert\mathbb{F}\rvert$
⚅	$\lvert\mathbb{F}\rvert$	1	1

Table 2. Kernel sizes $|K_m(G)|$ for $n > m$.

Proof. Let $G = \langle x, y, z\rangle$. Every element of Δ/Δ^2 can be written in the form $\alpha X + \beta Y + \Delta^2$ and the scalars $\alpha, \beta \in \mathbb{F}$ are unique by Lemma 4.6. To measure the size of the kernel, we write $\varphi_m(\alpha X + \beta Y + \Delta^2)$ in Lemma 4.7 as a linear combination of the images of $\mathfrak{D}_{2^m} \setminus \mathfrak{D}_{1+2^m}$ in $\Delta^{2^m}/\Delta^{1+2^m}$ for each case. Note that as $n > m$, the differences between $G_{⚀}$ and $G_{⚄}$ as well as between $G_{⚁}$ and $G_{⚅}$ cannot enter into the expression of $\varphi_m(\alpha X + \beta Y + \Delta^2)$, so we handle these two pairs of groups simultaneously. We write $w = z^{2^{\ell-1}}$ as in (4.2) and also use the equation $Y^{2^m} = X^{2^m} + W + X^{2^m}W$ for $G = G_{⚃}$.

For $m > \ell$, as $Z^{2^{m-1}}$ vanishes, $\varphi_m(\alpha X + \beta Y + \Delta^2)$ is written as follows:

$$\begin{aligned}
\text{⚀⚄}: &\quad & \alpha^{2^m} X^{2^m} + \Delta^{1+2^m},\\
\text{⚁⚅}: &\quad & (\alpha^{2^m} + \beta^{2^m})X^{2^m} + \Delta^{1+2^m},\\
\text{⚂}: &\quad & \alpha^{2^m} X^{2^m} + \beta^{2^m} W + \Delta^{1+2^m},\\
\text{⚃}: &\quad & (\alpha^{2^m} + \beta^{2^m})X^{2^m} + \beta^{2^m} W + \Delta^{1+2^m}.
\end{aligned}$$

Similarly, for $m < \ell$, the following is obtained:

$$\begin{aligned}
\text{⚀⚄}: &\quad & \alpha^{2^m} X^{2^m} + (\alpha\beta)^{2^{m-1}} Z^{2^{m-1}} + \Delta^{1+2^m},\\
\text{⚁⚅}: &\quad & (\alpha^{2^m} + \beta^{2^m})X^{2^m} + (\alpha\beta)^{2^{m-1}} Z^{2^{m-1}} + \Delta^{1+2^m},\\
\text{⚂}: &\quad & \alpha^{2^m} X^{2^m} + (\alpha\beta)^{2^{m-1}} Z^{2^{m-1}} + \Delta^{1+2^m},\\
\text{⚃}: &\quad & (\alpha^{2^m} + \beta^{2^m})X^{2^m} + (\alpha\beta)^{2^{m-1}} Z^{2^{m-1}} + \Delta^{1+2^m}.
\end{aligned}$$

Finally, for $m = \ell$, the expressions for $G_{⚀}$, $G_{⚁}$, $G_{⚄}$ and $G_{⚅}$ are as in the case $m < \ell$, and for the other two we have the following:

$$\begin{aligned}
\text{⚂}: &\quad & \alpha^{2^m} X^{2^m} + (\beta^{2^m} + (\alpha\beta)^{2^{m-1}})W + \Delta^{1+2^m},\\
\text{⚃}: &\quad & (\alpha^{2^m} + \beta^{2^m})X^{2^m} + (\beta^{2^m} + (\alpha\beta)^{2^{m-1}})W + \Delta^{1+2^m}.
\end{aligned}$$

All of the terms present are linearly independent by Lemma 4.6. Therefore, $\alpha X + \beta Y + \Delta^2$ belongs to the kernel $K_m(G)$ if and only if all of the coefficients present are equal to zero. Since the Frobenius map on $\mathbb{F}$ is injective, the cardinalities for $K_m(G)$ now follow easily. ■

We remark that in the case $n = m$, the kernel size can also give some useful information, but only if one restricts the possibilities for $\mathbb{F}$. As we prefer to work independently of the base field, we do not include the corresponding calculations.

We summarize the progress we have made on the proof of Theorem A in this section.

Proposition 4.9. *If G and H are two of the groups $G_{\text{⚀}}, \dots, G_{\text{⚅}}$ with $\mathbb{F}G \cong \mathbb{F}H$ but $G \not\cong H$, then G and H are, up to exchange, isomorphic to one of the following groups:*

1. *$G_{\text{⚀}}$ and $G_{\text{⚁}}$ with $n > m > \ell$,*
2. *$G_{\text{⚂}}$ and $G_{\text{⚃}}$ with $n > m > \ell$,*
3. *$G_{\text{⚄}}$ and $G_{\text{⚅}}$ with $n > m > \ell$,*
4. *$G_{\text{⚄}}$ and $G_{\text{⚅}}$ with $n = m \geq 2$.*

Proof. By Proposition 4.2, it suffices to show that one of the first three items holds under the assumption $n > m$. It follows from Proposition 4.5 that G and H are, up to exchange, isomorphic to one of the followings: $G_{\text{⚀}}$ and $G_{\text{⚁}}$, $G_{\text{⚂}}$ and $G_{\text{⚃}}$, $G_{\text{⚄}}$ and $G_{\text{⚅}}$. If $m = \ell$ or $m < \ell$, then the groups in each pair have different kernel sizes by Lemma 4.8, which contradicts $\mathbb{F}G \cong \mathbb{F}H$. Hence, we have $m > \ell$. ■

Some more information can be obtained from canonical ideals. The following proposition could be used to further reduce the cases, though we will not use it in this sense, but rather differently later on. It seems to have the potential to also be applicable to other classes of groups.

Proposition 4.10. *Let G be a finite p-group and $\mathbb{F}$ a field of characteristic p. Assume that G' is abelian of exponent p^ℓ. Then*

$$\mathbb{F}(\mho_r(\mathbf{Z}(G))) = \mho_r(\mathbf{Z}(\mathbb{F}G))$$

for every integer $r \geq \ell$ and, in particular, $\Delta(\mho_r(\mathbf{Z}(G)))$ is canonical in $\mathbb{F}G$. Consequently, if $\mathbb{F}G \cong \mathbb{F}H$, then $\mathbb{F}[G/\mho_r(\mathbf{Z}(G))] \cong \mathbb{F}[H/\mho_r(\mathbf{Z}(H))]$.

Proof. Recall that $\mathbf{Z}(\mathbb{F}G)$ has a basis that is given by class sums and a decomposition $\mathbf{Z}(\mathbb{F}G) = \mathbb{F}\mathbf{Z}(G) \oplus (\mathbf{Z}(\mathbb{F}G) \cap [\mathbb{F}G, \mathbb{F}G])$. We will show that class sums of non-central elements vanish under a p^r-power. So let $g \in G$ be a non-central element with conjugacy class $\{ga_1, \dots, ga_s\}$ for some $a_1, \dots, a_s \in G'$. Note that p divides s. The class sum of g equals $g(a_1 + \dots + a_s)$. As this element is central in $\mathbb{F}G$, it commutes in particular with g, hence $(a_1 + \dots + a_s)$ commutes with g. As G' is abelian of exponent $p^\ell \leq p^r$, we conclude that

$$(g(a_1 + \dots + a_s))^{p^r} = g^{p^r}(a_1^{p^r} + \dots + a_s^{p^r}) = g^{p^r}s = 0. \qquad ■$$

The next lemma is an easy observation which will be helpful in some calculations.

Lemma 4.11. *Let $G = \langle x, y, z \rangle$ be one of the groups $G_{\text{⚀}}, \dots, G_{\text{⚅}}$. Then $[X, Y]$ is central in $\mathbb{F}G$.*

Proof. We have $[X, Y] = xy + yx = xy + xyz$. As $(xy)^x = xyz = (xy)^y$ and $(xyz)^x = xy = (xyz)^y$, we conclude that $[X, Y]$ is a class sum and hence central in $\mathbb{F}G$. ■

4.3. Group base approximation

We will handle the rest of the cases by a procedure that could be called a "group base approximation". We will first make a few general observations on group bases satisfying the relations of the normal form given in Theorem 2.1, and then see in each single case why this leads to a contradiction.

4.3.1. General group bases. Now we fix integers n, m and ℓ with $n \geq m \geq 2$ and $\ell \geq 2$. Fix a group G from $G_{\text{⚀}}, \dots, G_{\text{⚅}}$ generated by x, y and z, which satisfy the defining relations. Also fix another group base H in $\mathbb{F}G$ from $G_{\text{⚀}}, \dots, G_{\text{⚅}}$ generated by a, b and c, which satisfy the defining relations. Thus, throughout this section, we assume

$$n \geq m \geq 2,\ \ell \geq 2, \quad G = G_{\boxed{?}},\ H = G_{\boxed{¿}}, \quad \boxed{?}, \boxed{¿} \in \{\text{⚀}, \dots, \text{⚅}\},$$
$$G = \langle x, y, z\rangle, \quad a, b, c \in 1 + \Delta(G), \quad H = \langle a, b, c\rangle, \quad \mathbb{F}G = \mathbb{F}H.$$

As before, we write Δ for $\Delta(G)$ and use the basis $\mathfrak{D}_k$ of Δ^k introduced in Lemma 4.6. Recall that $w = z^{2^{\ell-1}}$, so in this basis $W = Z^{2^{\ell-1}}$, and the weight of W is denoted by q as in (4.2); the exact value of q will be irrelevant, except the fact that $q \geq 4$ as $\ell \geq 2$.

Since $n \geq m \geq 2$, the squares x^2 and y^2 are not trivial and we have

$$\Delta = \mathbb{F}X \oplus \mathbb{F}Y \oplus \mathbb{F}XY \oplus \mathbb{F}Z \oplus \mathbb{F}X^2 \oplus \mathbb{F}Y^2 \oplus \Delta^3.$$

From now on square brackets denote Lie commutators in Δ, i.e., $[U, V] = UV + VU$ for $U, V \in \Delta$. We will frequently use without comment the commutator formula

$$[S, T] = (1 + S + T + ST)(1 + t^{-1}s^{-1}ts),$$

which holds for all $s, t \in G$. In particular, $[X, Y] = (1 + X + Y + XY)Z$. Moreover, as $z^{-1}z^x, z^{-1}z^y \in \langle z^2\rangle$, we have $[X, Z], [Y, Z] \in Z^2\mathbb{F}G \subseteq \Delta^4$.

We first consider A and B modulo Δ^3. Write

$$\begin{aligned} A &= \alpha_A X + \beta_A Y + \gamma_A XY + \delta_A Z + \xi_A X^2 + \eta_A Y^2 + U_A, \\ B &= \alpha_B X + \beta_B Y + \gamma_B XY + \delta_B Z + \xi_B X^2 + \eta_B Y^2 + U_B, \end{aligned} \tag{4.4}$$

where $\alpha_A, \alpha_B, \dots, \eta_A, \eta_B \in \mathbb{F}$ and $U_A, U_B \in \Delta^3$. Note that the scalars are uniquely determined. This notation will be fixed throughout this section. Observe that $A + \Delta^2$ and $B + \Delta^2$ span the two-dimensional vector space Δ/Δ^2, as a and b generate H. Hence, they must be linearly independent, and we have

$$\alpha_A \beta_B + \alpha_B \beta_A \neq 0. \tag{4.5}$$

We first show that XY does not appear as a summand in A and B.

Lemma 4.12. *We have $\gamma_A = \gamma_B = 0$.*

Proof. The proof is identical for A and B, so we only show $\gamma_A = 0$. The idea is to use the fact that A^2 is central in $\mathbb{F}G$, as a^2 is central in H.

Let Ξ be the linear subspace of Δ defined by

$$\Xi = \{R \in \Delta^2 \mid [R, S] \in \Delta^5 \text{ for all } S \in \Delta\}.$$

Note that $\Delta^4 \subseteq \Xi$ and $[X,Y] \in \Xi$ by Lemma 4.11. We will consider A^2 modulo Ξ. We will use that

$$\begin{aligned}
&[X,Z],[Y,Z] \in Z^2\mathbb{F}G \subseteq \Delta^4 \subseteq \Xi,\\
&[X,XY] = X[X,Y] \equiv XZ \mod \Xi,\\
&[Y,XY] = [X,Y]Y \equiv YZ \mod \Xi.
\end{aligned}$$

From (4.4), we get

$$\begin{aligned}
A^2 &\equiv \alpha_A\beta_A[X,Y] + \alpha_A\gamma_A[X,XY] + \beta_A\gamma_A[Y,XY]\\
&\equiv \alpha_A\gamma_A X[X,Y] + \beta_A\gamma_A[Y,X]Y \equiv \alpha_A\gamma_A XZ + \beta_A\gamma_A YZ \mod \Xi,
\end{aligned} \tag{4.6}$$

where $[X,Y] \in \Xi$ is used to go from the first to the second line. Computing commutators modulo Δ^5 gives

$$[XZ,Y] \equiv [YZ,X] \equiv Z^2 \mod \Delta^5, \quad [XZ,X] \equiv [YZ,Y] \equiv 0 \mod \Delta^5.$$

So modulo Δ^5 computing commutators with A^2 using (4.6) and the definition of Ξ yields

$$[A^2,X] \equiv \beta_A\gamma_A Z^2 \mod \Delta^5, \quad [A^2,Y] \equiv \alpha_A\gamma_A Z^2 \mod \Delta^5.$$

As A^2 is central in $\mathbb{F}G$, we conclude that $\alpha_A\gamma_A = \beta_A\gamma_A = 0$. But as $\alpha_A \neq 0$ or $\beta_A \neq 0$ by $A \notin \Delta^2$, this implies $\gamma_A = 0$. ■

The next lemma allows us to make conclusions about scalars from a relation between A^{2^n} and B^{2^n}.

Lemma 4.13. *We have*

$$\begin{aligned}
A^{2^n} &\equiv \alpha_A^{2^n} X^{2^n} + \beta_A^{2^n} Y^{2^n} \mod \mathbf{Z}(\mathbb{F}G) \cap [\mathbb{F}G,\mathbb{F}G],\\
B^{2^n} &\equiv \alpha_B^{2^n} X^{2^n} + \beta_B^{2^n} Y^{2^n} \mod \mathbf{Z}(\mathbb{F}G) \cap [\mathbb{F}G,\mathbb{F}G].
\end{aligned}$$

Proof. We first observe that, by Lemma 4.1 and (4.2), $\mathbf{Z}(G)$ is generated by x^2, y^2 and w. Thus,

$$\mathbb{F}\mathbf{Z}(G) \cap \Delta = \sum_{\substack{r,s,t \geq 0\\ 2r+2s+qt \geq 1}} \mathbb{F}X^{2r}Y^{2s}W^t \subseteq \mathbb{F}X^2 + \mathbb{F}Y^2 + \Delta^4. \tag{4.7}$$

We will prove the claims only for A as the arguments for B are identical. Recall that (4.4) and Lemma 4.12 imply

$$A = \alpha_A X + \beta_A Y + \delta_A Z + \xi_A X^2 + \eta_A Y^2 + U_A.$$

So, by $[X,Y] \equiv Z \mod \Delta^3$, it yields

$$A^2 \equiv \alpha_A^2 X^2 + \beta_A^2 Y^2 + \alpha_A\beta_A Z \mod \Delta^3. \tag{4.8}$$

Using the decomposition $\mathbf{Z}(\mathbb{F}G) = \mathbb{F}\mathbf{Z}(G) \oplus (\mathbf{Z}(\mathbb{F}G) \cap [\mathbb{F}G,\mathbb{F}G])$, we get

$$A^2 = \alpha_A^2 X^2 + \beta_A^2 Y^2 + R_A + S_A \tag{4.9}$$

for some $R_A \in \mathbb{F}\mathbf{Z}(G) \cap \Delta$ and $S_A \in \mathbf{Z}(\mathbb{F}G) \cap [\mathbb{F}G,\mathbb{F}G]$.

Now S_A can be written as a linear combination of class sums of non-central elements. It follows from $G' = \langle z \rangle$ that

$$S_A \in \mathbb{F}Z + \Delta^3.$$

Indeed, let $g = x^i y^j z^k$ be a representative of a non-central conjugacy class of G with $i, j, k \geq 0$. Since the conjugacy class of g can be written as

$$\{gz^{e_1}, \dots, gz^{e_t}\}$$

for some non-trivial power t of 2 and some $e_1, \dots, e_t \geq 0$, the class sum of the conjugacy class can be written as follows:

$$\begin{aligned} gz^{e_1} + \dots + gz^{e_t} &= x^i y^j z^k (z^{e_1} + \dots + z^{e_t}) \\ &= (1+X)^i (1+Y)^j (1+Z)^k ((1+Z)^{e_1} + \dots + (1+Z)^{e_t}) \\ &\equiv (1+X)^i (1+Y)^j (1+Z)^k (e_1 + \dots + e_t) Z \\ &\equiv (e_1 + \dots + e_t) Z \mod \Delta^3. \end{aligned}$$

Hence, S_A belongs to the desired vector space.

Since $R_A \in \mathbb{F}X^2 + \mathbb{F}Y^2 + \Delta^4$, $S_A \in \mathbb{F}Z + \Delta^3$ and $X^2 + \Delta^3$, $Y^2 + \Delta^3$, $Z + \Delta^3$ are linearly independent in Δ^2/Δ^3, reformulating (4.8) and (4.9) as

$$R_A + S_A \equiv \alpha_A \beta_A Z \mod \Delta^3,$$

it follows that $R_A \in \Delta^4$. Hence, $R_A^{2^{n-1}} \in \Delta^{2^{n+1}}$. Since $X^{2^{n+1}} = 0$, $X^{2^n} Y^{2^n} = 0$, $Y^{2^{n+1}} = 0$ and $W^2 = 0$ by the relations of G, we get $R_A^{2^{n-1}} = 0$ from (4.7). Raising (4.9) to a power hence yields

$$A^{2^n} = \alpha_A^{2^n} X^{2^n} + \beta_A^{2^n} Y^{2^n} + S_A^{2^{n-1}},$$

and the claim follows. ∎

The element $C = 1 + c$ will play an important role and we first approximate it modulo Δ^4.

Lemma 4.14. *The following congruence holds*:

$$C \equiv \lambda Z + \mu XZ + \nu YZ \mod \Delta^4,$$

where $\lambda = \alpha_A \beta_B + \alpha_B \beta_A$, $\mu = \lambda(1 + \alpha_A + \alpha_B)$ *and* $\nu = \lambda(1 + \beta_A + \beta_B)$.

Proof. From the definitions, we have

$$C = 1 + c = 1 + b^{-1}a^{-1}ba = 1 + (1+B)^{-1}(1+A)^{-1}(1+B)(1+A).$$

For $R \in \Delta$, one has $(1+R)^{-1} = 1 + R + R^2 + \dots + R^k$ for some k such that $R^k = 0$. Hence,

$$\begin{aligned} C &\equiv 1 + (1 + B + B^2 + B^3)(1 + A + A^2 + A^3)(1+B)(1+A) \\ &\equiv [A, B] + A[A, B] + B[A, B] \equiv (1 + A + B)[A, B] \mod \Delta^4, \end{aligned}$$

by an explicit multiplication, with cancellation afterwards as we may in characteristic 2.

Then, by the fact that $[X,Z],[Y,Z]\in\Delta^4$, $U_A,U_B\in\Delta^3$ and $\gamma_A=\gamma_B=0$ (Lemma 4.12), from (4.4) we obtain

$$C\equiv(1+\alpha_AX+\beta_AY+\alpha_BX+\beta_BY)[\alpha_AX+\beta_AY,\alpha_BX+\beta_BY]\mod\Delta^4.$$

Since $[X,Y]=(1+X+Y+XY)Z$, straightforward calculations yield that

$$\begin{aligned}C&\equiv(1+(\alpha_A+\alpha_B)X+(\beta_A+\beta_B)Y)(\alpha_A\beta_B+\alpha_B\beta_A)(Z+XZ+YZ)\\&\equiv(\alpha_A\beta_B+\alpha_B\beta_A)(Z+(1+\alpha_A+\alpha_B)XZ+(1+\beta_A+\beta_B)YZ)\mod\Delta^4.\quad\blacksquare\end{aligned}$$

We now define a variation of a power map that will turn out to be very useful to us. First set $\Gamma=\Delta(G')\mathbb{F}G=[\mathbb{F}G,\mathbb{F}G]\mathbb{F}G$. Note that $\Gamma=Z\mathbb{F}G$, and thus the subset

$$\mathfrak{C}=\left\{X^rY^sZ^tW^u\;\middle|\;\begin{array}{c}0\le r\le 2^n-1,\ 0\le s\le 2^m-1,\\0\le t\le 2^{\ell-1}-1,\ 0\le u\le 1,\ 2t+qu\ge 1\end{array}\right\}\tag{4.10}$$

of the basis of $\mathbb{F}G$ defined in Lemma 4.6 is a basis of Γ. In fact, it follows from the observations that $\mathfrak{C}$ is a linearly independent subset of $Z\mathbb{F}G$ and consists of $|G|-|G:G'|$ elements. The condition $2t+qu\ge 1$ is equivalent to $(t,u)\ne(0,0)$, but we formulate in this way to indicate the weight contributed by the powers of Z and W.

Recall that q denotes the weight of W. Set $d=1+2^{\ell-1}+q$, and define a map

$$\psi:\Gamma/\Gamma^2\to\Gamma^{2^{\ell-1}}/(\Gamma^{1+2^{\ell-1}}+\Delta^d)\cap\Gamma^{2^{\ell-1}}\tag{4.11}$$

that is induced from the $2^{\ell-1}$-power map. As will become clear, the reason for the definition of d is that W, $X^{2^{\ell-1}}W$ and $Y^{2^{\ell-1}}W$ are non-zero modulo $(\Gamma^{1+2^{\ell-1}}+\Delta^d)\cap\Gamma^{2^{\ell-1}}$, while other elements in $\mathfrak{C}$ that span the image of ψ are zero.

Lemma 4.15. *For $T\in\Delta^2$ and $\lambda,\mu,\nu\in\mathbb{F}$, we have*

$$\begin{aligned}&\psi(\lambda Z+\mu XZ+\nu YZ+TZ+\Gamma^2)\\&\qquad=\lambda^{2^{\ell-1}}W+\mu^{2^{\ell-1}}X^{2^{\ell-1}}W+\nu^{2^{\ell-1}}Y^{2^{\ell-1}}W+(\Gamma^{1+2^{\ell-1}}+\Delta^d)\cap\Gamma^{2^{\ell-1}}.\end{aligned}$$

Proof. To prove the lemma, we factor ψ as a composition of maps. Define the square-map

$$\psi_i:\Gamma^{2^i}/\Gamma^{1+2^i}\to\Gamma^{2^{i+1}}/\Gamma^{1+2^{i+1}}$$

for $i\ge 0$ and the natural projection

$$\pi:\Gamma^{2^{\ell-1}}/\Gamma^{1+2^{\ell-1}}\to\Gamma^{2^{\ell-1}}/(\Gamma^{1+2^{\ell-1}}+\Delta^d)\cap\Gamma^{2^{\ell-1}}.$$

Then $\psi=\pi\circ\psi_{\ell-2}\circ\cdots\circ\psi_1\circ\psi_0$. Note that this expression is well defined as $\ell\ge 2$.

Claim 1. For $g\in G$ and $i\ge 0$, one has $[g,Z^{2^i}]\in\Gamma^{2^{i+1}}$.

It suffices to show that $1+g^{-1}Z^{2^i}g\equiv 1+Z^{2^i}\mod\Gamma^{2^{i+1}}$. From the general formula $(1+R)^{-1}=1+R+R^2+\cdots$ for $R\in\Delta$, we get

$$1+Z^{-2^i}=(1+Z^{2^i})^{-1}=1+Z^{2^i}+(Z^{2^i})^2+\cdots\equiv 1+Z^{2^i}\mod\Gamma^{2^{i+1}}.$$

Note that $\{z^{2^i},z^{-2^i}\}$ is a conjugacy class of G. Thus, $1+g^{-1}Z^{2^i}g$ is equal to $1+Z^{2^i}$ or $1+Z^{-2^i}$ and the claim holds.

Claim 2. For $R, S \in \mathbb{F}G$, one has

$$\psi_i(RZ^{2^i} + SZ^{2^i} + \Gamma^{1+2^i}) = R^2 Z^{2^{i+1}} + S^2 Z^{2^{i+1}} + \Gamma^{1+2^{i+1}}.$$

From the previous claim we know $[R, Z^{2^i}], [S, Z^{2^i}] \in \Gamma^{2^{i+1}}$, so

$$\begin{aligned}\psi_i(RZ^{2^i} + SZ^{2^i} + \Gamma^{1+2^i}) &= (RZ^{2^i})^2 + (SZ^{2^i})^2 + [RZ^{2^i}, SZ^{2^i}] + \Gamma^{1+2^{i+1}} \\ &= R^2 Z^{2^{i+1}} + S^2 Z^{2^{i+1}} + [R, S]Z^{2^{i+1}} + \Gamma^{1+2^{i+1}}.\end{aligned}$$

As $[R, S] \in \Gamma$, the claim follows.

Now applying the last claim stepwise to $\psi_0, \psi_1, \dots, \psi_{\ell-2}$ gives

$$\begin{aligned}&(\psi_{\ell-2} \circ \dots \circ \psi_1 \circ \psi_0)(\lambda Z + \mu XZ + \nu YZ + TZ + \Gamma^2) \\ &\quad = \lambda^{2^{\ell-1}} W + \mu^{2^{\ell-1}} X^{2^{\ell-1}} W + \nu^{2^{\ell-1}} Y^{2^{\ell-1}} W + T^{2^{\ell-1}} W + \Gamma^{1+2^{\ell-1}}.\end{aligned}$$

As $T^{2^{\ell-1}} \in \Delta^{2^\ell}$, this means $T^{2^{\ell-1}} W \in \Delta^d$. Thus, applying π eliminates the last term, and the lemma follows. ■

4.3.2. Specific cases.

Next we consider the coefficients α_A and α_B. As the calculations are no longer uniform for all groups, we introduce case distinctions.

Lemma 4.16. *If $G \cong G_{\text{⚂}}$, $H \cong G_{\text{⚃}}$ and $n > m > \ell$, then $\alpha_A = \alpha_B$.*

If $G \cong G_{\text{⚄}}$ and $H \cong G_{\text{⚅}}$, then we have the following:

(1) *$m > \ell$ implies $\alpha_A = \alpha_B$,*

(2) *$n = m = \ell$ implies $\alpha_A(\alpha_A + \beta_A) = \alpha_B(\alpha_B + \beta_B)$,*

(3) *$n = m < \ell$ implies $\alpha_A \beta_A = \alpha_B \beta_B = 0$.*

Proof. Recall that φ_m denotes the 2^m-power map $\Delta/\Delta^2 \to \Delta^{2^m}/\Delta^{1+2^m}$. In this proof, the fact that the Frobenius map on $\mathbb{F}$ is injective will be used without further comment.

First consider $G \cong G_{\text{⚄}}$ and $H \cong G_{\text{⚅}}$. By Lemma 4.7 and $Y^{2^m} = 0$, we have

$$\varphi_m(A + \Delta^2) = \alpha_A^{2^m} X^{2^m} + (\alpha_A \beta_A)^{2^{m-1}} Z^{2^{m-1}} + \Delta^{1+2^m}$$

and, if additionally $n = m$ holds,

$$\varphi_m(A + \Delta^2) = \alpha_A^{2^m} W + (\alpha_A \beta_A)^{2^{m-1}} Z^{2^{m-1}} + \Delta^{1+2^m}.$$

Similar expressions hold for $\varphi_m(B + \Delta^2)$. Note that the relation $a^{2^m} = b^{2^m}$, which holds in H, implies $\varphi_m(A + \Delta^2) = \varphi_m(B + \Delta^2)$.

Now, consider $m > \ell$. Then $Z^{2^{m-1}} = 0$, and so $\varphi_m(A + \Delta^2) = \varphi_m(B + \Delta^2)$ implies $\alpha_A^{2^m} X^{2^m} + \Delta^{1+2^m} = \alpha_B^{2^m} X^{2^m} + \Delta^{1+2^m}$. As $X^{2^m} \in \mathfrak{D}_{2^m} \setminus \mathfrak{D}_{1+2^m}$, we have $\alpha_A = \alpha_B$. Note that if additionally $n = m$ holds, then we have $X^{2^m} = W$, but this does not change the conclusion, as then $W \in \mathfrak{D}_{2^m} \setminus \mathfrak{D}_{1+2^m}$.

Next, consider $n = m = \ell$. Then $\varphi_m(A + \Delta^2) = \varphi_m(B + \Delta^2)$ implies

$$(\alpha_A^{2^m} + (\alpha_A \beta_A)^{2^{m-1}})W + \Delta^{1+2^m} = (\alpha_B^{2^m} + (\alpha_B \beta_B)^{2^{m-1}})W + \Delta^{1+2^m}.$$

As $W \in \mathfrak{D}_{2^m} \setminus \mathfrak{D}_{1+2^m}$, this implies $\alpha_A^2 + \alpha_A \beta_A = \alpha_B^2 + \alpha_B \beta_B$ and hence the claim.

Finally, consider $n = m < \ell$. Then $W \in \Delta^{1+2^m}$ and $C^{2^{\ell-1}} \in \Delta^{1+2^m}$. So, because of $a^{2^m} = b^{2^m} = c^{2^{\ell-1}}$, we have

$$\varphi_m(A + \Delta^2) = \varphi_m(B + \Delta^2) = 0 + \Delta^{1+2^m}.$$

As

$$\begin{aligned}\varphi_m(A + \Delta^2) &= (\alpha_A\beta_A)^{2^{m-1}} Z^{2^{m-1}} + \Delta^{1+2^m},\\ \varphi_m(B + \Delta^2) &= (\alpha_B\beta_B)^{2^{m-1}} Z^{2^{m-1}} + \Delta^{1+2^m},\end{aligned}$$

this together with $Z^{2^{m-1}} \in \mathfrak{D}_{2^m} \setminus \mathfrak{D}_{1+2^m}$ implies $\alpha_A\beta_A = \alpha_B\beta_B = 0$.

Finally, consider $G \cong G_{\text{⚂}}$, $H \cong G_{\text{⚃}}$ and $n > m > \ell$. Then, by Lemma 4.7 and using $Y^{2^m} = W$, $Z^{2^\ell} = 0$ and $m > \ell$, we get from (4.4):

$$\begin{aligned}\varphi_m(A + \Delta^2) &= \alpha_A^{2^m} X^{2^m} + \beta_A^{2^m} W + \Delta^{1+2^m},\\ \varphi_m(B + \Delta^2) &= \alpha_B^{2^m} X^{2^m} + \beta_B^{2^m} W + \Delta^{1+2^m}.\end{aligned} \tag{4.12}$$

Now $H \cong G_{\text{⚃}}$ means $b^{2^m} = a^{2^m}c^{2^{\ell-1}}$, so

$$\begin{aligned}\varphi_m(B + \Delta^2) = B^{2^m} + \Delta^{1+2^m} &= 1 + a^{2^m}c^{2^{\ell-1}} + \Delta^{1+2^m}\\ &= A^{2^m} + C^{2^{\ell-1}} + A^{2^m}C^{2^{\ell-1}} + \Delta^{1+2^m}.\end{aligned} \tag{4.13}$$

We next consider A^{2^m} and B^{2^m} modulo $\Gamma + \Delta^{1+2^m}$ which is done by “deleting the Z’s and C’s”, roughly speaking. Formally, (4.12) and (4.13) imply

$$\alpha_A^{2^m} X^{2^m} \equiv A^{2^m} \equiv B^{2^m} \equiv \alpha_B^{2^m} X^{2^m} \mod \Gamma + \Delta^{1+2^m}.$$

Now as X^{2^m} does not lie in $\Gamma + \Delta^{1+2^m}$ by (4.10) and (4.3), we get $\alpha_A = \alpha_B$. ■

With these preparations, we are finally ready to solve the modular isomorphism problem for all the remaining cases. In the first two cases, $m \le \ell$ holds, and we use the explicit approximations of A^{2^n} and B^{2^n} given by Lemma 4.13. In the last two cases, $m > \ell$ holds, and we use the explicit approximation of $C^{2^{\ell-1}}$ given by Lemmas 4.14 and 4.15.

Lemma 4.17. *If $n = m < \ell$, then $\mathbb{F}G_{\text{⚄}} \not\cong \mathbb{F}G_{\text{⚅}}$.*

Proof. Assume the notation (4.4), $n = m < \ell$, $G \cong G_{\text{⚄}}$ and $H \cong G_{\text{⚅}}$. By the relations $X^{2^n} = W$ and $Y^{2^n} = 0$, we have

$$A^{2^n} \equiv \alpha_A^{2^n} W \mod \mathbf{Z}(\mathbb{F}G) \cap [\mathbb{F}G, \mathbb{F}G]$$

by Lemma 4.13. Similarly, we have

$$B^{2^n} \equiv \alpha_B^{2^n} W \mod \mathbf{Z}(\mathbb{F}G) \cap [\mathbb{F}G, \mathbb{F}G].$$

As in H the relation $a^{2^n} = b^{2^n}$ holds by $n = m$, from the fact that W is a non-zero element in $\mathbb{F}\mathbf{Z}(G)$ and the decomposition $\mathbf{Z}(\mathbb{F}G) = \mathbb{F}\mathbf{Z}(G) \oplus (\mathbf{Z}(\mathbb{F}G) \cap [\mathbb{F}G, \mathbb{F}G])$, we conclude that $\alpha_A = \alpha_B$.

As $n = m < \ell$, Lemma 4.16 implies $\alpha_A\beta_A = \alpha_B\beta_B = 0$. Hence, as $\alpha_A = \alpha_B$, we get $\alpha_A\beta_B + \alpha_B\beta_A = 0$, which contradicts (4.5). ■

The proof of the next case parallels that of the first case.

Lemma 4.18. *If $n = m = \ell$, then $\mathbb{F}G_{⚄} \not\cong \mathbb{F}G_{⚅}$.*

Proof. Assume the notation (4.4), $n = m = \ell$, $G \cong G_{⚄}$ and $H \cong G_{⚅}$. We conclude that $\alpha_A = \alpha_B$ by the same arguments as in the proof of Lemma 4.17.

As $n = m = \ell$, Lemma 4.16 and $\alpha_A = \alpha_B$ imply $\alpha_A\beta_A = \alpha_B\beta_B$. Hence, $\alpha_A\beta_B + \alpha_B\beta_A = 0$, which contradicts (4.5). ■

Lemma 4.19. *If $m > \ell$, then $\mathbb{F}G_{⚄} \not\cong \mathbb{F}G_{⚅}$.*

Proof. Assume the notation (4.4), $m > \ell$, $G \cong G_{⚄}$ and $H \cong G_{⚅}$. As $n > \ell$, we obtain $\mho_{n-1}(\mathbf{Z}(\mathbb{F}G)) = \mathbb{F}(\mho_{n-1}(\mathbf{Z}(G)))$ by Proposition 4.10. This is generated by W as an algebra since Lemma 4.1 shows that $\mho_{n-1}(\mathbf{Z}(G))$ is generated by w from the relations $x^{2^n} = w$ and $y^{2^m} = 1$. Thus, $\mho_{n-1}(\mathbf{Z}(\mathbb{F}G)) \cap \Gamma = \mathbb{F}W$. As a^2 is central and $c^{2^{\ell-1}} = a^{2^n}$ by the defining relations of H, we see that $C^{2^{\ell-1}} = (A^2)^{2^{n-1}}$ lies in $\mho_{n-1}(\mathbf{Z}(\mathbb{F}G))$. Hence, $C^{2^{\ell-1}} \in \mathbb{F}W$.

Recall the definition (4.11) of the map ψ. Now, by Lemmas 4.14 and 4.15, we know

$$\psi(C + \Gamma^2) = \lambda^{2^{\ell-1}}W + \mu^{2^{\ell-1}}X^{2^{\ell-1}}W + \nu^{2^{\ell-1}}Y^{2^{\ell-1}}W + (\Gamma^{1+2^{\ell-1}} + \Delta^d),$$

where $\lambda = \alpha_A\beta_B + \alpha_B\beta_A$, $\mu = \lambda(1 + \alpha_A + \alpha_B)$ and $\nu = \lambda(1 + \beta_A + \beta_B)$.

As $X^{2^{\ell-1}}W$ does not lie in $\mathbb{F}W$ and neither in $\Gamma^{1+2^{\ell-1}} + \Delta^d$ by (4.10) and (4.3), the coefficient of it in the expression of $\psi(C + \Gamma^2)$ is 0 by $C^{2^{\ell-1}} \in \mathbb{F}W$. This coefficient equals a power of μ and by Lemma 4.16, this implies $\lambda = 0$, which contradicts (4.5). ■

The proof of the last case parallels that of the previous case.

Lemma 4.20. *If $n > m > \ell$, then $\mathbb{F}G_{⚂} \not\cong \mathbb{F}G_{⚃}$.*

Proof. Assume the notation (4.4), $n > m > \ell$, $G \cong G_{⚂}$ and $H \cong G_{⚃}$. As $m > \ell$, we obtain $\mho_{m-1}(\mathbf{Z}(\mathbb{F}G)) = \mathbb{F}(\mho_{m-1}(\mathbf{Z}(G)))$ by Proposition 4.10. This is generated by X^{2^m} and W as an algebra, since Lemma 4.1 shows that $\mho_{m-1}(\mathbf{Z}(G))$ is generated by x^{2^m} and w from the relation $y^{2^m} = w$. Recall that $d = 1 + 2^{\ell-1} + q$. Now, the weight of $X^{2^m}W$ is $2^m + q$ which is bigger than d as $m > \ell$. Thus, $\mho_{m-1}(\mathbf{Z}(\mathbb{F}G)) \cap \Gamma \subseteq \mathbb{F}W + \Delta^d$. As $a^{-2}b^2$ is central and $(a^{-2}b^2)^{2^{m-1}} = a^{-2^m}b^{2^m} = a^{-2^m}a^{2^m}c^{2^{\ell-1}} = c^{2^{\ell-1}}$ by the defining relations of H, we see that $C^{2^{\ell-1}} = (1 + a^{-2}b^2)^{2^{m-1}}$ lies in $\mho_{m-1}(\mathbf{Z}(\mathbb{F}G))$. Hence, $C^{2^{\ell-1}} \in \mathbb{F}W + \Delta^d$.

The rest of the argument is essentially the same as at the end of the proof of the previous lemma: by the previous paragraph, we known that the coefficient of $X^{2^{\ell-1}}W$ in the expression of $\psi(C + \Gamma^2)$ is 0. On the other hand, by Lemmas 4.14 and 4.15, this coefficient equals a power of μ. By Lemma 4.16, we conclude that $\lambda = 0$, which contradicts (4.5). ■

Now we give a proof of Theorem A using the results obtained so far.

Proof of Theorem A. It remains to show that the groups in Corollary 3.4 are the only counterexamples to the modular isomorphism problem in our class.

First we show that H is two-generated and the central quotient of H is dihedral. The minimal number of generators is a well-known invariant and a proof can be found in Lemma 14.2.7 of [23]. Note that the central quotient of H is dihedral if and only if

$|H : \mathbf{Z}(H)| \geq 8$ and $|H : H'\mathbf{Z}(H)| = 4$; thus it is also an invariant by a result of Margolis, Sakurai and Stanojkovski (Corollary 2.8 and Lemma 5.9 in [21]). Since the order and the isomorphism type of the abelianization are invariant, the groups have common parameters n, m and ℓ.

By Theorems 2.1 and 3.1 and Proposition 4.9, it remains to show that $\mathbb{F}G_{⚄} \not\cong \mathbb{F}G_{⚅}$ when either $n = m \geq 2$ or $n > m > \ell$ and that $\mathbb{F}G_{⚂} \not\cong G_{⚃}$ when $n > m > \ell$. If $n = m \geq 2$, then we conclude that $\mathbb{F}G_{⚄} \not\cong \mathbb{F}G_{⚅}$ from Lemmas 4.17 to 4.19. If $n > m > \ell$, then we conclude that $\mathbb{F}G_{⚄} \not\cong \mathbb{F}G_{⚅}$ from Lemma 4.19, and $\mathbb{F}G_{⚂} \not\cong \mathbb{F}G_{⚃}$ from Lemma 4.20. ■

Remark 4.21. The arguments involved in the group base approximation partly explain the choice we make for the isomorphism in Theorem 3.1. There are of course many more choices for this isomorphism, but Lemma 4.12 imposes some restrictions, for example. A similar argument, as in the first case proved in Lemma 4.16, can be used to show that $\alpha_A = \alpha_B$ needs to hold in the setting of Theorem 3.1. Eventually the choice we make for the isomorphism seems to be the easiest.

Moreover, the arguments in Section 4 suggest that the straightforward calculations in the proof of Theorem 3.1 not only make this proof easy, but also make it possible. Any relation in a group H that requires to compute an actual commutator in the group algebra of another group G for some given elements is not only difficult to verify, it imposes conditions that are difficult to meet in the first place.

A. Distinction of groups

In the class of two-generated finite 2-groups with dihedral central quotient, each group has a presentation of the form in Theorem 2.1. The goal of this appendix is to establish by group-theoretical arguments when these groups are non-isomorphic and to obtain the classification of groups within this class. Let n, m and ℓ denote positive integers. Recall that a group is *homocyclic* if it is isomorphic to a direct product of copies of a cyclic group.

Theorem A.1. *The six groups $G_{⚀}, \dots, G_{⚅}$ are pairwise non-isomorphic if they do not have homocyclic abelianizations* (*i.e.*, $n > m$).

Theorem A.2. *The three groups $G_{⚀}$, $G_{⚄}$, $G_{⚅}$ are pairwise non-isomorphic if they have homocyclic abelianizations* (*i.e.*, $n = m$). *Moreover, in this case, $G_{⚀} \cong G_{⚁}$ and $G_{⚂} \cong G_{⚃} \cong G_{⚄}$.*

These theorems follow immediately from Theorem A and Lemma 3.2; nevertheless, we will provide a direct group-theoretical proof. We do this by considering the centers and maximal quotients of the groups. We will write $G_{⚀}(n, m, \ell), \dots, G_{⚅}(n, m, \ell)$ to make the parameters n, m and ℓ explicit when necessary.

A.1. Maximal quotients

To describe the maximal quotients, we first describe the socle in each case, as the central involutions are exactly the generators of minimal normal subgroups. By the socle of a finite p-group, we mean the subgroup generated by central elements of order p. From Lemma 4.1, we directly get the socles in all cases.

Lemma A.3. *Assume $n \geq 2$. Then the following hold*:

$$\Omega(\mathbf{Z}(G_{\text{⚀}})) = \begin{cases} \langle x^{2^{n-1}} \rangle \times \langle y^{2^{m-1}} \rangle \times \langle z^{2^{\ell-1}} \rangle \cong C_2 \times C_2 \times C_2 & (m \geq 2), \\ \langle x^{2^{n-1}} \rangle \times \langle z^{2^{\ell-1}} \rangle \cong C_2 \times C_2 & (m = 1), \end{cases}$$

$$\Omega(\mathbf{Z}(G_{\text{⚁}})) = \begin{cases} \langle x^{2^{n-1}} \rangle \times \langle x^{-2^{m-1}} y^{2^{m-1}} \rangle \times \langle z^{2^{\ell-1}} \rangle \cong C_2 \times C_2 \times C_2 & (m \geq 2), \\ \langle x^{2^{n-1}} \rangle \times \langle z^{2^{\ell-1}} \rangle \cong C_2 \times C_2 & (m = 1), \end{cases}$$

$$\Omega(\mathbf{Z}(G_{\text{⚂}})) = \langle x^{2^{n-1}} \rangle \times \langle z^{2^{\ell-1}} \rangle \cong C_2 \times C_2,$$

$$\Omega(\mathbf{Z}(G_{\text{⚃}})) = \langle x^{2^{n-1}} \rangle \times \langle z^{2^{\ell-1}} \rangle \cong C_2 \times C_2,$$

$$\Omega(\mathbf{Z}(G_{\text{⚄}})) = \begin{cases} \langle y^{2^{m-1}} \rangle \times \langle z^{2^{\ell-1}} \rangle \cong C_2 \times C_2 & (m \geq 2), \\ \langle z^{2^{\ell-1}} \rangle \cong C_2 & (m = 1), \end{cases}$$

$$\Omega(\mathbf{Z}(G_{\text{⚅}})) = \begin{cases} \langle x^{-2^{m-1}} y^{2^{m-1}} \rangle \times \langle z^{2^{\ell-1}} \rangle \cong C_2 \times C_2 & (m \geq 2), \\ \langle z^{2^{\ell-1}} \rangle \cong C_2 & (m = 1). \end{cases}$$

The next lemma describes all the maximal quotients of the six groups in Theorem 2.1.

Lemma A.4. *Assume $n \geq 2$. Let G be one of the groups $G_{\text{⚀}}(n, m, \ell), \dots, G_{\text{⚅}}(n, m, \ell)$ and Q a maximal quotient of G. Then $Q \cong G_{\boxed{?}}(n', m', \ell')$ for some $\boxed{?} \in \{\text{⚀}, \dots, \text{⚅}\}$ and n', m', ℓ' satisfying $n' + m' + \ell' = n + m + \ell - 1$; all the possible values of the parameters for Q are divided into five cases*:

(1) $n > m + 1$ *and* $m \geq 2$ (*Table* 3),

(2) $n = m + 1$ *and* $m \geq 2$ (*Table* 4),

(3) $n = m$ *and* $m \geq 2$ (*Table* 5),

(4) $n > m + 1$ *and* $m = 1$ (*Table* 6),

(5) $n = m + 1$ *and* $m = 1$ (*Table* 7),

and those are summarized in Tables 3 *to* 7.

Proof. In all cases, the proof is obtained by applying Lemma 2.3 to each maximal quotient in each case, which corresponds to a minimal normal subgroup generated by a non-trivial element of the socle in Lemma A.3. ■

	$(n-1, m, \ell)$	$(n, m-1, \ell)$	$(n, m, \ell-1)$
$G_{\text{⚀}}(n, m, \ell)$	$G_{\text{⚀}}$ $G_{\text{⚄}}$	$G_{\text{⚀}}$ $G_{\text{⚂}}$	$G_{\text{⚀}}$
$G_{\text{⚁}}(n, m, \ell)$	$G_{\text{⚁}}$ $G_{\text{⚅}}$	$G_{\text{⚁}}$ $G_{\text{⚃}}$	$G_{\text{⚁}}$
$G_{\text{⚂}}(n, m, \ell)$	$G_{\text{⚂}}$ $G_{\text{⚄}}$		$G_{\text{⚀}}$
$G_{\text{⚃}}(n, m, \ell)$	$G_{\text{⚃}}$ $G_{\text{⚅}}$		$G_{\text{⚁}}$
$G_{\text{⚄}}(n, m, \ell)$		$G_{\text{⚄}}$	$G_{\text{⚀}}$
$G_{\text{⚅}}(n, m, \ell)$		$G_{\text{⚅}}$	$G_{\text{⚁}}$

Table 3. Maximal quotients when $n > m + 1$, $m \geq 2$.

	$(n-1,m,\ell)$	$(n,m-1,\ell)$	$(n,m,\ell-1)$
$G_{⚀}(n,m,\ell)$	$G_{⚀}$ $G_{⚄}$	$G_{⚀}$ $G_{⚂}$	$G_{⚀}$
$G_{⚁}(n,m,\ell)$	$G_{⚀}$ $G_{⚅}$	$G_{⚁}$ $G_{⚃}$	$G_{⚁}$
$G_{⚂}(n,m,\ell)$	$G_{⚄}$ $G_{⚅}$		$G_{⚀}$
$G_{⚃}(n,m,\ell)$	$G_{⚄}$		$G_{⚁}$
$G_{⚄}(n,m,\ell)$		$G_{⚄}$	$G_{⚀}$
$G_{⚅}(n,m,\ell)$		$G_{⚅}$	$G_{⚁}$

Table 4. Maximal quotients when $n = m + 1$, $m \geq 2$.

	$(n-1,m,\ell)$	$(n,m-1,\ell)$	$(n,m,\ell-1)$
$G_{⚀}(n,m,\ell)$		$G_{⚀}$ $G_{⚁}$ $G_{⚂}$ $G_{⚃}$	$G_{⚀}$
$G_{⚁}(n,m,\ell)$		$G_{⚀}$ $G_{⚁}$ $G_{⚂}$ $G_{⚃}$	$G_{⚁}$
$G_{⚂}(n,m,\ell)$		$G_{⚄}$	$G_{⚀}$
$G_{⚃}(n,m,\ell)$		$G_{⚄}$	$G_{⚁}$
$G_{⚄}(n,m,\ell)$		$G_{⚄}$	$G_{⚀}$
$G_{⚅}(n,m,\ell)$		$G_{⚅}$	$G_{⚁}$

Table 5. Maximal quotients when $n = m$, $m \geq 2$.

	$(n-1,m,\ell)$	$(n,m-1,\ell)$	$(n,m,\ell-1)$
$G_{⚀}(n,m,\ell)$	$G_{⚀}$ $G_{⚄}$		$G_{⚀}$
$G_{⚁}(n,m,\ell)$	$G_{⚁}$ $G_{⚅}$		$G_{⚁}$
$G_{⚂}(n,m,\ell)$	$G_{⚂}$ $G_{⚄}$		$G_{⚀}$
$G_{⚃}(n,m,\ell)$	$G_{⚃}$ $G_{⚅}$		$G_{⚁}$
$G_{⚄}(n,m,\ell)$			$G_{⚀}$
$G_{⚅}(n,m,\ell)$			$G_{⚁}$

Table 6. Maximal quotients when $n > m + 1$, $m = 1$.

	$(n-1,m,\ell)$	$(n,m-1,\ell)$	$(n,m,\ell-1)$
$G_{⚀}(n,m,\ell)$	$G_{⚀}$ $G_{⚄}$		$G_{⚀}$
$G_{⚁}(n,m,\ell)$	$G_{⚀}$ $G_{⚅}$		$G_{⚁}$
$G_{⚂}(n,m,\ell)$	$G_{⚄}$ $G_{⚅}$		$G_{⚀}$
$G_{⚃}(n,m,\ell)$	$G_{⚄}$		$G_{⚁}$
$G_{⚄}(n,m,\ell)$			$G_{⚀}$
$G_{⚅}(n,m,\ell)$			$G_{⚁}$

Table 7. Maximal quotients when $n = m + 1$, $m = 1$.

We finish this subsection with an illustration of the studied groups by a graph, which can be derived from Lemma A.4 in Figure 1.

$$\begin{tikzcd}
2^{n+m+2} & G_{\text{⚂}}(n,m,2) & G_{\text{⚀}}(n,m,2) & G_{\text{⚄}}(n,m,2) & G_{\text{⚃}}(n,m,2) & G_{\text{⚁}}(n,m,2) & G_{\text{⚅}}(n,m,2) \\
2^{n+m+3} & G_{\text{⚂}}(n,m,3) \arrow[ur, two heads] & G_{\text{⚀}}(n,m,3) \arrow[u, two heads] & G_{\text{⚄}}(n,m,3) \arrow[ul, two heads] & G_{\text{⚃}}(n,m,3) \arrow[ur, two heads] & G_{\text{⚁}}(n,m,3) \arrow[u, two heads] & G_{\text{⚅}}(n,m,3) \arrow[ul, two heads] \\
\vdots & \vdots \arrow[ur, two heads] & \vdots \arrow[u, two heads] & \vdots \arrow[ul, two heads] & \vdots \arrow[ur, two heads] & \vdots \arrow[u, two heads] & \vdots \arrow[ul, two heads] \\
2^{n+m+\ell-1} & G_{\text{⚂}}(n,m,\ell-1) \arrow[ur, two heads] & G_{\text{⚀}}(n,m,\ell-1) \arrow[u, two heads] & G_{\text{⚄}}(n,m,\ell-1) \arrow[ul, two heads] & G_{\text{⚃}}(n,m,\ell-1) \arrow[ur, two heads] & G_{\text{⚁}}(n,m,\ell-1) \arrow[u, two heads] & G_{\text{⚅}}(n,m,\ell-1) \arrow[ul, two heads] \\
2^{n+m+\ell} & G_{\text{⚂}}(n,m,\ell) \arrow[ur, two heads] & G_{\text{⚀}}(n,m,\ell) \arrow[u, two heads] & G_{\text{⚄}}(n,m,\ell) \arrow[ul, two heads] & G_{\text{⚃}}(n,m,\ell) \arrow[ur, two heads] & G_{\text{⚁}}(n,m,\ell) \arrow[u, two heads] & G_{\text{⚅}}(n,m,\ell) \arrow[ul, two heads] \\
\vdots & \vdots \arrow[ur, two heads] & \vdots \arrow[u, two heads] & \vdots \arrow[ul, two heads] & \vdots \arrow[ur, two heads] & \vdots \arrow[u, two heads] & \vdots \arrow[ul, two heads]
\end{tikzcd}$$

Figure 1. Finite 2-groups with dihedral central quotient whose abelianization is isomorphic to $C_{2^n} \times C_{2^m}$ and not homocyclic. An arrow from a group G to H is drawn if H is isomorphic to a maximal quotient of G, that is, G is an immediate descendant of H.

A.2. Inductive argument

We will now proceed to prove Theorems A.1 and A.2. This will be achieved by a double induction. The outer induction runs on the first parameter, i.e., n, and the inner on the second parameter, i.e., m. We will need the following two cases for the base of the inductions.

Recall the standard presentations of finite 2-groups of maximal class: the dihedral, semidihedral and generalized quaternion groups.

$$\begin{aligned}
D_{2^{n+1}} &= \langle a, b \mid a^2 = 1,\ b^{2^n} = 1,\ b^a = b^{-1} \rangle,\\
S_{2^{n+1}} &= \langle a, b \mid a^2 = 1,\ b^{2^n} = 1,\ b^a = b^{2^{n-1}-1} \rangle,\\
Q_{2^{n+1}} &= \langle a, b \mid a^2 = b^{2^{n-1}},\ b^{2^n} = 1,\ b^a = b^{-1} \rangle.
\end{aligned}$$

Proposition A.5. *Assume $\ell \geq 2$. Then*

$$D_{2^{\ell+2}} \cong G_{⚀}(1,1,\ell), \quad S_{2^{\ell+2}} \cong G_{⚄}(1,1,\ell), \quad Q_{2^{\ell+2}} \cong G_{⚅}(1,1,\ell).$$

In particular, $G_{⚀}(1,1,\ell)$, $G_{⚄}(1,1,\ell)$ and $G_{⚅}(1,1,\ell)$ are pairwise non-isomorphic.

Proof. Since the three cases have the same kind of isomorphism $a \mapsto y$ and $b \mapsto xy$, we only prove that $Q_{2^{\ell+2}} \cong G_{⚅}(1,1,\ell)$ here.

Let $G_{⚅}(1,1,\ell) = \langle x, y, z \rangle$ and define $a = y$ and $b = xy$. Since

$$b^2 = xyxy = x^2y[y,x]y = x^2yzy = z^{2^{\ell-1}}yzy = z^{2^{\ell-1}}y^2z[z,y] = z^{2^\ell}z[z,y] = z^{-1},$$

we have, using that y^2 is central in the last equation,

$$\begin{aligned}
a^2 &= y^2 = z^{2^{\ell-1}} = z^{-2^{\ell-1}} = b^{2^\ell},\\
b^{2^{\ell+1}} &= z^{-2^\ell} = 1,\\
b^a &= (xy)^y = y^{-1}xy^2 = yx = xy[y,x] = xyz = bb^{-2} = b^{-1}.
\end{aligned}$$

Hence, there is an epimorphism from $Q_{2^{\ell+2}}$ to $G_{⚅}(1,1,\ell)$. Since both groups have the same order, they must be isomorphic. ■

Lemma A.6. *Assume $n \geq 2$. Then $G_{⚀}(n,1,1) \ncong G_{⚁}(n,1,1)$.*

Proof. Observe that $G_{⚀}(n,1,1)$ has a maximal subgroup that is isomorphic to $C_{2^{n-1}} \times C_2 \times C_2$, namely, $\langle x^2, y, z \rangle$, while $G_{⚁}(n,1,1)$ does not. Indeed, we have $\Phi(G_{⚁}(n,1,1)) = \langle x^2, z \rangle$, so that the maximal subgroups of $G_{⚁}(n,1,1)$ are $\langle x, z \rangle$, $\langle y, z \rangle$ and $\langle xy, x^2 \rangle$. Note here that $(xy)^2 = x^2y^2z = x^4z$, so that $z \in \langle xy, x^2 \rangle$. Hence, all the maximal subgroups of $G_{⚁}(n,1,1)$ are two-generated. ■

We are ready for the inductions.

Proof of Theorems A.1 and A.2. We first note that when $n = m$, then the isomorphisms $G_{⚀}(n,m,\ell) \cong G_{⚁}(n,m,\ell)$ and $G_{⚂}(n,m,\ell) \cong G_{⚃}(n,m,\ell) \cong G_{⚄}(n,m,\ell)$ are clear from the presentations.

We proceed by induction on n. If $n = 1$, then also $m = 1$ and the groups $G_{⚀}(n,m,\ell)$, $G_{⚄}(n,m,\ell)$ and $G_{⚅}(n,m,\ell)$ are pairwise non-isomorphic by Proposition A.5.

So assume that $n \geq 2$ and that Theorems A.1 and A.2 hold for smaller values of n. We proceed by induction on m. When $m = 1$, then by Lemma 4.1 the centers of $G_{⚀}(n,m,\ell)$, $G_{⚁}(n,m,\ell)$, $G_{⚂}(n,m,\ell)$ and $G_{⚃}(n,m,\ell)$ are not isomorphic to the centers of $G_{⚄}(n,m,\ell)$ and $G_{⚅}(n,m,\ell)$. By induction and Tables 6 and 7, only $G_{⚀}(n,m,\ell)$ or $G_{⚁}(n,m,\ell)$ can map onto one of the groups $G_{⚀}(n-1,m,\ell)$ or $G_{⚁}(n-1,m,\ell)$, so these two groups are not isomorphic to either of $G_{⚂}(n,m,\ell)$ or $G_{⚃}(n,m,\ell)$. To see that $G_{⚀}(n,m,\ell)$ is not isomorphic to $G_{⚁}(n,m,\ell)$, note that, again by induction and Tables 6 and 7, $G_{⚁}(n,m,\ell)$ maps onto $G_{⚅}(n-1,m,\ell)$, while $G_{⚀}(n,m,\ell)$ does not. To see that $G_{⚂}(n,m,\ell)$ is not isomorphic to $G_{⚃}(n,m,\ell)$, note that, by Tables 6 and 7, exactly one of them maps onto $G_{⚅}(n-1,m,\ell)$ by induction. To distinguish between $G_{⚄}(n,m,\ell)$ and $G_{⚅}(n,m,\ell)$, we observe that, again by Tables 6 and 7, the only maximal quotient of $G_{⚄}(n,m,\ell)$ is $G_{⚀}(n,m,\ell-1)$, while the only maximal quotient of $G_{⚅}(n,m,\ell)$ is $G_{⚁}(n,m,\ell-1)$. If $\ell=2$, then these quotients are not isomorphic and hence neither are the groups $G_{⚄}(n,m,\ell)$ and $G_{⚅}(n,m,\ell)$ by Lemma A.6. In the case $\ell > 2$, the quotients $G_{⚀}(n,m,\ell-1)$ and $G_{⚁}(n,m,\ell-1)$ are also not isomorphic, as we showed earlier in this paragraph. This finishes the case $m = 1$.

Consider next $n > m \geq 2$ and assume that Theorems A.1 and A.2 hold for smaller values of n or m. Looking on the centers of the groups in Lemma 4.1, we see that we only need to show that $G_{⚀}(n,m,\ell) \ncong G_{⚁}(n,m,\ell)$, $G_{⚂}(n,m,\ell) \ncong G_{⚃}(n,m,\ell)$ and $G_{⚄}(n,m,\ell) \ncong G_{⚅}(n,m,\ell)$. To distinguish between $G_{⚀}(n,m,\ell)$ and $G_{⚁}(n,m,\ell)$, note that, by induction and Tables 3 and 4, the group $G_{⚀}(n,m,\ell)$ maps onto $G_{⚀}(n,m-1,\ell)$, while $G_{⚁}(n,m,\ell)$ does not. To see that $G_{⚂}(n,m,\ell) \ncong G_{⚃}(n,m,\ell)$, we note that, again by induction and Tables 3 and 4, exactly one of them maps onto $G_{⚅}(n-1,m,\ell)$. Finally, to observe that $G_{⚄}(n,m,\ell)$ and $G_{⚅}(n,m,\ell)$ are not isomorphic, we also use induction and Tables 3 and 4 to see that $G_{⚄}(n,m,\ell)$ maps onto $G_{⚄}(n,m-1,\ell)$, while $G_{⚅}(n,m,\ell)$ does not.

The last case to consider is $n = m$. Recall that then $G_{⚀}(n,m,\ell) \cong G_{⚁}(n,m,\ell)$ and $G_{⚂}(n,m,\ell) \cong G_{⚃}(n,m,\ell) \cong G_{⚄}(n,m,\ell)$. So after looking at the centers in Lemma 4.1, it only remains to show that $G_{⚄}(n,m,\ell)$ and $G_{⚅}(n,m,\ell)$ are not isomorphic. By induction and Table 5, we observe that $G_{⚅}(n,m,\ell)$ maps onto $G_{⚅}(n,m-1,\ell)$, which is not the case for $G_{⚄}(n,m,\ell)$. This finishes the inner induction and hence also the induction step of the outer induction. ■

Acknowledgments. We would like to acknowledge the anonymous referees for their helpful suggestions which improved the presentation of this article.

Funding. This work has been supported by the Madrid Government (Comunidad de Madrid - Spain) under the multiannual Agreement with UAM in the line for the Excellence of the University Research Staff in the context of the V PRICIT (Regional Programme of Research and Technological Innovation). The authors acknowledges financial support from the Spanish Ministry of Science and Innovation, through the Severo Ochoa Programme for Centers of Excellence in R&D (CEX2019-000904-S) and through the Ramón y Cajal grant program.

References

[1] Bagiński, C.: Modular group algebras of 2-groups of maximal class. *Comm. Algebra* **20** (1992), no. 5, 1229–1241. Zbl 0751.20004 MR 1157906

[2] Bagiński, C.: On the isomorphism problem for modular group algebras of elementary abelian-by-cyclic p-groups. *Colloq. Math.* **82** (1999), no. 1, 125–136. Zbl 0943.20007 MR 1736040

[3] Brauer, R.: Representations of finite groups. In *Lectures on Modern Mathematics, Vol. I*, pp. 133–175. Wiley, New York-London, 1963. Zbl 0124.26504 MR 178056

[4] Broche, O., García-Lucas, D. and del Río, Á.: A classification of the finite 2-generator cyclic-by-abelian groups of prime-power order. *Internat. J. Algebra Comput.* **33** (2023), no. 4, 641–686. Zbl 1520.20042 MR 4615617

[5] Carlson, J. F.: Periodic modules over modular group algebras. *J. London Math. Soc. (2)* **15** (1977), no. 3, 431–436. Zbl 0365.20015 MR 472985

[6] Dixon, J. D., du Sautoy, M. P. F., Mann, A. and Segal, D.: *Analytic pro-p groups*. Second edition. Cambridge Stud. Adv. Math. 61, Cambridge University Press, Cambridge, 1999. Zbl 0934.20001 MR 1720368

[7] Drensky, V.: The isomorphism problem for modular group algebras of groups with large centres. In *Representation theory, group rings, and coding theory*, pp. 145–153. Contemp. Math. 93, American Mathematical Society, Providence, RI, 1989. Zbl 0682.20004 MR 1003349

[8] Eick, B., García-Lucas, D., Konovalov, O., Margolis, L. and Moede, T.: ModIsom, Computing automorphisms and checking isomorphisms for modular group algebras of finite p-groups, Version 3.0.0. 2024, https://gap-packages.github.io/modisom/, visited on 14 December 2024.

[9] García-Lucas, D. and del Río, Á.: On the modular isomorphism problem for 2-generated groups with cyclic derived subgroup. To appear in *J. Algebra Appl.*, DOI 10.1142/s0219498825503311.

[10] García-Lucas, D., del Río, Á. and Stanojkovski, M.: On group invariants determined by modular group algebras: even versus odd characteristic. *Algebr. Represent. Theory* **26** (2023), no. 6, 2683–2707. Zbl 1532.20026 MR 4681329

[11] García-Lucas, D., Margolis, L. and del Río, Á.: Non-isomorphic 2-groups with isomorphic modular group algebras. *J. Reine Angew. Math.* **783** (2022), 269–274. Zbl 1514.20019 MR 4373245

[12] Hertweck, M. and Soriano, M.: On the modular isomorphism problem: groups of order 2^6. In *Groups, rings and algebras*, pp. 177–213. Contemp. Math. 420, American Mathematical Society, Providence, RI, 2006. Zbl 1120.20005 MR 2279240

[13] Huppert, B.: *Endliche Gruppen. I*. Grundlehren Math. Wiss. 134, Springer, Berlin-New York, 1967. Zbl 0217.07201 MR 224703

[14] Isaacs, I. M.: *Algebra: A graduate course*. Grad. Stud. Math. 100, American Mathematical Society, Providence, RI, 2009. Zbl 1157.00004 MR 2472787

[15] Jennings, S. A.: The structure of the group ring of a p-group over a modular field. *Trans. Amer. Math. Soc.* **50** (1941), 175–185. Zbl 0025.24401 MR 4626

[16] Johnson, D. L.: *Presentations of groups*. Second edition. London Math. Soc. Stud. Texts 15, Cambridge University Press, Cambridge, 1997. Zbl 0906.20019 MR 1472735

[17] Külshammer, B.: Bemerkungen über die Gruppenalgebra als symmetrische Algebra. II. *J. Algebra* **75** (1982), no. 1, 59–69. Zbl 0488.16010 MR 650409

[18] Margolis, L.: The modular isomorphism problem: A survey. *Jahresber. Dtsch. Math.-Ver.* **124** (2022), no. 3, 157–196. Zbl 1535.20021 MR 4472590

[19] Margolis, L. and Moede, T.: The modular isomorphism problem for small groups – revisiting Eick's algorithm. *J. Comp. Algebra* **1** (2022), 1–7.

[20] Margolis, L. and Moede, T.: ModIsomExt, An extension of ModIsom, Version 1.0.0. 2020, https://www.tu-braunschweig.de/en/iaa/personal/moede, visited on 14 December 2024.

[21] Margolis, L., Sakurai, T. and Stanojkovski, M.: Abelian invariants and a reduction theorem for the modular isomorphism problem. *J. Algebra* **636** (2023), 1–27. Zbl 1533.16037 MR 4644311

[22] Passman, D. S.: The group algebras of groups of order p^4 over a modular field. *Michigan Math. J.* **12** (1965), 405–415. Zbl 0134.26304 MR 185022

[23] Passman, D. S.: *The algebraic structure of group rings*. Pure Appl. Math., Wiley, New York, 1977. Zbl 0368.16003 MR 470211

[24] Sandling, R.: The isomorphism problem for group rings: A survey. In *Orders and their applications (Oberwolfach, 1984)*, pp. 256–288. Lecture Notes in Math. 1142, Springer, Berlin, 1985. Zbl 0565.20005 MR 812504

[25] Sehgal, S. K.: *Topics in group rings*. Monogr. Textb. Pure App. Math. 50, Marcel Dekker, New York, 1978. Zbl 0411.16004 MR 508515

Received May 22, 2024; revised September 19, 2024.

Leo Margolis
Departamento de Matemáticas, Facultad de Ciencias, Universidad Autónoma de Madrid
C/ Francisco Tomás y Valiente 7, 28049 Madrid, Spain;
leo.margolis@icmat.es

Taro Sakurai
Department of Mathematics and Informatics, Graduate School of Science, Chiba University
1-33, Yayoi-cho, Inage-ku, Chiba 263-8522, Japan;
tsakurai@math.s.chiba-u.ac.jp