WHERE DO ISOMORPHISMS OF GROUP ALGEBRAS FAIL TO LIFT?

LEO MARGOLIS AND TARO SAKURAI

Abstract. Counterexamples to the Modular Isomorphism Problem were discovered recently. These are non-isomorphic finite 2-groups G and H that have isomorphic group algebras over the binary field $\mathbb{Z}/2\mathbb{Z}$ and non-isomorphic group algebras over the 2-adic integers $\mathbb{Z}_2$. We show that the groups G and H already have non-isomorphic group algebras over the ring $\mathbb{Z}/4\mathbb{Z}$.

1. Introduction

The Integral Isomorphism Problem asks whether non-isomorphic finite groups must have non-isomorphic group algebras over the integers $\mathbb{Z}$. This problem was proposed by Higman [7], who proved that it has a positive solution for finite abelian groups. For a prime p, Roggenkamp–Scott [17] and Weiss [21] proved that non-isomorphic finite p-groups have non-isomorphic group algebras even over the p-adic integers $\mathbb{Z}_p$. This result is sharp, because Hertweck [6] discovered counterexamples among finite solvable groups whose orders are divisible by exactly two distinct primes. In positive characteristic p, the Modular Isomorphism Problem asks whether non-isomorphic finite p-groups must have non-isomorphic group algebras over the prime field $\mathbb{Z}/p\mathbb{Z}$. For a survey, see [12]. Deskins [4] proved that this problem has a positive solution for finite abelian p-groups. Recently García-Lucas–Margolis–del Río [5] discovered counterexamples to the problem, later generalized in [1, 13].

These are non-isomorphic finite 2-groups G and H that have isomorphic group algebras over the binary field $\mathbb{Z}/2\mathbb{Z}$. By contrast, the groups G and H have non-isomorphic group algebras over the 2-adic integers $\mathbb{Z}_2$. Indeed, a Maranda-type theorem [19, (III.5.10)] shows that the same is true over the ring $\mathbb{Z}/2^k\mathbb{Z}$ for sufficiently large k. Sehgal [19, (III.5.11)] asked whether every isomorphism between modular group algebras lifts to an isomorphism between p-adic group algebras for finite p-groups (see also [11, Question 4.9] for Morita equivalences of blocks). The recent counterexamples answer this question in the negative. Hence there must be a minimal $k \geq 2$ such that the groups G and H have non-isomorphic group algebras over the ring $\mathbb{Z}/2^k\mathbb{Z}$, as the following diagram summarizes.

$$\begin{array}{ccccccccccc}
\mathbb{Z}/2\mathbb{Z}\,G & \twoheadleftarrow & \cdots & \twoheadleftarrow & \mathbb{Z}/2^{k-1}\mathbb{Z}\,G & \twoheadleftarrow & \mathbb{Z}/2^{k}\mathbb{Z}\,G & \twoheadleftarrow & \mathbb{Z}/2^{k+1}\mathbb{Z}\,G & \twoheadleftarrow & \cdots \qquad \mathbb{Z}_2\,G \\
\| & & & & \| & & \twoheadleftarrow & & \twoheadleftarrow & & \twoheadleftarrow \\
\mathbb{Z}/2\mathbb{Z}\,H & \twoheadleftarrow & \cdots & \twoheadleftarrow & \mathbb{Z}/2^{k-1}\mathbb{Z}\,H & \twoheadleftarrow & \mathbb{Z}/2^{k}\mathbb{Z}\,H & \twoheadleftarrow & \mathbb{Z}/2^{k+1}\mathbb{Z}\,H & \twoheadleftarrow & \cdots \qquad \mathbb{Z}_2\,H
\end{array}$$

In this paper, we prove that the groups G and H already have non-isomorphic group algebras over the ring $\mathbb{Z}/4\mathbb{Z}$. More generally, we prove the following.

Date: June 5, 2026.

2020 *Mathematics Subject Classification.* Primary 20C05; Secondary 16S34, 20D15, 16U60.

Key words and phrases. Isomorphism problem, group algebras, counterexamples, finite 2-groups, ground rings.

Theorem A. *Let R be a commutative ring with an ideal $\mathfrak{r}$. Suppose $n > m > \ell \geq 2$ and let*

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

If R has a maximal ideal $\mathfrak{m}$ such that $\mathfrak{m}^2 \subseteq \mathfrak{r} \subseteq \mathfrak{m}$ and $R/\mathfrak{r}$ has characteristic 4, then $RG \ncong RH$. On the other hand, if R has characteristic 2, then $RG \cong RH$.

The non-isomorphic groups G and H of order $2^{n+m+\ell}$ in the theorem are essentially[1] the only known counterexamples to the Modular Isomorphism Problem. Since our ground ring is no longer a field, we lay the groundwork for our analysis in Section 2. The theorem is proved in Section 3. Our proof is based on a group base approximation used in [13]. In Section 4 we study the rational and complex cases, which are not covered in Theorem A, and show that the situation is more delicate when 2 is a unit in the ground ring.

2. Preliminaries

We use standard group-theoretical notation. For a group G, we write its center as $Z(G)$, its derived subgroup as G' and its Frattini subgroup as $\Phi(G)$. The n-th term of the lower central series is denoted by $\gamma_n(G)$. For $g, h \in G$, their commutator is defined as $[g,h] = g^{-1}h^{-1}gh$ and conjugation is defined as $g^h = h^{-1}gh$. We write $|g|$ for the order and g^G for the conjugacy class of g in G. For a subgroup $K \leq G$, its centralizer and normalizer in G are denoted by $C_G(K)$ and $N_G(K)$, respectively. Let p be a prime and suppose that G is a finite p-group. For a normal subgroup $N \trianglelefteq G$, we define

$$\Omega(G : N) = \langle\, g \in G \mid g^p \in N \,\rangle.$$

For a non-negative integer k, we define $\Omega_k(G) = \langle\, g \in G \mid g^{p^k} = 1 \,\rangle$ and $G^{p^k} = \langle\, g^{p^k} \mid g \in G \,\rangle$. A cyclic group of order n is denoted by C_n.

For a commutative ring S and a finite group G, we write the center of the group algebra SG as $Z(SG)$. For $A, B \in SG$, their Lie commutator is defined as $[A,B] = AB - BA$. The augmentation ideal $\Delta(SG)$ of SG is defined to be the kernel of the map

$$\varepsilon_{SG} \colon SG \to S,\quad \sum_{g \in G} \alpha_g g \mapsto \sum_{g \in G} \alpha_g,$$

called the augmentation map.

For an ideal $\mathfrak{n}$ of S, we set $F = S/\mathfrak{n}$ and

$$\Delta(SG : \mathfrak{n}) = \{\, x \in SG \mid \varepsilon_{SG}(x) \in \mathfrak{n} \,\} = \mathfrak{n} \oplus \Delta(SG).$$

Let $\pi \colon S \to F$ be the natural projection and extend it to $\hat{\pi} \colon SG \to FG$ in the natural manner. Note that $\operatorname{Ker} \hat{\pi} = \mathfrak{n} \oplus \mathfrak{n}\Delta(SG)$.

In the rest of this section, we will prove some preparatory lemmas which will then serve to study the concrete groups in the next section. We start with a lemma, which is well known, but seems not to be contained in this short and general form in the literature.

Lemma 2.1. *Let R and S be commutative rings and G and H finite groups. Suppose that there is a ring homomorphism $R \to S$. If $RG \cong RH$, then $SG \cong SH$.*

[1] Taking the same power of these groups and taking the direct product with a common finite 2-group P also yields counterexamples for a trivial reason. So the only known counterexamples are of the form $G \times \cdots \times G \times P$ and $H \times \cdots \times H \times P$.

Proof. Let $\rho\colon R \to S$ be a ring homomorphism and $\varphi\colon RG \to RH$ an R-algebra isomorphism. For $g, h \in G$, take $\alpha_{g,h} \in R$ that satisfy $\varphi(g) = \sum_{h\in H} \alpha_{g,h} h$ and define $\psi\colon SG \to SH$ by $\psi(g) = \sum_{h\in H} \rho(\alpha_{g,h})h$. It is straightforward to check that ψ is indeed an S-algebra isomorphism whose inverse is defined similarly. □

Lemma 2.2. *Let S be a commutative ring with an ideal $\mathfrak{n}$ and G a finite group. Write $F = S/\mathfrak{n}$, $\pi\colon S \to F$ and $\hat{\pi}\colon SG \to FG$ as before. Then*

$$\Delta(SG) \cap \hat{\pi}^{-1}(\Delta(FG)^2) = \mathfrak{n}\Delta(SG) + \Delta(SG)^2.$$

Proof. It is easy to see that the right-hand side is contained in the left-hand side. To see the converse, take $A \in \Delta(SG) \cap \hat{\pi}^{-1}(\Delta(FG)^2)$. Then there are some $\alpha_{g,h} \in F$ such that

$$\hat{\pi}(A) = \sum_{g\in G} \sum_{h\in G} \alpha_{g,h}(g-1)(h-1).$$

Since π is surjective, there are some $\beta_{g,h} \in S$ such that $\pi(\beta_{g,h}) = \alpha_{g,h}$. Then

$$A - \sum_{g\in G} \sum_{h\in G} \beta_{g,h}(g-1)(h-1) \in \operatorname{Ker}\hat{\pi}.$$

It follows from $(g-1)(h-1) \in \Delta(SG)^2$ and $\operatorname{Ker}\hat{\pi} = \mathfrak{n} \oplus \mathfrak{n}\Delta(SG)$ that $A \in \mathfrak{n} \oplus (\mathfrak{n}\Delta(SG) + \Delta(SG)^2)$. Since $A \in \Delta(SG)$, we conclude that $A \in \mathfrak{n}\Delta(SG) + \Delta(SG)^2$. □

Proposition 2.3. *Let S be a commutative ring with an ideal $\mathfrak{n}$ and G a finite group. Write $F = S/\mathfrak{n}$. Then there is an isomorphism of F-modules*

$$\Delta(SG : \mathfrak{n})/\Delta(SG : \mathfrak{n})^2 \cong \mathfrak{n}/\mathfrak{n}^2 \oplus \Delta(FG)/\Delta(FG)^2.$$

Proof. Recall that $\Delta(SG : \mathfrak{n}) = \mathfrak{n} \oplus \Delta(SG)$. As

$$\frac{\Delta(SG : \mathfrak{n})}{\Delta(SG : \mathfrak{n})^2} = \frac{\mathfrak{n} \oplus \Delta(SG)}{\mathfrak{n}^2 \oplus (\mathfrak{n}\Delta(SG) + \Delta(SG)^2)} \cong \frac{\mathfrak{n}}{\mathfrak{n}^2} \oplus \frac{\Delta(SG)}{\mathfrak{n}\Delta(SG) + \Delta(SG)^2},$$

it suffices to prove that

$$\frac{\Delta(SG)}{\mathfrak{n}\Delta(SG) + \Delta(SG)^2} \cong \frac{\Delta(FG)}{\Delta(FG)^2}.$$

Consider the canonical map $\Delta(SG) \to \Delta(FG)/\Delta(FG)^2$. By Lemma 2.2, we see that the kernel of this map is $\mathfrak{n}\Delta(SG) + \Delta(SG)^2$, as expected. □

The n-th dimension subgroup of a group G with respect to a commutative ring S is the subgroup of G defined by

$$D_{n,S}(G) = \{\, g \in G \mid g - 1 \in \Delta(SG)^n \,\}.$$

When G is a finite p-group and S is a field of characteristic p, the following purely group-theoretical formula describing the dimension subgroups was observed by Jennings and reformulated by Lazard.

Proposition 2.4 ([15, Theorem 11.1.20])**.** *Let F be a field of positive characteristic p and G a finite p-group. Then $D_{n,F}(G) = \prod_{ip^j \geq n} \gamma_i(G)^{p^j}$. In particular,*

$$\Delta(FG)/\Delta(FG)^2 \cong F \otimes_{\mathbb{Z}/p\mathbb{Z}} G/\Phi(G)$$

as F-vector spaces and a basis of $\Delta(FG)/\Delta(FG)^2$ is given by representatives $g_1 - 1$, $\ldots$, $g_\ell - 1$ where $g_1, \ldots, g_\ell$ form a minimal generating set of G.

No compact formula of this kind is known for dimension subgroups in the general situation, although some information is available, see e.g. [14, 18].

Moreover, the following is useful for computations in Section 3.

Lemma 2.5. *Let S be a commutative ring, G a group and n a positive integer. Then $\gamma_n(G) \leq D_{n,S}(G)$.*

Proof. This follows from the fact that the series $D_{n,S}(G)$ is central [15, Exercise 11.2(i)]. □

The following easy observations will be very useful for calculations in group algebras over commutative rings of characteristic 4.

Lemma 2.6. *Let p be a prime, n a positive integer and $0 < i < p^n$. Then*

$$\nu\left(\binom{p^n}{i}\right) = (p-1)(n-\nu(i)),$$

where ν denotes the p-adic valuation.

Proof. Let $k = \nu(i)$ and expand i as

$$i = i_k p^k + i_{k+1}p^{k+1} + \cdots + i_{n-1}p^{n-1},$$

where $0 \leq i_k, i_{k+1}, \ldots, i_{n-1} < p$ and $i_k \neq 0$. Since

$$p^n - 1 = (p-1)(1 + p + \cdots + p^{n-1}) = p^k - 1 + (p-1)p^k + \cdots + (p-1)p^{n-1},$$

we obtain

$$p^n - i = (p - i_k)p^k + (p - 1 - i_{k+1})p^{k+1} + \cdots + (p - 1 - i_{n-1})p^{n-1}.$$

It follows from Kummer's theorem on binomial coefficients [10, p. 116] that

$$\begin{aligned}\nu\left(\binom{p^n}{i}\right) &= (i_k + i_{k+1} + \cdots + i_{n-1}) \\ &\quad + ((p - i_k) + (p - 1 - i_{k+1}) + \cdots + (p - 1 - i_{n-1})) - 1 \\ &= (p-1)(n-k).\end{aligned}$$

□

Lemma 2.7. *Let S be a commutative ring with $4S = 0$, G a group and $A, B \in SG$ two commuting elements. Then for each positive integer n we have*

$$(A+B)^{2^n} = A^{2^n} + B^{2^n} + 2A^{2^{n-1}}B^{2^{n-1}}.$$

In particular, for $g \in G$ we have

$$(g-1)^{2^n} = (g^{2^n} - 1) + 2(g^{2^{n-1}} - 1).$$

Proof. It is enough to show that $\binom{2^n}{0} = \binom{2^n}{2^n} \equiv 1 \mod 4$, $\binom{2^n}{2^{n-1}} \equiv 2 \mod 4$ and $\binom{2^n}{i} \equiv 0 \mod 4$ otherwise. Of course, $\binom{2^n}{0} = \binom{2^n}{2^n} = 1$. Let ν denote the 2-adic valuation. By Lemma 2.6 we have $\nu\left(\binom{2^n}{i}\right) = n - \nu(i)$ for every $0 < i < 2^n$. So $\binom{2^n}{i} \equiv 0 \mod 4$ for $i \neq 2^{n-1}$ and $\binom{2^n}{2^{n-1}} \equiv 2 \mod 4$. □

Lemma 2.8. *Let S be a commutative ring with an ideal $\mathfrak{n}$ and $4S = 0$. Let n be a positive integer and $C_{2^n} = \langle u \mid u^{2^n} = 1 \rangle$. Set $U = u - 1 \in SC_{2^n}$. Then for each non-negative integer k,*

$$\Delta(SC_{2^n} : \mathfrak{n})^k = \bigoplus_{0 \leq i < 2^{n-1}} \mathfrak{n}^{k-i}U^i \oplus \bigoplus_{2^{n-1} \leq i < 2^n} \left(\mathfrak{n}^{k-i} + 2\mathfrak{n}^{k-i-2^{n-1}}\right)U^i$$

where $\mathfrak{n}^j = S$ for $j \leq 0$.

Proof. Let Ξ_k denote the right-hand side of the equation. Set $\Theta = \Delta(SC_{2^n} : \mathfrak{n})$.

First, $\Theta^k \supseteq \mathfrak{n}^{k-i}U^i$ for $0 \leq i < 2^n$ is clear. As $4S = 0$, Lemma 2.7 shows that

$$U^{2^n} = u^{2^n} + 2u^{2^{n-1}} + 1 = 2U^{2^{n-1}}.$$

Hence $2U^{2^{n-1}} \in \Theta^{2^n}$ and $\Theta^k \supseteq 2\mathfrak{n}^{k-i-2^{n-1}}U^i$ for $2^{n-1} \leq i < 2^n$. Thus $\Theta^k \supseteq \Xi_k$.

Next, we show that $\Theta^k \subseteq \Xi_k$ by induction on $k \geq 0$. The base case $k = 0$ is evident. Let $A \in \Theta^k$ and $B \in \Theta$. By the inductive hypothesis, we can write

$$A = \sum_{0 \leq i < 2^{n-1}} \alpha_i U^i + \sum_{2^{n-1} \leq i < 2^n} (\alpha_i + 2\xi_i) U^i$$
$$B = \sum_{0 \leq i < 2^{n-1}} \beta_i U^i + \sum_{2^{n-1} \leq i < 2^n} (\beta_i + 2\eta_i) U^i$$

with some $\alpha_i \in \mathfrak{n}^{k-i}$, $\beta_i \in \mathfrak{n}^{1-i}$ for $0 \leq i < 2^n$ and $\xi_i \in \mathfrak{n}^{k-i-2^{n-1}}$, $\eta_i \in \mathfrak{n}^{1-i-2^{n-1}}$ for $2^{n-1} \leq i < 2^n$. Then

$$\begin{aligned} AB = &\sum_{\substack{0 \leq i < 2^n \\ i+j < 2^{n-1}+2^n}} \sum_{0 \leq j < 2^n} \alpha_i \beta_j U^{i+j} + \sum_{\substack{0 \leq i < 2^n \\ i+j \geq 2^{n-1}+2^n}} \sum_{0 \leq j < 2^n} \alpha_i \beta_j U^{i+j} \\ &+ \sum_{\substack{0 \leq i < 2^n \\ i+j < 2^n}} \sum_{2^{n-1} \leq j < 2^n} 2\alpha_i \eta_j U^{i+j} + \sum_{\substack{0 \leq i < 2^n \\ i+j \geq 2^n}} \sum_{2^{n-1} \leq j < 2^n} 2\alpha_i \eta_j U^{i+j} \\ &+ \sum_{\substack{2^{n-1} \leq i < 2^n \\ i+j < 2^n}} \sum_{0 \leq j < 2^n} 2\xi_i \beta_j U^{i+j} + \sum_{\substack{2^{n-1} \leq i < 2^n \\ i+j \geq 2^n}} \sum_{0 \leq j < 2^n} 2\xi_i \beta_j U^{i+j} \end{aligned}$$

with $\alpha_i \beta_j \in \mathfrak{n}^{k+1-(i+j)}$ and $\alpha_i \eta_j, \xi_i \beta_j \in \mathfrak{n}^{k+1-(i+j)-2^{n-1}}$. The fourth and sixth double sums vanish as $2U^{2^n} = 4U^{2^{n-1}} = 0$. The second double sum also vanishes as $U^{2^{n-1}+2^n} = 2U^{2^n} = 4U^{2^{n-1}} = 0$. Thus

$$\begin{aligned} AB = &\sum_{\substack{0 \leq i < 2^n \\ i+j < 2^n}} \sum_{0 \leq j < 2^n} \alpha_i \beta_j U^{i+j} + \sum_{\substack{0 \leq i < 2^n \\ 2^n \leq i+j < 2^{n-1}+2^n}} \sum_{0 \leq j < 2^n} \alpha_i \beta_j U^{i+j} \\ &+ \sum_{\substack{0 \leq i < 2^n \\ i+j < 2^n}} \sum_{2^{n-1} \leq j < 2^n} 2\alpha_i \eta_j U^{i+j} + \sum_{\substack{2^{n-1} \leq i < 2^n \\ i+j < 2^n}} \sum_{0 \leq j < 2^n} 2\xi_i \beta_j U^{i+j}. \end{aligned}$$

In the second double sum, each term can be rewritten as

$$\alpha_i \beta_j U^{i+j} = 2\alpha_i \beta_j U^{i+j-2^{n-1}}$$

and its coefficient satisfies

$$\alpha_i \beta_j \in \mathfrak{n}^{k+1-(i+j)} = \mathfrak{n}^{k+1-(i+j-2^{n-1})-2^{n-1}}.$$

Thus $AB \in \Xi_{k+1}$. □

The above equations agree with those that follow from Jennings' theory when S is a field of characteristic 2. The next example illustrates the previous lemma explicitly for the cyclic group of order 4.

Example 2.9. Let S be a commutative ring with an ideal $\mathfrak{n}$ and $4S = 0$. Let $C_4 = \langle u \mid u^4 = 1 \rangle$. Set $U = u - 1 \in SC_4$ and $\Theta = \Delta(SC_4 : \mathfrak{n})$. Then Lemma 2.8

shows the following.

$$\begin{aligned}
\Theta^0 &= S \ \oplus SU \ \oplus SU^2 \qquad\quad \oplus SU^3 \\
\Theta^1 &= \mathfrak{n} \ \oplus SU \ \oplus SU^2 \qquad\quad \oplus SU^3 \\
\Theta^2 &= \mathfrak{n}^2 \oplus \mathfrak{n}U \ \oplus SU^2 \qquad\quad \oplus SU^3 \\
\Theta^3 &= \mathfrak{n}^3 \oplus \mathfrak{n}^2U \oplus \mathfrak{n}U^2 \qquad\quad \oplus SU^3 \\
\Theta^4 &= \mathfrak{n}^4 \oplus \mathfrak{n}^3U \oplus (\mathfrak{n}^2+2S)U^2 \oplus \mathfrak{n}U^3 \\
\Theta^5 &= \mathfrak{n}^5 \oplus \mathfrak{n}^4U \oplus (\mathfrak{n}^3+2\mathfrak{n})U^2 \oplus (\mathfrak{n}^2+2S)U^3 \\
&\ \ \vdots
\end{aligned}$$

Accordingly, the successive quotients as $S/\mathfrak{n}$-modules are the following.

$$\begin{aligned}
\Theta^0/\Theta^1 &\cong S/\mathfrak{n} \\
\Theta^1/\Theta^2 &\cong \mathfrak{n}/\mathfrak{n}^2 \ \oplus S/\mathfrak{n} \\
\Theta^2/\Theta^3 &\cong \mathfrak{n}^2/\mathfrak{n}^3 \oplus \mathfrak{n}/\mathfrak{n}^2 \ \oplus S/\mathfrak{n} \\
\Theta^3/\Theta^4 &\cong \mathfrak{n}^3/\mathfrak{n}^4 \oplus \mathfrak{n}^2/\mathfrak{n}^3 \oplus \mathfrak{n}/(\mathfrak{n}^2+2S) \qquad \oplus S/\mathfrak{n} \\
\Theta^4/\Theta^5 &\cong \mathfrak{n}^4/\mathfrak{n}^5 \oplus \mathfrak{n}^3/\mathfrak{n}^4 \oplus (\mathfrak{n}^2+2S)/(\mathfrak{n}^3+2\mathfrak{n}) \oplus \mathfrak{n}/(\mathfrak{n}^2+2S) \\
&\ \ \vdots
\end{aligned}$$

Lemma 2.10. *Let S be a commutative ring with an ideal $\mathfrak{n}$ containing 2 and $4S = 0$. Let*

$$D_{16} = \langle\, u, v, w \mid u^2 = 1, v^2 = 1, w^4 = 1, [v,u] = w, [w,u] = w^2, [w,v] = w^2 \,\rangle$$

be the dihedral group of order 16. Set $U = u - 1, V = v - 1, W = w - 1 \in SD_{16}$. Moreover, let $\mathscr{B} = \{\, U^sV^tW^i \mid 0 \le s,t,i < 2 \,\}$ and define a function $\omega\colon \mathscr{B} \to \mathbb{Z}$ by

$$\omega(U^sV^tW^i) = s + t + 2i \qquad (0 \le s,t,i < 2).$$

Then for each non-negative integer k,

$$\Delta(SD_{16} : \mathfrak{n})^k = \bigoplus_{Q\in\mathscr{B}} \mathfrak{n}^{k-\omega(Q)}Q \oplus \bigoplus_{Q\in\mathscr{B}} \left(\mathfrak{n}^{k-4-\omega(Q)} + 2\mathfrak{n}^{k-8-\omega(Q)}\right) QW^2$$

where $\mathfrak{n}^j = S$ for $j \le 0$.

Proof. Let Ξ_k denote the right-hand side of the equation. Set $\Theta = \Delta(SD_{16} : \mathfrak{n})$. As an additional notation, set $z = w^2 = [w,u] = [w,v]$ and $Z = z - 1 \in SD_{16}$. Then, by Lemma 2.7, we have $W^2 = Z + 2W$. (Though this is not strictly necessary, we note that $Z \in \Theta^3$ by Lemma 2.5.)

We will argue by induction on k. Since every element of D_{16} can be written as $u^sv^tw^iz^j$ $(0 \le s,t,i,j < 2)$, the base case $k = 0$ is clear:

$$SD_{16} = \bigoplus_{Q\in\mathscr{B}} Q \oplus \bigoplus_{Q\in\mathscr{B}} QW^2.$$

So assume that the lemma holds for all non-negative integers at most k. Note that $U, V \in \Theta$, $UV, W \in \Theta^2$, $UW, VW \in \Theta^3$ and $UVW, W^2 \in \Theta^4$. Thus, it is clear that $\mathfrak{n}^{(k+1)-\omega(Q)}Q \subseteq \Theta^{k+1}$ and $\mathfrak{n}^{(k+1)-4-\omega(Q)}QW^2 \subseteq \Theta^{k+1}$ for each $Q \in \mathscr{B}$. Moreover, to see that $\Xi_{k+1} \subseteq \Theta^{k+1}$ we need to show that $2W^2 \in \Theta^8$. This follows, using $Z^2 = 2Z$ as $z^2 = 1$, from

$$(W^2)^2 = (Z + 2W)^2 = Z^2 = 2Z = 2(W^2 + 2W) = 2W^2,$$

as the first element of this equation is contained in Θ^8. Hence we establish $\Xi_{k+1} \subseteq \Theta^{k+1}$.

Also, we obtain that Θ/Θ^2 is generated by the images of $\mathfrak{n}$, U and V. Hence to show $\Theta^{k+1} \subseteq \Xi_{k+1}$ it is sufficient to show that for A a generic element in Θ^k all of $\mathfrak{n}A$, UA, VA are contained in Ξ_{k+1}.

Let, by the induction hypothesis,

$$A = \sum_{Q\in\mathscr{B}} \alpha_Q Q + \sum_{Q\in\mathscr{B}} (\beta_Q + 2\gamma_Q)\, QW^2$$

for $\alpha_Q \in \mathfrak{n}^{k-\omega(Q)}$, $\beta_Q \in \mathfrak{n}^{k-4-\omega(Q)}$ and $\gamma_Q \in \mathfrak{n}^{k-8-\omega(Q)}$ for all $Q \in \mathscr{B}$. Clearly, $\mathfrak{n}A \subseteq \Xi_{k+1}$. Next, using the equation $U^2 = 2U$, which holds as $u^2 = 1$ and $2 = -2$ in S, we obtain

$$U \sum_{Q\in\mathscr{B}} \alpha_Q Q = \sum_{0\le t,i<2} (\alpha_{V^tW^i} + 2\alpha_{UV^tW^i}) UV^tW^i$$

which is contained in Ξ_{k+1} as $2 \in \mathfrak{n}$ by assumption. For the same reasons

$$U \sum_{Q\in\mathscr{B}} \beta_Q QW^2 = \sum_{0\le t,i<2} (\beta_{V^tW^i} + 2\beta_{UV^tW^i}) UV^tW^iW^2,$$
$$U \sum_{Q\in\mathscr{B}} 2\gamma_Q QW^2 = \sum_{0\le t,i<2} 2\gamma_{V^tW^i} UV^tW^iW^2$$

and we get $U\sum_{Q\in\mathscr{B}} \beta_Q QW^2, U\sum_{Q\in\mathscr{B}} 2\gamma_Q QW^2 \in \Xi_{k+1}$, so that $UA \in \Xi_{k+1}$.

Next, consider VA. We have $V^2 = 2V$ as before. The calculations here are more evolved and we separate A according to the summands $Q \in \mathscr{B}$. When Q does not have U as a factor, a short computation yields the following.

$$V(\alpha_1 1 + (\beta_1 + 2\gamma_1)W^2) = \alpha_1 V + (\beta_1 + 2\gamma_1)VW^2,$$
$$V(\alpha_V V + (\beta_V + 2\gamma_V)VW^2) = 2\alpha_V V + 2\beta_V VW^2,$$
$$V(\alpha_W W + (\beta_W + 2\gamma_W)WW^2) = \alpha_W VW + (\beta_W + 2\gamma_W)VWW^2,$$
$$V(\alpha_{VW} VW + (\beta_{VW} + 2\gamma_{VW})VWW^2) = 2\alpha_{VW} VW + 2\beta_{VW} VWW^2.$$

When Q does have U as a factor, by elementary commutator formulas

$$VU = UV + (1 + U + V + UV)W, \qquad WV = VW + (1 + V + W + VW)Z$$

and the power formulas $Z^2 = 2Z$, $Z = W^2 + 2W$, a lengthy computation yields the following.

$$\begin{aligned}
&V(\alpha_U U + (\beta_U + 2\gamma_U)UW^2)\\
&\quad = \alpha_U(UV + W + UW + VW + UVW)\\
&\qquad + (\beta_U + 2\gamma_U)(UV + W + UW + VW + UVW)W^2,\\
&V(\alpha_{UV} UV + (\beta_{UV} + 2\gamma_{UV})UVW^2)\\
&\quad = 2\alpha_{UV}(UV + W + UW) - \alpha_{UV}(VW + UVW)\\
&\qquad - (\alpha_{UV} + 2\beta_{UV})(1 + U)W^2 + 2\beta_{UV} UVW^2\\
&\qquad + \alpha_{UV}(W + UW)W^2 - (\beta_{UV} + 2\gamma_{UV})(VW + UVW)W^2,\\
&V(\alpha_{UW} UW + (\beta_{UW} + 2\gamma_{UW})UWW^2)\\
&\quad = \alpha_{UW} UVW + (\alpha_{UW} + 2\beta_{UW})(1 + U + V + UV)W^2\\
&\qquad + (\beta_{UW} + 2\gamma_{UW})UVWW^2,\\
&V(\alpha_{UVW} UVW + (\beta_{UVW} + 2\gamma_{UVW})UVWW^2)\\
&\quad = 2\alpha_{UVW} UVW - (\alpha_{UVW} + 2\beta_{UVW})(V + UV + W + UW)W^2\\
&\qquad + 2\beta_{UVW} UVWW^2.
\end{aligned}$$

From these formulas, we conclude that $VA \in \Xi_{k+1}$.

Overall $\Theta^{k+1} = \Xi_{k+1}$. □

3. Proof of main theorem

This section is devoted to proving Theorem A. Throughout this section, we assume that $n > m > \ell \geq 2$ and G and H are the groups of order $2^{n+m+\ell}$ defined as

$$G = \langle\, x, y, z \mid x^{2^n} = 1,\ y^{2^m} = 1,\quad z^{2^\ell} = 1,\ [y,x] = z,\ [z,x] = z^{-2},\ [z,y] = z^{-2} \,\rangle,$$

$$H = \langle\, a, b, c \mid a^{2^n} = 1,\ b^{2^m} = a^{2^m},\ c^{2^\ell} = 1,\ [b,a] = c,\ [c,a] = c^{-2},\ [c,b] = c^{-2} \,\rangle,$$

which are counterexamples to the Modular Isomorphism Problem. At the time of writing, these groups are essentially the only known examples. We fix not only the groups G and H but also the generators x, y, z and a, b, c that are used in their presentations.

Moreover, we fix a commutative ring R with an ideal $\mathfrak{r}$ and a maximal ideal $\mathfrak{m}$ such that $\mathfrak{m}^2 \subseteq \mathfrak{r} \subseteq \mathfrak{m}$ and $R/\mathfrak{r}$ has characteristic 4. By Lemma 2.1, it suffices to work over a quotient ring $S = R/\mathfrak{r}$ to prove Theorem A. We fix the commutative ring S of characteristic 4 for the rest of this section. Let $\mathfrak{n} = \mathfrak{m}/\mathfrak{r}$ and observe that it is a maximal ideal of S with $2 \in \mathfrak{n}$ and $2 \notin \mathfrak{n}^2$.

Set $\Theta = \Delta(SH : \mathfrak{n}) = \mathfrak{n} \oplus \Delta(SH)$. Note that the successive quotients Θ/Θ^2, Θ^2/Θ^3, ... have the canonical vector space structure over the residue field $F = S/\mathfrak{n}$, as $\mathfrak{n}\Theta^k \subseteq \Theta^{k+1}$ for each non-negative integer k. We write $A = a - 1$, $B = b - 1$, $C = c - 1 \in SH$ and α, β for scalars in F.

Hypothesis 3.1. For the convenience of the readers, we summarize the common assumptions that will be used throughout.

- $n > m > \ell \geq 2$.
- The groups $G = \langle x, y, z\rangle$, $H = \langle a, b, c\rangle$ are defined as above.
- The commutative ring S has characteristic 4.
- The maximal ideal $\mathfrak{n}$ of S satisfies $2 \in \mathfrak{n}$ and $2 \notin \mathfrak{n}^2$.
- $\Theta = \Delta(SH : \mathfrak{n}) \subseteq SH$.
- $A = a - 1$, $B = b - 1$, $C = c - 1 \in SH$.
- $\alpha, \beta \in F = S/\mathfrak{n}$.

We will prove the following after several preliminary observations.

Proposition 3.2. *Under Hypothesis 3.1, $SG \ncong SH$.*

We first record some elementary facts about the groups G and H.

Lemma 3.3. *Under Hypothesis 3.1, $x^2, y^2 \in Z(G)$ and $a^2, b^2 \in Z(H)$.*

Lemma 3.4. *Under Hypothesis 3.1, $\Theta/\Theta^2 \cong \mathfrak{n}/\mathfrak{n}^2 \oplus FA \oplus FB$.*

Proof. This follows from Propositions 2.3 and 2.4. □

First, we need to know how to approximate powers and commutators.

Lemma 3.5. *Under Hypothesis 3.1, $[B, A] \equiv C \mod \Theta^3$.*

Proof. Note that $[B, A] = (1 + A + B + AB)C$. Lemma 2.5 shows that $C \in \Theta^2$, and the lemma follows. □

Lemma 3.6. *Under Hypothesis 3.1, $(\alpha A + \beta B)^2 \equiv \alpha^2 A^2 + \beta^2 B^2 + \alpha\beta C \mod \Theta^3$.*

Proof.

$$\begin{aligned}(\alpha A + \beta B)^2 &\equiv \alpha^2 A^2 + \beta^2 B^2 + \alpha\beta[B, A] \mod \Theta^3 && \text{(by } 2AB \in \Theta^3\text{)}\\ &\equiv \alpha^2 A^2 + \beta^2 B^2 + \alpha\beta C \mod \Theta^3 && \text{(by Lemma 3.5).}\end{aligned}$$

□

Lemma 3.7. *Under Hypothesis 3.1,* $[C, A] \equiv [C, B] \equiv 2C \mod \Theta^4$.

Proof. Because the same proof works for B, we give the proof only for A. Set $d = [c, a]$ and $D = d - 1 \in SH$. Since $C \in \Theta^2$ and $D \in \Theta^3$ by Lemma 2.5,

$$\begin{aligned}
[C, A] &= (1 + A + C + AC)D \equiv D && (\text{by } D \in \Theta^3)\\
&= (1 + C)^{-2} - 1 && (\text{by } d = c^{-2})\\
&= (1 - 2C + 3C^2 - \cdots) - 1 \equiv 2C \mod \Theta^4 && (\text{by } C \in \Theta^2). \qquad \square
\end{aligned}$$

Lemma 3.8. *Under Hypothesis 3.1,* $A^2 \equiv 2A$ *and* $B^2 \equiv 2B \mod Z(SH)$.

Proof. Note that $A^2 + 2A = a^2 - 1$ and $B^2 + 2B = b^2 - 1$. Since a^2 and b^2 are central in H by Lemma 3.3, $A^2 + 2A$ and $B^2 + 2B$ are central in SH. $\square$

Lemma 3.9. *Under Hypothesis 3.1,*

$$(\alpha A + \beta B)^4 \equiv \alpha^4 A^4 + \beta^4 B^4 + \alpha^2\beta^2 C^2 \mod \Theta^5.$$

Proof. Recall that $C \in \Theta^2$ by Lemma 2.5. First Lemma 3.6 shows that

$$(\alpha A + \beta B)^4 \equiv (\alpha^2 A^2 + \beta^2 B^2 + \alpha\beta C)^2 \mod \Theta^5$$

and, in the same way, we get

$$\begin{aligned}
(\alpha A + \beta B)^4 \equiv{}& \alpha^4 A^4 + \beta^4 B^4 + \alpha^2\beta^2 C^2\\
&+ \alpha^2\beta^2[B^2, A^2] + \alpha^3\beta[C, A^2] + \alpha\beta^3[C, B^2] \mod \Theta^5.
\end{aligned}$$

Applying Lemma 3.8 yields

$$(\alpha A + \beta B)^4 \equiv \alpha^4 A^4 + \beta^4 B^4 + \alpha^2\beta^2 C^2 + 2\alpha^3\beta[C, A] + 2\alpha\beta^3[C, B] \mod \Theta^5$$

and, by Lemma 3.7, we conclude that

$$(\alpha A + \beta B)^4 \equiv \alpha^4 A^4 + \beta^4 B^4 + \alpha^2\beta^2 C^2 \mod \Theta^5. \qquad \square$$

Lemma 3.10. *Under Hypothesis 3.1,*

$$(\alpha A + \beta B)^{2^{m+1}} \equiv (\alpha + \beta)^{2^{m+1}} A^{2^{m+1}} \mod \Theta^{1+2^{m+1}}.$$

Proof. First applying Lemma 3.9 yields

$$(\alpha A + \beta B)^{2^{m+1}} \equiv (\alpha^4 A^4 + \beta^4 B^4 + \alpha^2\beta^2 C^2)^{2^{m-1}} \mod \Theta^{1+2^{m+1}}.$$

To compute this further, observe that A^4 is central in SH as $A^4 = a^4 + 2a^2 + 1$ and a^2 is central in H by Lemma 3.3. The same is true for B^4 as well. Hence it follows from Lemma 2.7 that

$$(\alpha A + \beta B)^{2^{m+1}} \equiv \alpha^{2^{m+1}} A^{2^{m+1}} + \beta^{2^{m+1}} B^{2^{m+1}} + \alpha^{2^m}\beta^{2^m} C^{2^m} \mod \Theta^{1+2^{m+1}},$$

where we used $2A^{2^m} B^{2^m} \equiv 2A^{2^m} C^{2^{m-1}} \equiv 2B^{2^m} C^{2^{m-1}} \equiv 0$ here, which also follows using Lemma 2.7. Now $a^{2^m} = b^{2^m}$ and Lemma 2.7 show that

$$A^{2^{m+1}} = (a^{2^{m+1}} - 1) - 2(a^{2^m} - 1) = (b^{2^{m+1}} - 1) - 2(b^{2^m} - 1) = B^{2^{m+1}}.$$

Similarly, $m > \ell$, $c^{2^\ell} = 1$ and Lemma 2.7 show that

$$C^{2^m} = (c^{2^m} - 1) - 2(c^{2^{m-1}} - 1) = 0.$$

Combining these, we conclude that

$$\begin{aligned}
(\alpha A + \beta B)^{2^{m+1}} &\equiv (\alpha^{2^{m+1}} + \beta^{2^{m+1}}) A^{2^{m+1}}\\
&\equiv (\alpha^{2^{m+1}} + 2\alpha^{2^m}\beta^{2^m} + \beta^{2^{m+1}}) A^{2^{m+1}} && (\text{by } 2A^{2^{m+1}} \equiv 0)\\
&\equiv (\alpha + \beta)^{2^{m+1}} A^{2^{m+1}} \mod \Theta^{1+2^{m+1}} && (\text{by Lemma 2.7}). \qquad \square
\end{aligned}$$

Lemma 3.11. *Under Hypothesis 3.1,* $A^{2^{m+1}} \not\equiv 0 \mod \Theta^{1+2^{m+1}}$.

Proof. The basic idea of the proof is reducing the problem to the cyclic case. Consider the normal subgroup $N = \langle a^{2^{m+1}}, a^{-1}b, c\rangle$ of H and let $K = \langle\, u \mid u^{2^{m+1}} = 1\,\rangle$. Set $U = u - 1 \in SK$. Since $H/N \cong K$ and $SH/\Delta(SN)SH \cong SK$ by $n > m$, we have a surjective homomorphism $SH \to SK$ defined by $A \mapsto U$. As this homomorphism maps $\Delta(SH : \mathfrak{n})$ onto $\Delta(SK : \mathfrak{n})$, it suffices to prove that

$$U^{2^{m+1}} \not\equiv 0 \mod \Delta(SK : \mathfrak{n})^{1+2^{m+1}}.$$

The coefficients of U^{2^m} in the direct sum decomposition of $\Delta(SK : \mathfrak{n})^{1+2^{m+1}}$ in Lemma 2.8 are elements of $(\mathfrak{n}^{1+2^m} + 2\mathfrak{n})$. By Lemma 2.7, we have $U^{2^{m+1}} = 2U^{2^m}$ and as $2 \in \mathfrak{n}$ and $2 \notin \mathfrak{n}^2$, we get $2U^{2^m} \notin (\mathfrak{n}^{1+2^m} + 2\mathfrak{n})U^{2^m}$. Hence, $U^{2^{m+1}} \not\equiv 0 \mod \Delta(SK : \mathfrak{n})^{1+2^{m+1}}$. □

Lemma 3.12. *Under Hypothesis 3.1,* $2C \not\equiv 0 \mod \Theta^4$.

Proof. The basic idea of the proof is reducing the problem to the dihedral case. Consider the normal subgroup $N = \langle a^2, b^2, c^4\rangle$ of H and let

$$K = \langle\, u, v, w \mid u^2 = 1,\ v^2 = 1,\ w^4 = 1,\ [v,u] = w,\ [w,u] = w^2,\ [w,v] = w^2\,\rangle.$$

Set $U = u-1, V = v-1, W = w-1 \in SK$. Since $H/N \cong K$ and $SH/\Delta(SN)SH \cong SK$, we have a surjective homomorphism $SH \to SK$ defined by $A \mapsto U$, $B \mapsto V$ and $C \mapsto W$. As this homomorphism maps $\Delta(SH : \mathfrak{n})$ onto $\Delta(SK : \mathfrak{n})$, it suffices to prove that

$$2W \not\equiv 0 \mod \Delta(SK : \mathfrak{n})^4.$$

By Lemma 2.10 and $2W \notin \mathfrak{n}^2W$ as $2 \notin \mathfrak{n}^2$, we get $2W \not\equiv 0 \mod \Delta(SK : \mathfrak{n})^4$. □

Proof of Proposition 3.2. Suppose that there exists an algebra isomorphism $SG \to SH$ to obtain a contradiction. Then we may construct a normalized isomorphism $\psi\colon SG \to SH$ from this by [16, p. 193]. In particular, it is compatible with the augmentation ideals. Set $Y = y - 1 \in SG$. By Lemma 3.4, there are unique scalars α, β of F such that

$$\psi(Y) \equiv \alpha A + \beta B \mod \Theta^2.$$

Note that no elements corresponding to $\mathfrak{n}/\mathfrak{n}^2$ are needed in these approximations as ψ is normalized. Since ψ is an isomorphism of S-algebra and $Y \notin \Delta(SG : \mathfrak{n})^2$ by Lemma 3.4, we have $(\alpha, \beta) \neq (0, 0)$. For the rest of the proof, we turn to showing the contrary.

Recall the power relation $y^{2^m} = 1$ in G. Then $Y^{2^{m+1}} = 0$ by Lemma 2.7 and

$$0 \equiv \psi(Y)^{2^{m+1}} \equiv (\alpha + \beta)^{2^{m+1}} A^{2^{m+1}} \mod \Theta^{1+2^{m+1}} \tag{3.1}$$

by Lemma 3.10. Also recall that y^2 is central in G by Lemma 3.3. Then $Y^2 + 2Y = y^2 - 1$ is central in SG. As ψ is an isomorphism, $\psi(Y)^2 + 2\psi(Y)$ must be central in SH. In particular, it must commute with A and B. By Lemma 3.6,

$$\psi(Y)^2 + 2\psi(Y) \equiv \alpha^2A^2 + \beta^2B^2 + \alpha\beta C + 2\alpha A + 2\beta B \mod \Theta^3.$$

So by Lemma 3.8,

$$\psi(Y)^2 + 2\psi(Y) \equiv 2(\alpha + \alpha^2)A + 2(\beta + \beta^2)B + \alpha\beta C \mod Z(SH) + \Theta^3.$$

Then it follows from Lemmas 3.5 and 3.7 that

$$0 \equiv [\psi(Y)^2 + 2\psi(Y), A] \equiv 2(\beta + \beta^2 + \alpha\beta)C \mod \Theta^4, \tag{3.2}$$

$$0 \equiv [\psi(Y)^2 + 2\psi(Y), B] \equiv 2(\alpha + \alpha^2 + \alpha\beta)C \mod \Theta^4. \tag{3.3}$$

From formulas (3.1), (3.2) and (3.3) we get

$$\begin{cases} \alpha+\beta=0 \\ \beta+\beta^2+\alpha\beta=0 \\ \alpha+\alpha^2+\alpha\beta=0 \end{cases}$$

by Lemmas 3.11 and 3.12. This gives $(\alpha,\beta)=(0,0)$ and shows that $SG \ncong SH$. □

Proof of Theorem A. From the assumptions, the quotient ring $S=R/\mathfrak{r}$ has characteristic 4 and $\mathfrak{n}=\mathfrak{m}/\mathfrak{r}$ is a maximal ideal of S with $2\in\mathfrak{n}$ and $2\notin\mathfrak{n}^2$. By Proposition 3.2, $SG\ncong SH$. Hence, $RG\ncong RH$ by Lemma 2.1.

On the other hand, if R has characteristic 2, then the proof of [13, Theorem 3.1] carries over verbatim just replacing the field in the proof by the ring R which shows $RG\cong RH$ in this case. □

4. Rational and complex group algebras

Theorem A shows that $RG\cong RH$ when R has characteristic 2. It also shows that $RG\ncong RH$ in many cases[2] when the characteristic of R is divisible by 4. When 2 is a unit in R, the situation is more delicate as the following shows (cf. [12, Corollary 8.2]).

Proposition 4.1. *Let G and H be the groups defined in Theorem A. Then $\mathbb{C}G\cong\mathbb{C}H$, but $\mathbb{Q}G\ncong\mathbb{Q}H$.*

A proof will be given after a series of lemmas. Let ν denote the 2-adic valuation on the integers and let ϕ denote Euler's totient function. We write $\mathscr{C}(\Gamma)$ for the set of conjugacy classes of cyclic subgroups of a finite group Γ. Then

$$|\mathscr{C}(\Gamma)|=\sum_{g\in\Gamma}\frac{1}{|\Gamma:N_\Gamma(\langle g\rangle)|}\times\frac{1}{\phi(|g|)}$$

as $|\Gamma:N_\Gamma(\langle g\rangle)|$ equals the number of conjugates of $\langle g\rangle$ and $\phi(|g|)$ equals the number of generators of $\langle g\rangle$. The following closed formula for the number of cyclic subgroups of a finite abelian p-group will be useful for us.

Lemma 4.2. *Let p be a prime and $n\ge m\ge\ell\ge 0$ integers. Then*

$$\begin{aligned}&|\mathscr{C}(C_{p^n}\times C_{p^m}\times C_{p^\ell})|\\ &\quad=(n-m)p^{m+\ell}+(p^{2\ell+1}+p^{2\ell})\frac{p^{m-\ell}-1}{p-1}+(p^2+p+1)\frac{p^{2\ell}-1}{p^2-1}+1.\end{aligned}$$

Proof. There are many known formulas to calculate the number of cyclic subgroups of a finite abelian group and we will use the one given in [20, Theorem 1]. In our case it reads

$$|\mathscr{C}(C_{p^n}\times C_{p^m}\times C_{p^\ell})|=\sum_{\substack{0\le i\le n\\0\le j\le m\\0\le k\le\ell}}\frac{\phi(p^i)\phi(p^j)\phi(p^k)}{\phi(\operatorname{lcm}(p^i,p^j,p^k))}.$$

To get the closed formula, we derive three difference equations first.

$$\begin{cases} |\mathscr{C}(C_{p^{n+1}}\times C_{p^m}\times C_{p^\ell})|-|\mathscr{C}(C_{p^n}\times C_{p^m}\times C_{p^\ell})|=p^{m+\ell}, \\ |\mathscr{C}(C_{p^{m+1}}\times C_{p^{m+1}}\times C_{p^\ell})|-|\mathscr{C}(C_{p^m}\times C_{p^m}\times C_{p^\ell})|=p^{m+\ell+1}+p^{m+\ell}, \\ |\mathscr{C}(C_{p^{\ell+1}}\times C_{p^{\ell+1}}\times C_{p^{\ell+1}})|-|\mathscr{C}(C_{p^\ell}\times C_{p^\ell}\times C_{p^\ell})|=p^{2\ell+2}+p^{2\ell+1}+p^{2\ell}. \end{cases}$$

[2]Note that the ring $\mathbb{Z}[T]/(4,T^2-2)$ is excluded from Theorem A, for instance.

We only show the second one in detail as similar arguments show the rest as well. Recall that $\phi(p^{m+1}) = p^{m+1} - p^m$ and $\sum_{0\le k\le \ell} \phi(p^k) = p^\ell$. Then

$$\begin{aligned}
&|\mathscr{C}(C_{p^{m+1}} \times C_{p^{m+1}} \times C_{p^\ell})| - |\mathscr{C}(C_{p^m} \times C_{p^m} \times C_{p^\ell})| \\
&\quad = \sum_{\substack{0\le j\le m \\ 0\le k\le \ell}} \phi(p^j)\phi(p^k) + \sum_{\substack{0\le i\le m \\ 0\le k\le \ell}} \phi(p^i)\phi(p^k) - \phi(p^{m+1}) \sum_{0\le k\le \ell} \phi(p^k) \\
&\quad = p^{m+\ell} + p^{m+\ell} - (p^{m+1} - p^m)p^\ell \\
&\quad = p^{m+\ell+1} + p^{m+\ell}.
\end{aligned}$$

From these difference equations, we obtain

$$\begin{aligned}
&|\mathscr{C}(C_{p^n} \times C_{p^m} \times C_{p^\ell})| \\
&\quad = (n-m)p^{m+\ell} + |\mathscr{C}(C_{p^m} \times C_{p^m} \times C_{p^\ell})| \\
&\quad = (n-m)p^{m+\ell} + (p^{2\ell+1} + p^{2\ell})\frac{p^{m-\ell} - 1}{p-1} + |\mathscr{C}(C_{p^\ell} \times C_{p^\ell} \times C_{p^\ell})| \\
&\quad = (n-m)p^{m+\ell} + (p^{2\ell+1} + p^{2\ell})\frac{p^{m-\ell} - 1}{p-1} + (p^2+p+1)\frac{p^{2\ell} - 1}{p^2-1} + 1.
\end{aligned}$$

□

Lemma 4.3. *Let Γ be the group G or H defined in Theorem A and K a cyclic subgroup of $C_\Gamma(\Gamma')$. Then*

$$K \trianglelefteq \Gamma \iff K \le Z(\Gamma) \text{ or } K \le \Omega(\Gamma : \Gamma').$$

Proof. Set $\alpha = x$, $\beta = y$ and $\gamma = z$, if $\Gamma = G$, and $\alpha = a$, $\beta = b$ and $\gamma = c$, if $\Gamma = H$. Observe that $C_\Gamma(\Gamma')$ is a maximal and abelian subgroup of Γ generated by $\alpha\beta$, α^2, β^2 and γ. Set $\delta = y^2$, if $\Gamma = G$, and $\delta = a^2$, if $\Gamma = H$. Then

$$C_\Gamma(\Gamma') = \langle \alpha^{-1}\beta \rangle \times \langle \delta \rangle \times \langle \gamma \rangle.$$

Moreover, $\Omega(\Gamma : \Gamma')$ is generated by γ and the socle of $\langle \alpha^{-1}\beta, \delta \rangle$ which is also central in Γ. Hence, the second condition implies the first. So we assume $K \trianglelefteq \Gamma$ and $K \not\le Z(\Gamma)$ and prove $K \le \Omega(\Gamma : \Gamma')$.

Let g be a generator of K and write it as

$$g = (\alpha^{-1}\beta)^i \delta^j \gamma^k \qquad (0 \le i < |\alpha^{-1}\beta|,\ 0 \le j < |\delta|,\ 0 \le k < |\gamma|).$$

The first assumption $K \trianglelefteq \Gamma$ implies $K^\alpha = K$. As $g^\alpha = g[g, \alpha]$, there is an integer $t \ge 0$ such that $[g, \alpha] = g^t$. Since $[g, \alpha] = \gamma^{i-2k}$, we obtain

$$(\alpha^{-1}\beta)^{it} = 1, \quad \delta^{jt} = 1, \quad \gamma^{kt} = \gamma^{i-2k}$$

and accordingly

$$\nu(it) \ge \nu(|\alpha^{-1}\beta|), \quad \nu(jt) \ge \nu(|\delta|), \quad \nu(kt - i + 2k) \ge \nu(|\gamma|). \tag{4.1}$$

The second assumption $K \not\le Z(\Gamma)$ implies $[g, \alpha] \ne 1$ as $\Gamma = \langle \alpha, C_\Gamma(\Gamma') \rangle$. So $\gamma^{kt} \ne 1$ and

$$\nu(|\gamma|) > \nu(kt). \tag{4.2}$$

From (4.2), the first of (4.1) and $|\alpha^{-1}\beta| > |\gamma|$, we obtain $\nu(i) \ge \nu(|\alpha^{-1}\beta|) - \nu(t) > \nu(|\gamma|) - \nu(t) \ge \nu(2k)$, which implies $\nu(i - 2k) = \nu(2k)$. From (4.2) and the third of (4.1), we also obtain $\nu(kt - i + 2k) > \nu(kt)$, which implies $\nu(i - 2k) = \nu(kt - kt + i - 2k) = \nu(kt)$. These yield $\nu(2k) = \nu(kt)$, and hence $\nu(t) = 1$. Thus $\langle g^2 \rangle = \langle g^t \rangle = \langle [g, \alpha] \rangle$ and $K \le \Omega(\Gamma : \Gamma')$. □

Lemma 4.4. *Let G and H be the groups defined in Theorem A. Then*

$$|\mathscr{C}(H)| - |\mathscr{C}(G)| = (n-m)2^{m-1}(2^{\ell-1} - 1).$$

Proof. We start the calculation, first for G. For better overview, we record the conjugation action:

$$y^x = yz,\ x^y = xz^{-1},\ z^x = z^y = z^{-1},\ x^z = xz^2,\ y^z = yz^2.$$

Inside maximal abelian subgroup of G. We first consider the elements in the maximal subgroup which is also abelian

$$C_G(G') = \langle xy\rangle \times \langle y^2\rangle \times \langle z\rangle \cong C_{2^n} \times C_{2^{m-1}} \times C_{2^\ell}.$$

Every element in $C_G(G')$ has either class length 1, when it lies in the center $Z(G)$, or 2, as then the centralizer equals $C_G(G')$. By Lemma 4.3, we can count the number of conjugacy classes of cyclic subgroups of G lying in $C_G(G')$ using the inclusion-exclusion principle as

$$\begin{aligned}
&\sum_{g\in C_G(G')} \frac{1}{|G : N_G(\langle g\rangle)|} \times \frac{1}{\phi(|g|)} \\
&\quad= \sum_{g\in Z(G)\cup\Omega(G:G')} \frac{1}{\phi(|g|)} + \frac{1}{2} \sum_{g\in C_G(G')\setminus(Z(G)\cup\Omega(G:G'))} \frac{1}{\phi(|g|)} \\
&\quad= \frac{1}{2}\big(|\mathscr{C}(C_G(G'))| + |\mathscr{C}(Z(G))| + |\mathscr{C}(\Omega(G:G'))|\big) \\
&\qquad - \frac{1}{2}\big(|\mathscr{C}(\Omega(G:G')\cap Z(G))|\big).
\end{aligned} \tag{4.3}$$

Outside maximal abelian subgroup of G. The elements of $G \setminus C_G(G') = x\Phi(G) \sqcup y\Phi(G)$ are of the form

$$x(x^2)^i(y^2)^j z^k \quad \text{or} \quad y(x^2)^i(y^2)^j z^k \qquad (0 \le i < 2^{n-1},\ 0 \le j < 2^{m-1},\ 0 \le k < 2^\ell).$$

Such an element g satisfies $g^{yx} = gz$ which implies $g^G = gG'$. It also satisfies $z^{2^{\ell-1}} \notin \langle g\rangle$, so $G' \cap \langle g\rangle = 1$ and thus $N_G(\langle g\rangle) = C_G(g)$. For the elements of $x\Phi(G)$, note that they have the common order 2^n. So the contribution is

$$\sum_{g\in x\Phi(G)} \frac{1}{|G : N_G(\langle g\rangle)|} \times \frac{1}{\phi(|g|)} = \frac{|x\Phi(G)|}{|G'| \times |(\mathbb{Z}/2^n\mathbb{Z})^\times|} = \frac{2^{n-1} \times 2^{m-1} \times 2^\ell}{2^\ell \times 2^{n-1}} = 2^{m-1}.$$

For the elements of $y\Phi(G)$, the calculation is more delicate because their orders vary. Consider a chain of sets

$$y\Omega_m(\Phi(G)) \subseteq y\Omega_{m+1}(\Phi(G)) \subseteq \cdots \subseteq y\Omega_{n-1}(\Phi(G)) = y\Phi(G)$$

and observe that an element $g \in y\Omega_t(\Phi(G)) \setminus y\Omega_{t-1}(\Phi(G))$ has order 2^t for each $m+1 \le t \le n-1$. Also an element $g \in y\Omega_m(\Phi(G))$ has order 2^m. So the

contribution is

$$\begin{aligned}
&\sum_{g\in y\Phi(G)} \frac{1}{|G:N_G(\langle g\rangle)|}\times\frac{1}{\phi(|g|)}\\
&\quad=\sum_{g\in y\Omega_m(\Phi(G))} \frac{1}{|G:N_G(\langle g\rangle)|}\times\frac{1}{\phi(|g|)}\\
&\qquad+\sum_{t=m+1}^{n-1}\sum_{g\in y\Omega_t(\Phi(G))\setminus y\Omega_{t-1}(\Phi(G))} \frac{1}{|G:N_G(\langle g\rangle)|}\times\frac{1}{\phi(|g|)}\\
&\quad=\frac{|y\Omega_m(\Phi(G))|}{|G'|\times|(\mathbb{Z}/2^m\mathbb{Z})^\times|}+\sum_{t=m+1}^{n-1}\frac{|y\Omega_t(\Phi(G))\setminus y\Omega_{t-1}(\Phi(G))|}{|G'|\times|(\mathbb{Z}/2^t\mathbb{Z})^\times|}\\
&\quad=\frac{2^m\times 2^{m-1}\times 2^\ell}{2^\ell\times 2^{m-1}}+\sum_{t=m+1}^{n-1}\frac{2^{t-1}\times 2^{m-1}\times 2^\ell}{2^\ell\times 2^{t-1}}\\
&\quad=2^m+(n-m-1)2^{m-1}.
\end{aligned}$$

The overall contribution of $G\setminus C_G(G')$ to $|\mathscr{C}(G)|$ is

$$\begin{aligned}
&\sum_{g\in G\setminus C_G(G')} \frac{1}{|G:N_G(\langle g\rangle)|}\times\frac{1}{\phi(|g|)}\\
&\quad=\sum_{g\in x\Phi(G)} \frac{1}{|G:N_G(\langle g\rangle)|}\times\frac{1}{\phi(|g|)}+\sum_{g\in y\Phi(G)} \frac{1}{|G:N_G(\langle g\rangle)|}\times\frac{1}{\phi(|g|)}\\
&\quad=2^m+(n-m)2^{m-1}.
\end{aligned}\tag{4.4}$$

For the calculation in H, we also record the conjugacy action, which is essentially the same as for G:

$$b^a=bc,\ a^b=ac^{-1},\ c^a=c^b=c^{-1},\ a^c=ac^2,\ b^c=bc^2.$$

Inside maximal abelian subgroup of H. The arguments are very similar to the case of the maximal abelian subgroup of G, so we make them shorter. First note that

$$C_H(H')=\langle a^2\rangle\times\langle a^{-1}b\rangle\times\langle c\rangle\cong C_{2^{n-1}}\times C_{2^m}\times C_{2^\ell}$$

is a maximal subgroup of H which is abelian. The class length of an element in $C_H(H')$ is 1, if it is central in H, and 2 otherwise. By Lemma 4.3, again by the inclusion-exclusion principle, we obtain the contribution of $C_H(H')$ to $|\mathscr{C}(H)|$ as

$$\begin{aligned}
&\sum_{h\in C_H(H')} \frac{1}{|H:N_H(\langle h\rangle)|}\times\frac{1}{\phi(|h|)}\\
&\quad=\sum_{h\in Z(H)\cup\Omega(H:H')} \frac{1}{\phi(|h|)}+\frac{1}{2}\sum_{h\in C_H(H')\setminus(Z(H)\cup\Omega(H:H'))}\frac{1}{\phi(|h|)}\\
&\quad=\frac{1}{2}\big(|\mathscr{C}(C_H(H'))|+|\mathscr{C}(Z(H))|+|\mathscr{C}(\Omega(H:H'))|\big)\\
&\qquad-\frac{1}{2}\big(|\mathscr{C}(\Omega(H:H')\cap Z(H))|\big).
\end{aligned}\tag{4.5}$$

Outside maximal abelian subgroup of H. The elements in $H\setminus C_H(H')=aC_H(H')$ are of the form

$$a(a^2)^i(a^{-1}b)^jc^k\qquad(0\le i<2^{n-1},\ 0\le j<2^m,\ 0\le k<2^\ell).$$

Such an element h satisfies $h^{ba}=hc$ which implies $h^H=hH'$ and its order equals 2^n. It also satisfies $c^{2^{\ell-1}}\notin\langle h\rangle$, so $H'\cap\langle h\rangle=1$ and thus $N_H(\langle h\rangle)=C_H(h)$. The

overall contribution of $H \setminus C_H(H')$ to $|\mathscr{C}(H)|$ is

$$\begin{aligned}(4.6)\qquad &\sum_{h\in H\setminus C_H(H')} \frac{1}{|H : N_H(\langle h\rangle)|}\times\frac{1}{\phi(|h|)}\\ &\quad= \frac{|H\setminus C_H(H')|}{|H'|\times|(\mathbb{Z}/2^n\mathbb{Z})^\times|} = \frac{2^{n-1}\times 2^m\times 2^\ell}{2^\ell\times 2^{n-1}} = 2^m.\end{aligned}$$

Comparing the values. We first note that

$$\begin{aligned} Z(G) &\cong Z(H) && \cong C_{2^{n-1}}\times C_{2^{m-1}}\times C_2,\\ \Omega(G:G') &\cong \Omega(H:H') && \cong C_2\times C_2\times C_{2^\ell},\\ \Omega(G:G')\cap Z(G) &\cong \Omega(H:H')\cap Z(H) && \cong C_2\times C_2\times C_2.\end{aligned}$$

So, comparing the expressions in (4.3) and (4.5), the groups are pairwise isomorphic except for $C_G(G')$ and $C_H(H')$ themselves. Hence the difference between the numbers of conjugacy classes of cyclic groups of H and G, which equals (4.5) + (4.6) − (4.3) − (4.4), is

$$(4.7)\qquad |\mathscr{C}(H)| - |\mathscr{C}(G)| = \frac{1}{2}\big(|\mathscr{C}(C_H(H'))| - |\mathscr{C}(C_G(G'))|\big) - (n-m)2^{m-1}.$$

Recall that $C_H(H') \cong C_{2^{n-1}}\times C_{2^m}\times C_{2^\ell}$ and $C_G(G')\cong C_{2^n}\times C_{2^{m-1}}\times C_{2^\ell}$. It follows from Lemma 4.2 that

$$\begin{aligned}&|\mathscr{C}(C_H(H'))| - |\mathscr{C}(C_G(G'))|\\ &\quad= ((n-m-1)2^{m+\ell} + (2^{2\ell+1}+2^{2\ell})(2^{m-\ell}-1))\\ &\qquad - ((n-m+1)2^{m+\ell-1} + (2^{2\ell+1}+2^{2\ell})(2^{m-\ell-1}-1))\\ &\quad= (n-m)2^{m+\ell-1}.\end{aligned}$$

Hence substituting $|\mathscr{C}(C_H(H'))| - |\mathscr{C}(C_G(G'))|$ in (4.7) gives

$$|\mathscr{C}(H)| - |\mathscr{C}(G)| = (n-m)2^{m-1}(2^{\ell-1}-1).$$

□

Proof of Proposition 4.1. To see that $\mathbb{C}G\cong\mathbb{C}H$, note that both G and H possess a maximal subgroup which is abelian, namely $C_G(G')$ and $C_H(H')$, respectively. Hence, by [8, Theorem 12.11], the degrees of irreducible characters are either one or two. Then the Wedderburn decompositions of these algebras are

$$\begin{aligned}\mathbb{C}G &\cong |G/G'|\mathbb{C}\times\frac{1}{4}(|G|-|G/G'|)M_2(\mathbb{C}),\\ \mathbb{C}H &\cong |H/H'|\mathbb{C}\times\frac{1}{4}(|H|-|H/H'|)M_2(\mathbb{C})\end{aligned}$$

where $M_2(\mathbb{C})$ denotes the matrix algebra of degree 2 over $\mathbb{C}$. As $|G| = |H|$ and $|G/G'| = |H/H'|$, we have $\mathbb{C}G\cong\mathbb{C}H$.

To see that $\mathbb{Q}G\ncong\mathbb{Q}H$, note that the difference of the numbers of conjugacy classes of cyclic subgroups

$$|\mathscr{C}(H)| - |\mathscr{C}(G)| = (n-m)2^{m-1}(2^{\ell-1}-1)$$

is positive by Lemma 4.4, $n > m$ and $\ell\geq 2$. As the number of conjugacy classes of cyclic subgroups coincides with the number of Wedderburn components of the rational group algebra of a finite group [9, Corollary 7.1.12 (Artin)], this shows that $\mathbb{Q}G\ncong\mathbb{Q}H$. □

Brauer [2, Problem 2*] asked whether there are non-isomorphic finite groups that have isomorphic group algebras over every field. Dade [3] discovered an example among finite solvable groups whose orders are divisible by exactly two distinct

primes. Although our groups G and H have isomorphic group algebras over every field of characteristic 2 by Theorem A, these groups can be distinguished over the rationals by Proposition 4.1. We conclude by posing the following problem (see also [12, Problem 8.3]).

Problem. Let p be a prime. Are there non-isomorphic finite p-groups that have isomorphic group algebras over every field?

Acknowledgments

The authors would like to thank the referee for providing a reference in the proof of Lemma 2.5. The first author acknowledges financial support from the Spanish Ministry of Science and Innovation, through the Ramón y Cajal grant program (reference RYC2021-032471-I). He would also like to thank Chiba University for its hospitality.

References

[1] C. Bagiński and K. Zabielski. The modular isomorphism problem—the alternative perspective on counterexamples. *J. Pure Appl. Algebra*, 229(1):Paper No. 107826, 5, 2025. doi:10.1016/j.jpaa.2024.107826.

[2] R. Brauer. Representations of finite groups. In *Lectures on Modern Mathematics, Vol. I*, pages 133–175. Wiley, New York-London, 1963.

[3] E. C. Dade. Deux groupes finis distincts ayant la même algèbre de groupe sur tout corps. *Math. Z.*, 119:345–348, 1971. doi:10.1007/BF01109886.

[4] W. E. Deskins. Finite Abelian groups with isomorphic group algebras. *Duke Math. J.*, 23:35–40, 1956. doi:10.1215/S0012-7094-56-02304-3.

[5] D. García-Lucas, L. Margolis, and Á. del Río. Non-isomorphic 2-groups with isomorphic modular group algebras. *J. Reine Angew. Math.*, 783:269–274, 2022. doi:10.1515/crelle-2021-0074.

[6] M. Hertweck. A counterexample to the isomorphism problem for integral group rings. *Ann. of Math. (2)*, 154(1):115–138, 2001. doi:10.2307/3062112.

[7] G. Higman. *Units in group rings*. D. Phil. thesis, University of Oxford, 1940. https://solo.bodleian.ox.ac.uk/permalink/44OXF_INST/35n82s/alma990202619510107026.

[8] I. M. Isaacs. *Character theory of finite groups*. Pure and Applied Mathematics, No. 69. Academic Press [Harcourt Brace Jovanovich, Publishers], New York-London, 1976.

[9] E. Jespers and Á. del Río. *Group ring groups. Vol. 1. Orders and generic constructions of units*. De Gruyter Graduate. De Gruyter, Berlin, 2016.

[10] E. E. Kummer. Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen. *J. Reine Angew. Math.*, 44:93–146, 1852. doi:10.1515/crll.1852.44.93.

[11] M. Linckelmann. Finite-dimensional algebras arising as blocks of finite group algebras. In *Representations of algebras*, volume 705 of *Contemp. Math.*, pages 155–188. Amer. Math. Soc., [Providence], RI, 2018. doi:10.1090/conm/705/14202.

[12] L. Margolis. The modular isomorphism problem: a survey. *Jahresber. Dtsch. Math.-Ver.*, 124(3):157–196, 2022. doi:10.1365/s13291-022-00249-5.

[13] L. Margolis and T. Sakurai. Identification of non-isomorphic 2-groups with dihedral central quotient and isomorphic modular group algebras. *Rev. Mat. Iberoam.*, 41(5):1973–2002, 2025. doi:10.4171/RMI/1531.

[14] I. B. S. Passi. *Group rings and their augmentation ideals*, volume 715 of *Lecture Notes in Mathematics*. Springer, Berlin, 1979.

[15] D. S. Passman. *The algebraic structure of group rings*. Pure and Applied Mathematics. Wiley-Interscience [John Wiley & Sons], New York-London-Sydney, 1977.

[16] C. Polcino Milies and S. K. Sehgal. *An introduction to group rings*, volume 1 of *Algebra and Applications*. Kluwer Academic Publishers, Dordrecht, 2002.

[17] K. W. Roggenkamp and L. Scott. Isomorphisms of p-adic group rings. *Ann. of Math. (2)*, 126:593–647, 1987. doi:10.2307/1971362.

[18] R. Sandling. Dimension subgroups over arbitrary coefficient rings. *J. Algebra*, 21:250–265, 1972. doi:10.1016/0021-8693(72)90020-8.

[19] S. K. Sehgal. *Topics in group rings*, volume 50 of *Monographs and Textbooks in Pure and Applied Math.* Marcel Dekker, Inc., New York, 1978.

[20] L. Tóth. On the number of cyclic subgroups of a finite Abelian group. *Bull. Math. Soc. Sci. Math. Roumanie (N.S.)*, 55(103)(4):423–428, 2012. https://www.jstor.org/stable/43679274.

[21] A. Weiss. Rigidity of p-adic p-torsion. *Ann. of Math. (2)*, 127(2):317–332, 1988. doi:10.2307/2007056.

(Leo Margolis) Universidad Autónoma de Madrid, Departamento de Matemáticas, C/ Francisco Tomás y Valiente 7, Facultad de Ciencias, módulo 17, 28049 Madrid, Spain.
Email address: leo.margolis@uam.es

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