A counterexample to the modular isomorphism problem

Diego García-Lucas
(joint with Leo Margolis and Ángel del Río)

University of Murcia

Algebra and Logic Seminar,
Departament of Algebra and Logic, IMI/BAS
May 13, 2022

Table of contents

Group rings

Let R be a ring and G a finite group.

- Let
$$RG = \left\{ \sum_{g \in G} r_g g, \quad \text{with } r_g \in R \right\}$$
With the product of the group extended linearly and the obvious sum, RG is a ring.

Group rings

Let R be a ring and G a finite group.

- Let
$$RG = \left\{ \sum_{g \in G} r_g g, \quad \text{with } r_g \in R \right\}$$
With the product of the group extended linearly and the obvious sum, RG is a ring.
- If R is a commutative ring, RG has estructure of R-algebra.

Group rings

Let R be a ring and G a finite group.

- Let
$$RG = \left\{ \sum_{g \in G} r_g g, \quad \text{with } r_g \in R \right\}$$
With the product of the group extended linearly and the obvious sum, RG is a ring.
- If R is a commutative ring, RG has estructure of R-algebra.

Notation: unless stated otherwise,

- R will be an arbitrary coommutative ring or field,
- F a field of characteristic p, and
- k the field with p elements.

The isomorphism problem

Let R be a ring and G, H finite groups.

Isomorphism problem

Does $RG \cong RH$ implies $G \cong H$?

It has obviously negative answer in general: if G and H are abelian groups and have the same order, then $\mathbb{C}G \cong \mathbb{C}H$.

The isomorphism problem

Let R be a ring and G, H finite groups.

Isomorphism problem

Does $RG \cong RH$ implies $G \cong H$?

It has obviously negative answer in general: if G and H are abelian groups and have the same order, then $\mathbb{C}G \cong \mathbb{C}H$.

The isomorphism problem is the same as the question "If H is a group basis of RG, then $G \cong H$?"

The Isomorphism Problem for fields

Question 1

Does $RG \cong RH$ for every field R implies $G \cong H$?

The Isomorphism Problem for fields

Question 1

Does $RG \cong RH$ for every field R implies $G \cong H$?

Theorem (Passman, 1965)

There exists a set of

$$p^{\frac{2}{27}(n^3-23n^2)}$$

nonisomorphic p-groups of order p^n that have isomorphic group algebras over all fields of characteristic not equal to p.

The Isomorphism Problem for fields

Question 1

Does $RG \cong RH$ for every field R implies $G \cong H$?

Theorem (Passman, 1965)

There exists a set of

$$p^{\frac{2}{27}(n^3-23n^2)}$$

nonisomorphic p-groups of order p^n that have isomorphic group algebras over all fields of characteristic not equal to p.

Question 1, however, has negative answer in general:

Theorem (Dade, 1971)

There exist two non-isomorphic metabelian finite groups G and H, with order divisible by two diferent primes, such that $RG \cong RH$ for every field R.

The Modular Isomorphism Problem

Fix an integer prime p. Let G and H finite p-groups.

Question 2

Does $FG \cong FH$ for each field F of characteristic p implies $G \cong H$?

The Modular Isomorphism Problem

Fix an integer prime p. Let G and H finite p-groups.

Question 2

Does $FG \cong FH$ for each field F of characteristic p implies $G \cong H$?

If k is the field with p element then

$$kG \cong kH \qquad \Rightarrow \qquad FG \cong F \otimes_k kG \cong F \otimes_k kH \cong FH$$

for each field F with characteristic p.

Hence Question 2 is equivalent to:

Question 2', or Modular Isomorphism Problem (MIP)

If k the field with p elements, does $kG \cong kH$ implies $G \cong H$?

This question was explicitly mentioned by R. Brauer in a survey in 1963.

The Isomorphism Problem with integral coefficients

Let G and H finite groups.

Question 3

Does $RG \cong RH$ for every ring R implies $G \cong H$?

The Isomorphism Problem with integral coefficients

Let G and H finite groups.

Question 3

Does $RG \cong RH$ for every ring R implies $G \cong H$?

Since

$$\mathbb{Z}G \cong \mathbb{Z}H \quad \Rightarrow \quad RG \cong R \otimes_{\mathbb{Z}} \mathbb{Z}G \cong R \otimes_{\mathbb{Z}} \mathbb{Z}H \cong RH,$$

this question is equivalent to

Question 3', or Isomorphism Problem with integral coefficients

Does $\mathbb{Z}G \cong \mathbb{Z}H$ implies $G \cong H$?

The Isomorphism Problem with integral coefficients

Let G and H finite groups.

Question 3

Does $RG \cong RH$ for every ring R implies $G \cong H$?

Since

$$\mathbb{Z}G \cong \mathbb{Z}H \quad \Rightarrow \quad RG \cong R \otimes_{\mathbb{Z}} \mathbb{Z}G \cong R \otimes_{\mathbb{Z}} \mathbb{Z}H \cong RH,$$

this question is equivalent to

Question 3', or Isomorphism Problem with integral coefficients

Does $\mathbb{Z}G \cong \mathbb{Z}H$ implies $G \cong H$?

"*There are, however, two glimmers of hope. The first one concerns integral group rings, and the second concern p-groups over $GF(p)$*" (The algebraic structure of group rings, Passman, 1977)

The first glimmer of hope

Theorem (Higman, 1940)

If G and H are abelian groups, then $\mathbb{Z}G \cong \mathbb{Z}H$ implies $G \cong H$.

The first glimmer of hope

Theorem (Higman, 1940)

If G and H are abelian groups, then $\mathbb{Z}G \cong \mathbb{Z}H$ implies $G \cong H$.

Theorem (Whitcomb, 1968)

If G and H are metabelian groups, then $\mathbb{Z}G \cong \mathbb{Z}H$ implies $G \cong H$.

The first glimmer of hope

Theorem (Higman, 1940)

If G and H are abelian groups, then $\mathbb{Z}G \cong \mathbb{Z}H$ implies $G \cong H$.

Theorem (Whitcomb, 1968)

If G and H are metabelian groups, then $\mathbb{Z}G \cong \mathbb{Z}H$ implies $G \cong H$.

Theorem (Roggenkamp-Scott, 1987)

If G and H are p-groups, then $\mathbb{Z}G \cong \mathbb{Z}H$ implies $G \cong H$.

The first glimmer of hope

Theorem (Higman, 1940)

If G and H are abelian groups, then $\mathbb{Z}G \cong \mathbb{Z}H$ implies $G \cong H$.

Theorem (Whitcomb, 1968)

If G and H are metabelian groups, then $\mathbb{Z}G \cong \mathbb{Z}H$ implies $G \cong H$.

Theorem (Roggenkamp-Scott, 1987)

If G and H are p-groups, then $\mathbb{Z}G \cong \mathbb{Z}H$ implies $G \cong H$.

Theorem (Weiss, 1988)

If G and H are nilpotent groups, then $\mathbb{Z}G \cong \mathbb{Z}H$ implies $G \cong H$.

Fading the first glimmer of hope

Theorem (Hertweck, 2001)

There exist two nonisomorphic groups with order $2^{21} \cdot 97^{28}$ such that

$$\mathbb{Z}G \cong \mathbb{Z}H.$$

The second glimmer of hope

Fix an integer prime p. Let G and H finite p-groups.

Question 2

Does $FG \cong FH$ for each field F of characteristic p implies $G \cong H$?

Is equivalent to:

Question 2', or Modular Isomorphism Problem (MIP)

If k the field with p elements, does $kG \cong kH$ implies $G \cong H$?

Question 2''

If F is a fixed field of characteristic p, does $FG \cong FH$ implies $G \cong H$?

A positive answer to Question 2'' implies a positive answer to MIP.

The second glimmer of hope: Positive results to the MIP

(arbitrary field of characteristic p/only the prime field/**relevant**)

- abelian p-groups (Deskins, 1956);
- p-groups of small order:
  - Not computer aided results:
    - p-groups of order at most p^4 (Passman, 1965);
    - 2-groups with order 2^5 (Makasikis, 1976; Navarro-Sambale, 2017);
    - p-groups with order p^5 (Salim-Sandling, 1996);
    - 2-groups with order 2^6 (Hertweck-Soriano, 2006);
  - Computer aided results:
    - Groups of order 2^6 (Wursthorn, 1990);
    - Groups of order 2^7 (Wursthorn, 1997);
    - **Groups of order** 2^8 and 3^6 (Eick, 2008, revised by Margolis-Moede, 2020);
    - Groups of order 5^6 (with exceptions) and 3^7 (Margolis-Moede, 2020, based on Eick's algorithm).

Positive results to the MIP (II)

- p-groups with trivial third dimension subgroup (Passi-Sehgal, 1972).
- 2-groups of maximal class (Carlson, 1977).
- p-groups of maximal class, with order not greater than p^{p+1} and with a maximal subgroup which is abelian (Bagiński-Caranti, 1988);
- p-groups of nilpotency class 2 with elementary abelian derived subgroup (Sandling, 1989).
- p-groups with center of index p^2 (Drensky, 1989);
- Metacyclic p-groups (Bagiński, 1988, for $p > 3$, completed by Sandling, 1996).
- Elementary-abelian-by-cyclic p-groups (Bagiński, 1999).
- 2-**generated** p-**group with nilpotency class** 3 **and elementary abelian derived subgroup** (Bagiński, 1999; Margolis-Moede, 2020).

Positive results to the MIP (III)

- 2-groups of almost maximal class (Bagiński-Konovalov, 2004);
- Groups with trivial fourth dimension subgroup for $p > 2$ (Hertweck, 2007).
- p-groups with a cyclic subgroup of index p^2 (Bagiński-Konovalov, 2007);
- 3-groups of maximal class (except two families of groups) (Bagiński-Kurdics, 2019)
- **p-groups 2-generated of nilpotency class 2 with cyclic derived subgroup** (Broche-del Río, 2019). ($p > 2$; $p = 2$);
- 2-groups of nilpotency class 3 s.t. $[G : \mathcal{Z}(G)] = |\Phi(G)| = 8$ (Margolis-Sakurai-Stanojkovski, 2021);
- 2-groups with cyclic centre such that $G/\mathcal{Z}(G)$ is dihedral (Margolis-Sakurai-Stanojkovski, 2021).

The modular group algebra

Let F be a field of characteristic p, and G a finite p-group.

- The augmentation map is

$$\varepsilon : FG \to F, \qquad \sum_{g \in G} r_g g \mapsto \sum_{g \in G} r_g \qquad (r_g \in F).$$

The modular group algebra

Let F be a field of characteristic p, and G a finite p-group.

- The augmentation map is

$$\varepsilon : FG \to F, \qquad \sum_{g\in G} r_g g \mapsto \sum_{g\in G} r_g \qquad (r_g \in F).$$

- $I(FG) := \ker(\varepsilon)$ is the Jacobson radical of FG.
- $I(FG)$ is nilpotent.

The modular group algebra

Let F be a field of characteristic p, and G a finite p-group.

- The augmentation map is

$$\varepsilon : FG \to F, \qquad \sum_{g \in G} r_g g \mapsto \sum_{g \in G} r_g \qquad (r_g \in F).$$

- $I(FG) := \ker(\varepsilon)$ is the Jacobson radical of FG.
- $I(FG)$ is nilpotent.
- FG is a local ring, i.e.,

$$FG = F + I(FG).$$

- The group of units of FG is $FG \setminus I(FG)$.

The modular group algebra

Let F be a field of characteristic p, and G a finite p-group.

- The augmentation map is

$$\varepsilon : FG \to F, \qquad \sum_{g \in G} r_g g \mapsto \sum_{g \in G} r_g \qquad (r_g \in F).$$

- $I(FG) := \ker(\varepsilon)$ is the Jacobson radical of FG.
- $I(FG)$ is nilpotent.
- FG is a local ring, i.e.,

$$FG = F + I(FG).$$

- The group of units of FG is $FG \setminus I(FG)$.
- $V(FG) = 1 + I(FG)$ is called the group of normalized units.

Contrasts: Maschke Theorem

Let R be a field and G a finite group.

- If $\mathrm{char}(R) \nmid |G|$, then RG is semisimple. Hence we can apply the Wedderburn decomposition theorem, so

$$RG = \oplus M_{n_i \times n_i}(D_i),$$

where $M_{n_i \times n_i}(D_i)$ is the $n_i \times n_i$-matrix ring over a division ring D_i.

Contrasts: Maschke Theorem

Let R be a field and G a finite group.

- If $\mathrm{char}(R) \nmid |G|$, then RG is semisimple. Hence we can apply the Wedderburn decomposition theorem, so

$$RG = \oplus M_{n_i \times n_i}(D_i),$$

where $M_{n_i \times n_i}(D_i)$ is the $n_i \times n_i$-matrix ring over a division ring D_i.

- If $\mathrm{char}(R) \mid |G|$ then

$$RG = b_1 RG \oplus b_2 RG \oplus \cdots \oplus b_n RG,$$

where $\{b_1, \ldots, b_n\}$ is a complete set of orthogonal primitive central idempotents.

Contrasts: Maschke Theorem

Let R be a field and G a finite group.

- If $\operatorname{char}(R) \nmid |G|$, then RG is semisimple. Hence we can apply the Wedderburn decomposition theorem, so

$$RG = \oplus M_{n_i \times n_i}(D_i),$$

where $M_{n_i \times n_i}(D_i)$ is the $n_i \times n_i$-matrix ring over a division ring D_i.

- If $\operatorname{char}(R) \mid |G|$ then

$$RG = b_1 RG \oplus b_2 RG \oplus \cdots \oplus b_n RG,$$

where $\{b_1, \ldots, b_n\}$ is a complete set of orthogonal primitive central idempotents.

  - If $\operatorname{char}(R) = p$ and $|G| = p^N$, then $\{b_1, \ldots, b_n\} = \{1\}$,

$$RG = R + I(RG).$$

The modular group algebra

Let F be a field of characteristic p, and G a finite p-group. The subgroup of G

$$\mathcal{M}_i(G) = G \cap (1 + I(FG)^i) \qquad (i \geq 1)$$

is called the i-th dimension subgroup of G.

The modular group algebra

Let F be a field of characteristic p, and G a finite p-group. The subgroup of G

$$\mathcal{M}_i(G) = G \cap (1 + I(FG)^i) \qquad (i \geq 1)$$

is called the i-th dimension subgroup of G.

Theorem (Jennings, 1941)

The dimension subgroups satisfy the recursive relation

$$\begin{aligned} \mathcal{M}_1(G) &= G; \\ \mathcal{M}_i(G) &= [\mathcal{M}_{i-1}(G), G]\mathcal{M}_{\lceil \frac{i}{p} \rceil}(G)^p \qquad (i \geq 2) \end{aligned}$$

Jennings bases

Theorem (Jennings, 1941)

Assume n is an integer such that $\mathcal{M}_n(G) = 1$. Let $g_1, \ldots, g_\ell$ be the union of the bases of

$$\frac{\mathcal{M}_1(G)}{\mathcal{M}_2(G)}, \quad \frac{\mathcal{M}_2(G)}{\mathcal{M}_3(G)}, \quad \ldots, \quad \frac{\mathcal{M}_{n-1}(G)}{\mathcal{M}_n(G)}$$

when these quotients are viewed as vector spaces over the field with p elements. Then the set

$$B = \left\{ \prod_{i=1}^{\ell} (g_1 - 1)^{\alpha_1} \ldots (g_\ell - 1)^{\alpha_\ell} \; : \; 0 \leq \alpha_i < p, \; \alpha_1 \ldots \alpha_\ell \neq 0 \right\}$$

is a basis of $I(FG)$.

Jennings bases

Proposition (Jennings, 1941)

Let B be a Jennings basis. Then there is a sequence of subsets

$$B = B_1 \supseteq B_2 \supseteq \dots$$

such that for each $t \geq 1$,

$$I(FG)^t = \mathrm{span}_F B_t.$$

The concept of Hertweck-Soriano

Let k be the field with p elements.

Lemma (Passi-Sehgal)

Let J be a multiplicatively closed subspace of kG. If

$$G \cap (1 + J + I(FG)^n) = \mathcal{M}_n(G) \qquad \text{for each } n \geq 1 \qquad (\star)$$

then

$$\tilde{G} \cap (1 + J + I(FG)^n) = \mathcal{M}_n(\tilde{G})$$

for each group basis $\tilde{G}$ and each $n \geq 1$. In particular

$$\tilde{G} \cap (1 + J) = 1.$$

The concept of Hertweck-Soriano

- Start with a group basis G.
- Use a Jennings basis to construct an ideal J verifying $(\star)$.
- Then $\tilde{G} \cap (1+J) = 1$ for each group basis $\tilde{G}$.
- Thus every group basis $\tilde{G}$ embeds into $V(FG/J)$.
- Find all the subgroups in $V(FG/J)$ of order $|G|$.

The concept of Hertweck-Soriano

- Start with a group basis G.
- Use a Jennings basis to construct an ideal J verifying $(\star)$.
- Then $\tilde{G} \cap (1+J) = 1$ for each group basis $\tilde{G}$.
- Thus every group basis $\tilde{G}$ embeds into $V(FG/J)$.
- Find all the subgroups in $V(FG/J)$ of order $|G|$.
    - If all of them are isomorphic to G, we are done.
    - If any of them is not isomorphic to G, consider all its preimages in FG.

The groups

For $n_1 > n_2 > 2$, consider the groups

$$\begin{aligned} G &= \left\langle x, y, z \mid z = [y,x],\ x^{2^{n_1}} = y^{2^{n_2}} = z^4 = 1,\ z^x = z^y = z^{-1} \right\rangle \\ H &= \left\langle a, b, c \mid c = [b,a],\ a^{2^{n_1}} = b^{2^{n_2}} = c^4 = 1,\ c^a = c^{-1},\ c^b = c \right\rangle \end{aligned}$$

(notation: $x^y = y^{-1}xy$ and $[y,x] = y^{-1}x^{-1}yx$)

G and H are non-isomorphic

$$C_G(G') = \langle z, x^2, xy \rangle \quad \Rightarrow \quad \frac{C_G(G')}{G'} = \langle x^2 G', xyG' \rangle \text{ has exponent } 2^{n_1}.$$

$$\text{since} \quad |x| = |xG'| = 2^{n_1}, \qquad |y| = |yG'| = 2^{n_2} < 2^{n_1}.$$

G and H are non-isomorphic

$$C_G(G') = \langle z, x^2, xy \rangle \quad \Rightarrow \quad \frac{C_G(G')}{G'} = \langle x^2 G', xyG' \rangle \text{ has exponent } 2^{n_1}.$$

since $\quad |x| = |xG'| = 2^{n_1}, \qquad |y| = |yG'| = 2^{n_2} < 2^{n_1}.$

$$C_H(H') = \langle c, a^2, b \rangle \quad \Rightarrow \quad \frac{C_G(H')}{H'} = \langle a^2 H', bH' \rangle \text{ has exponent } 2^{n_1 - 1}.$$

since $\quad |a| = |aH'| = 2^{n_1}, \qquad |b| = |bH'| = 2^{n_2} < 2^{n_1}.$

Fading the second glimmer of hope

For $n_1 > n_2 > 2$, consider the groups

$$G = \langle x, y, z \mid z = [y, x],\ x^{2^{n_1}} = y^{2^{n_2}} = z^4 = 1,\ z^x = z^y = z^{-1} \rangle$$
$$H = \left\langle a, b, c \mid c = [b, a],\ a^{2^{n_1}} = b^{2^{n_2}} = c^4 = 1,\ c^a = c^{-1},\ c^b = c \right\rangle$$

Theorem (G-L, Margolis, del Río)

The groups G and H are non-isomorphic but if F is a field of characteristic 2 then the group algebras FG and FH are isomorphic.

The group $\widetilde{G}$

Remark

If k is the field with two element then

$$kG \cong kH \qquad \Rightarrow \qquad FG \cong F \otimes_k kG \cong F \otimes_k kH \cong FH$$

for each field F with characteristic 2 .

The group $\widetilde{G}$

Remark

If k is the field with two element then

$$kG \cong kH \qquad \Rightarrow \qquad FG \cong F \otimes_k kG \cong F \otimes_k kH \cong FH$$

for each field F with characteristic 2 .

From now on we will work in kH. Write

$$\widetilde{x} = a \quad \text{and} \quad \widetilde{y} = b(a + b + ab)c.$$

Consider

$$\widetilde{G} = \langle \widetilde{x}, \widetilde{y} \rangle \subseteq V(kH).$$

$\widetilde{G}$ is an epimorphic image of G.

Recall that

$$G = \left\langle x, y, z \;\mid\; z = [y, x],\ x^{2^{n_1}} = y^{2^{n_2}} = z^4 = 1,\ z^x = z^{-1},\ z^y = z^{-1} \right\rangle$$

Write $\widetilde{z} = [\widetilde{y}, \widetilde{x}]$.

$\widetilde{G}$ is an epimorphic image of G.

Recall that

$$G = \left\langle x, y, z \mid z = [y, x],\ x^{2^{n_1}} = y^{2^{n_2}} = z^4 = 1,\ z^x = z^{-1},\ z^y = z^{-1} \right\rangle$$

Write $\widetilde{z} = [\widetilde{y}, \widetilde{x}]$.

- $\tilde{x}^{2^{n_1}} = a^{2^{n_1}} = 1$.

$\widetilde{G}$ is an epimorphic image of G.

Recall that

$$G = \left\langle x, y, z \;\middle|\; z = [y, x],\ x^{2^{n_1}} = y^{2^{n_2}} = z^4 = 1,\ z^x = z^{-1},\ z^y = z^{-1} \right\rangle$$

Write $\widetilde{z} = [\widetilde{y}, \widetilde{x}]$.

- $\tilde{x}^{2^{n_1}} = a^{2^{n_1}} = 1.$
- $\widetilde{x}^2 = a^2 \in \mathcal{Z}(kH)$ implies

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

(We used the formula $[u, v \cdot w] = [u, v] \cdot [u, w]^v$.)

$\widetilde{G}$ is an epimorphic image of G (II)

- Observe that a^2, b^4, c^2 and $b^2c \in \mathcal{Z}(H)$ and the conjugacy class of b in H is $\{b, bc\}$. Then

$$\widetilde{y}^2 = b^4c^2 + a^2(b^2c + b^4c^2) + a^2b^2c(b + bc) \in \mathcal{Z}(kH).$$

$\widetilde{G}$ is an epimorphic image of G (II)

- Observe that a^2, b^4, c^2 and $b^2c \in \mathcal{Z}(H)$ and the conjugacy class of b in H is $\{b, bc\}$. Then

$$\widetilde{y}^2 = b^4c^2 + a^2(b^2c + b^4c^2) + a^2b^2c(b + bc) \in \mathcal{Z}(kH).$$

Thus

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

(Here we used the formula $[u \cdot w, v] = [u, v]^w \cdot [w, v]$.)

$\widetilde{G}$ is an epimorphic image of G (II)

- Observe that a^2, b^4, c^2 and $b^2c \in \mathcal{Z}(H)$ and the conjugacy class of b in H is $\{b, bc\}$. Then

$$\widetilde{y}^2 = b^4c^2 + a^2(b^2c + b^4c^2) + a^2b^2c(b + bc) \in \mathcal{Z}(kH).$$

Thus

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

(Here we used the formula $[u \cdot w, v] = [u, v]^w \cdot [w, v]$.)

- Finally,

$$\begin{aligned}\widetilde{y}^{2^{n_2}} = (\widetilde{y}^2)^{2^{n_2-1}} &= b^{2^{n_2+1}}c^{2^{n_2}} + a^{2^{n_2}}(b^{2^{n_2}}c^{2^{n_2-1}} + b^{2^{n_2+1}}c^{2^{n_2}}) \\ &+ a^{2^{n_2}}b^{2^{n_2}}c^{2^{n_2-1}}(b^{2^{n_2-1}} + b^{2^{n_2-1}}c^{2^{n_2-1}}) \\ &= 1.\end{aligned}$$

$\widetilde{G}$ is an epimorphic image of G (III)

- Denote $J = (c-1)kH$.
  - Observe that $c^4 = 1$ implies
  $$J^4 = (c^4 - 1)kH = 0.$$
  - Since kH/J is commutative we have that
  $$V(kH)' \subseteq 1 + J.$$

Hence

$$z^4 \in \left(V(kH)'\right)^4 \subseteq (1+J)^4 = 1 + J^4 = 1.$$

$\widetilde{G}$ is an epimorphic image of G (III)

- Denote $J = (c-1)kH$.
  - Observe that $c^4 = 1$ implies
  $$J^4 = (c^4 - 1)kH = 0.$$
  - Since kH/J is commutative we have that
  $$V(kH)' \subseteq 1 + J.$$

Hence

$$z^4 \in \left(V(kH)'\right)^4 \subseteq (1+J)^4 = 1 + J^4 = 1.$$

This proves that $G \twoheadrightarrow \widetilde{G}$.

Results that we will use

Proposition

Let A be a finite dimensional algebra over a field, $J(A)$ its Jacobson radical and B a subalgebra of A. Then

$$A = B + J(A) \quad \text{implies} \quad A = B.$$

Results that we will use

Proposition

Let A be a finite dimensional algebra over a field, $J(A)$ its Jacobson radical and B a subalgebra of A. Then

$$A = B + J(A) \quad \text{implies} \quad A = B.$$

Since $I(kH)^2$ is the Jacobson radical of $I(kH)$,

Corollary

Let $g_1, \ldots, g_d$ be a generating set for H. Then for any $\alpha_1, \ldots, \alpha_d \in I(kH)^2$,

$$g_1 - 1 + \alpha_1, \ldots, g_d - 1 + \alpha_d \qquad \text{generate } I(kH).$$

$\widetilde{G}$ contains a basis kH

Observe that

$$c-1 \in H'-1 \subseteq I(kH)^2$$

- $\tilde{x} = a$.

$\widetilde{G}$ contains a basis kH

Observe that

$$c - 1 \in H' - 1 \subseteq I(kH)^2$$

- $\tilde{x} = a$.
- It holds

$$\begin{aligned} \tilde{y} &= b(a+b+ab)c \\ &\equiv b(a+b+ab) \\ &= b(1+(1+a)(1+b)) \\ &\equiv b \mod I(kH)^2 \end{aligned}$$

- By the Corollary $\tilde{x} - 1$ and $\tilde{y} - 1$ generate $I(kH)$.

$\widetilde{G}$ contains a basis kH

Observe that

$$c - 1 \in H' - 1 \subseteq I(kH)^2$$

- $\tilde{x} = a$.
- It holds

$$\begin{aligned} \tilde{y} &= b(a+b+ab)c \\ &\equiv b(a+b+ab) \\ &= b(1+(1+a)(1+b)) \\ &\equiv b \mod I(kH)^2 \end{aligned}$$

- By the Corollary $\tilde{x} - 1$ and $\tilde{y} - 1$ generate $I(kH)$.
- $\tilde{x}, \tilde{y}, 1$ generate kH.

$\widetilde{G}$ contains a basis kH

Observe that

$$c - 1 \in H' - 1 \subseteq I(kH)^2$$

- $\tilde{x} = a$.
- It holds

$$\begin{aligned} \tilde{y} &= b(a+b+ab)c \\ &\equiv b(a+b+ab) \\ &= b(1+(1+a)(1+b)) \\ &\equiv b \mod I(kH)^2 \end{aligned}$$

- By the Corollary $\tilde{x}-1$ and $\tilde{y}-1$ generate $I(kH)$.
- $\tilde{x}, \tilde{y}, 1$ generate kH.
- $\tilde{G} = \langle \tilde{x}, \tilde{y} \rangle$ generates kH as a vector space.

Proof of the theorem

We have proved:

- $\tilde{G}$ is an epimorphic image of G. In particular $|\tilde{G}| \leq |G|$.
- $\tilde{G}$ contains a basis of kH.

Hence

$$|G| = |H| = \dim_k(kH) \leq |\tilde{G}| \leq |G|,$$

Proof of the theorem

We have proved:

- $\tilde{G}$ is an epimorphic image of G. In particular $|\tilde{G}| \leq |G|$.
- $\tilde{G}$ contains a basis of kH.

Hence

$$|G| = |H| = \dim_k(kH) \leq |\tilde{G}| \leq |G|,$$

so

$$\tilde{G} \cong G \quad \text{and} \quad \tilde{G} \text{ is a basis of } kH.$$

Q.E.D.

Non-invariants

Let $n_1 = 4$ and $n_2 = 3$. Then $|G| = |H| = 2^9$,

Non-invariants

Let $n_1 = 4$ and $n_2 = 3$. Then $|G| = |H| = 2^9$,

$$\exp(C_G(G')) = 2^3, \quad \text{and} \quad \exp(C_H(H')) = 2^4;$$

$$|\mathrm{Aut}(G)| = 2^{15}, \quad \text{and} \quad |\mathrm{Aut}(H)| = 2^{14};$$

Non-invariants

Let $n_1 = 4$ and $n_2 = 3$. Then $|G| = |H| = 2^9$,

$$\exp(C_G(G')) = 2^3, \quad \text{and} \quad \exp(C_H(H')) = 2^4;$$

$$|\mathrm{Aut}(G)| = 2^{15}, \quad \text{and} \quad |\mathrm{Aut}(H)| = 2^{14};$$

Let $N(G)$ be the number of conjugacy classes of cyclic subgroups of G.

$$N(G) = 66, \quad \text{and} \quad N(H) = 62$$

Non-invariants

Let $n_1 = 4$ and $n_2 = 3$. Then $|G| = |H| = 2^9$,

$$\exp(C_G(G')) = 2^3, \quad \text{and} \quad \exp(C_H(H')) = 2^4;$$

$$|\mathrm{Aut}(G)| = 2^{15}, \quad \text{and} \quad |\mathrm{Aut}(H)| = 2^{14};$$

Let $N(G)$ be the number of conjugacy classes of cyclic subgroups of G.

$$N(G) = 66, \quad \text{and} \quad N(H) = 62$$

Corollary

The following group-theoretical invariants are not determined by kG:

- The exponent of $C_G(G')$.
- The size of $\mathrm{Aut}(G)$.
- The number of conjugacy classes of cyclic subgroups of G.

Questions

$$N(G) \neq N(H) \qquad \text{implies} \qquad \mathbb{Q}G \not\cong \mathbb{Q}H.$$

(because $N(G)$ is the number of the indecomposable direct summands of $\mathbb{Q}G$)

Questions

$$N(G) \neq N(H) \qquad \text{implies} \qquad \mathbb{Q}G \ncong \mathbb{Q}H.$$

(because $N(G)$ is the number of the indecomposable direct summands of $\mathbb{Q}G$)

Question 5

Let G and H be finite p-groups.

$$RG \cong RH \text{ for every field } R \quad \text{implies} \quad G \cong H?$$

Relation with the known results

MIP has positive answer	G and H
2-generated with cyclic derived subgroup and nilpotency class 2	2-generated with cyclic derived subgroup and nilpotency class 3
2-generated with nilpotency class 3 and elementary abelian derived subgroup	2-generated with nilpotency class 3 and cyclic derived subgroup of order 4
Order 2^8	Order 2^n with $n \geq 9$.

Questions (II)

Question 6

Has MIP a positive answer for p-groups of odd order (i.e., with $p > 2$)? The following families are of special interest:

- p-groups with cyclic derived subgroup
- p-groups which are 2-generated.
- p-groups with nilpotency class 3.

Questions (II)

Question 6

Has MIP a positive answer for p-groups of odd order (i.e., with $p > 2$)? The following families are of special interest:

- p-groups with cyclic derived subgroup
- p-groups which are 2-generated.
- p-groups with nilpotency class 3.

Theorem (G-L, del Río, Stanojkovski)

Let G be finite p-group, $p > 2$, with cyclic derived subgroup, and F be an arbitrary field of characteristic p. Then

$$\exp(C_G(G'))$$

is determined by FG.

Questions (III)

Question 7

Does MIP has positive answer for p-groups of nilpotency class 2?

It was already mentioned in Sandling's survey "The isomorphism problem for group rings" in 1985:
"Nonetheless, it is a sad reflection on the state of the modular isomorphism problem that the case of class 2 groups is yet to be decided in general."

Questions (III)

Question 7

Does MIP has positive answer for p-groups of nilpotency class 2?

It was already mentioned in Sandling's survey "The isomorphism problem for group rings" in 1985:
"Nonetheless, it is a sad reflection on the state of the modular isomorphism problem that the case of class 2 groups is yet to be decided in general."
Let k be the field with p elements.

Question 8

There exist finite p-groups G and H and a field F of characteristic p such that

$$FG \cong FH \quad \text{but} \quad kG \ncong kH?$$

References I

C. Bagiński, *The isomorphism question for modular group algebras of metacyclic p-groups*, Proc. Amer. Math. Soc. **104** (1988), no. 1, 39–42.

______, *On the isomorphism problem for modular group algebras of elementary abelian-by-cyclic p-groups*, Colloq. Math. **82** (1999), no. 1, 125–136.

C. Bagiński and A. Caranti, *The modular group algebras of p-groups of maximal class*, Canad. J. Math. **40** (1988), no. 6, 1422–1435.

O. Broche and Á. del Río, *The Modular Isomorphism Problem for two generated groups of class two*, https://arxiv.org/abs/2003.13281, Indian Journal of Pure and Applied Mathematics, in press (2020).

C. Bagiński and A. Konovalov, *The modular isomorphism problem for finite p-groups with a cyclic subgroup of index p^2*, Groups St. Andrews 2005. Vol. 1, London Math. Soc. Lecture Note Ser., vol. 339, Cambridge Univ. Press, Cambridge, 2007, pp. 186–193.

R. Brauer, *Representations of finite groups*, Lectures on Modern Mathematics, Vol. I, Wiley, New York, 1963, pp. 133–175.

J. F. Carlson, *Periodic modules over modular group algebras*, J. London Math. Soc. (2) **15** (1977), no. 3, 431–436.

E. Dade, *Deux groupes finis distincts ayant la même algèbre de groupe sur tout corps*, Math. Z. **119** (1971), 345–348.

References II

W. E. Deskins, *Finite Abelian groups with isomorphic group algebras*, Duke Math. J. **23** (1956), 35–40. MR 77535

V. Drensky, *The isomorphism problem for modular group algebras of groups with large centres*, Representation theory, group rings, and coding theory **93** (1989), 145–153.

B. Eick, *Computing automorphism groups and testing isomorphisms for modular group algebras*, J. Algebra **320** (2008), no. 11, 3895–3910.

B. Eick and A. Konovalov, *The modular isomorphism problem for the groups of order 512*, Groups St Andrews 2009 in Bath. Volume 2, London Math. Soc. Lecture Note Ser., vol. 388, Cambridge Univ. Press, Cambridge, 2011, pp. 375–383.

D. García-Lucas, L. Margolis, and Á. del Río, *Non-isomorphic 2-groups with isomorphic modular group algebras*, J. Reine Angew. Math. **154** (2022), no. 783, 269–274.

G. Higman, *Units in group rings*, 1940, Thesis (Ph.D.)–Univ. Oxford.

______, *The units of group-rings*, Proc. London Math. Soc. (2) **46** (1940), 231–248.

M. Hertweck and M. Soriano, *On the modular isomorphism problem: groups of order* 2^6, Groups, rings and algebras, Contemp. Math., vol. 420, Amer. Math. Soc., Providence, RI, 2006, pp. 177–213.

R. L. Kruse and D. T. Price, *Nilpotent rings*, Gordon and Breach Science Publishers, New York-London-Paris, 1969.

References III

L. Margolis, *The Modular Isomorphism Problem: A Survey*, Jahresber. Dtsch. Math. Ver. (2022).

L. Margolis and T. Moede, *The Modular Isomorphism Problem for small groups – revisiting Eick's algorithm*, arXiv:2010.07030, https://arxiv.org/abs/2010.07030.

L. Margolis and M. Stanojkovski, *On the modular isomorphism problem for groups of class* 3 *and obelisks*, 2022.

D. S. Passman, *The group algebras of groups of order p^4 over a modular field*, Michigan Math. J. **12** (1965), 405–415. MR 0185022

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

K. W. Roggenkamp and L. Scott, *Isomorphisms of p-adic group rings*, Ann. of Math. (2) **126** (1987), no. 3, 593–647.

R. Sandling, *The modular group algebra of a central-elementary-by-abelian p-group*, Arch. Math. (Basel) **52** (1989), no. 1, 22–27.

______, *The modular group algebra problem for metacyclic p-groups*, Proc. Amer. Math. Soc. **124** (1996), no. 5, 1347–1350.

M. A. M. Salim and R. Sandling, *The modular group algebra problem for groups of order p^5*, J. Austral. Math. Soc. Ser. A **61** (1996), no. 2, 229–237.

References IV

A. Weiss, *Rigidity of p-adic p-torsion*, Ann. of Math. (2) **127** (1988), no. 2, 317–332.

A. Whitcomb, *The Group Ring Problem*, ProQuest LLC, Ann Arbor, MI, 1968, Thesis (Ph.D.)–The University of Chicago.

Thanks for your attention