On the Modular Isomorphism Problem for groups of class 3

Mima Stanojkovski, joint with L. Margolis
(partial support: FWO, CIRM-FBK Trento)

Max-Planck-Institut für
Mathematik
in den Naturwissenschaften

GOThIC - Winter Series 2021

21st January 2021

MAX-PLANCK-GESELLSCHAFT

My first conference - IGT 2014

Introduction

Group rings, algebras, and associated problems

Let G be a finite group and R be a commutative ring.

The group ring of G over R is the free R-module on G

$$RG = \bigoplus_{g \in G} Rg$$

where the ring multiplication is given by

$$\left(\sum_{g \in G} r_g g\right) \cdot \left(\sum_{h \in G} s_h h\right) = \sum_{g \in G} \sum_{h \in G} (r_g s_h) gh$$

If R is a field, then RG is the group algebra of G over R; if $R = \mathbb{Z}$, then RG is the integral group ring of G.

Group rings arise naturally in the context of group representations, but have applications in many areas of mathematics.

Question. Which properties of the group G can be recovered from its group ring/algebra RG? (invariants)

Facts.

- $\mathrm{rk}\, RG = |G|$
- RG is abelian $\iff$ G is abelian

Question. Which properties of the group G can be recovered from its group ring/algebra RG? (invariants)

Facts.

- $\mathrm{rk}\, RG = |G|$
- RG is abelian $\iff$ G is abelian

The Isomorphism Problem (IP). Let G and H be finite groups and let R be a commutative ring. Is it true that

$$RG \cong RH \iff G \cong H?$$

A group H with $RG \cong RH$ is a group base of RG.

Remark. G is a subgroup of the group of units $U(RG)$ of RG, actually a subgroup of the trivial units $U(R)G$ in RG

Remark. G is a subgroup of the group of units $U(RG)$ of RG, actually a subgroup of the trivial units $U(R)G$ in RG

Exercise. $U(\mathbb{F}_pG) = \mathbb{F}_p^*G \iff |\mathbb{F}_pG| = 4, 8, 9, p.$

Remark. G is a subgroup of the group of units $U(RG)$ of RG, actually a subgroup of the trivial units $U(R)G$ in RG

Exercise. $U(\mathbb{F}_pG) = \mathbb{F}_p^*G \iff |\mathbb{F}_pG| = 4, 8, 9, p.$

Theorem (Higman '40)

If G is abelian, then all the torsion elements of $U(\mathbb{Z}G)$ are trivial. Moreover, $U(\mathbb{Z}G) = \pm G \iff$ one of the following holds:

- *G is abelian and $\exp(G)$ divides 4 or 6*
- *G is a Hamiltonian 2-group, i.e. $G \cong Q_8 \times C_2 \times \ldots \times C_2$*

Remark. G is a subgroup of the group of units $U(RG)$ of RG, actually a subgroup of the trivial units $U(R)G$ in RG

Exercise. $U(\mathbb{F}_pG) = \mathbb{F}_p^*G \iff |\mathbb{F}_pG| = 4, 8, 9, p.$

Theorem (Higman '40)

If G is abelian, then all the torsion elements of $U(\mathbb{Z}G)$ are trivial. Moreover, $U(\mathbb{Z}G) = \pm G \iff$ one of the following holds:

- *G is abelian and $\exp(G)$ divides 4 or 6*
- *G is a Hamiltonian 2-group, i.e. $G \cong Q_8 \times C_2 \times \ldots \times C_2$*

Remark. The solution to the (IP) heavily depends on the choice of the base ring R. Wedderburn's theorem yields $\mathbb{C}C_4 \cong \mathbb{C}(C_2 \times C_2)$, however $\mathbb{Z}C_4 \ncong \mathbb{Z}(C_2 \times C_2)$ and $\mathbb{Q}C_4 \ncong \mathbb{Q}(C_2 \times C_2)$.

Remark. For each pair (G, R), one has that $RG \cong R \otimes_{\mathbb{Z}} \mathbb{Z}G$. In particular, a negative solution to (IP) over $\mathbb{Z}$ is a negative solution to (IP) over any R.

Remark. For each pair (G, R), one has that $RG \cong R \otimes_{\mathbb{Z}} \mathbb{Z}G$. In particular, a negative solution to (IP) over $\mathbb{Z}$ is a negative solution to (IP) over any R.

The (IP) for integral group rings has a positive solution for:

- abelian groups (Higman '40)
- metabelian groups (Whitcomb '68)
- nilpotent groups (Roggenkamp and Scott '87)
- supersolvable groups (Kimmerle '91)
- ...

Theorem (Hertweck '98)

There are solvable non-isomorphic groups G and H of derived length 4 and order $2^{21}97^{28}$ such that $\mathbb{Z}G \cong \mathbb{Z}H$.

The Modular Isomorphism Problem (MIP). Let k be a field of characteristic $p > 0$ and let G and H be finite p-groups. Is it true that

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

Most classical version of the (IP) that is still open today.

Assumptions from now on.

- p is a prime number,
- $k = \mathbb{F}_p$ is the field of p elements.

Today.

- A look into the history of the (MIP) and known results.
- The (MIP) positively solved for some new families of groups and new group theoretic invariants.

Definitions and notation

Finite p-groups and associated objects

Let G be a finite group. The lower central series of G is

$$\gamma_1(G) = G \text{ and } \gamma_{i+1}(G) = [G, \gamma_i(G)]$$

while the upper central series of G is

$$\mathrm{Z}_0(G) = 1 \text{ and } \mathrm{Z}_{i+1}(G)/\mathrm{Z}_i(G) = \mathrm{Z}(G/\mathrm{Z}_i(G)).$$

The group G is nilpotent if there exists c such that $\gamma_c(G) = 1$ (equivalently $\mathrm{Z}_c(G) = G$). The smallest such c is called the (nilpotency) class of G.

Recall. p-group $\Longrightarrow$ nilpotent

From now on: G is a finite p-group. Then:

- for $m \geq 0$ integer, write $G^{p^m} = \langle g^{p^m} \mid g \in G \rangle$
- the Frattini subgroup of G is $\Phi(G) = \gamma_2(G)G^p$ and satisfies $\mathrm{d}(G) = \log_p |G : \Phi(G)|$.
- The Jennings series (or dimension subgroups) of G is

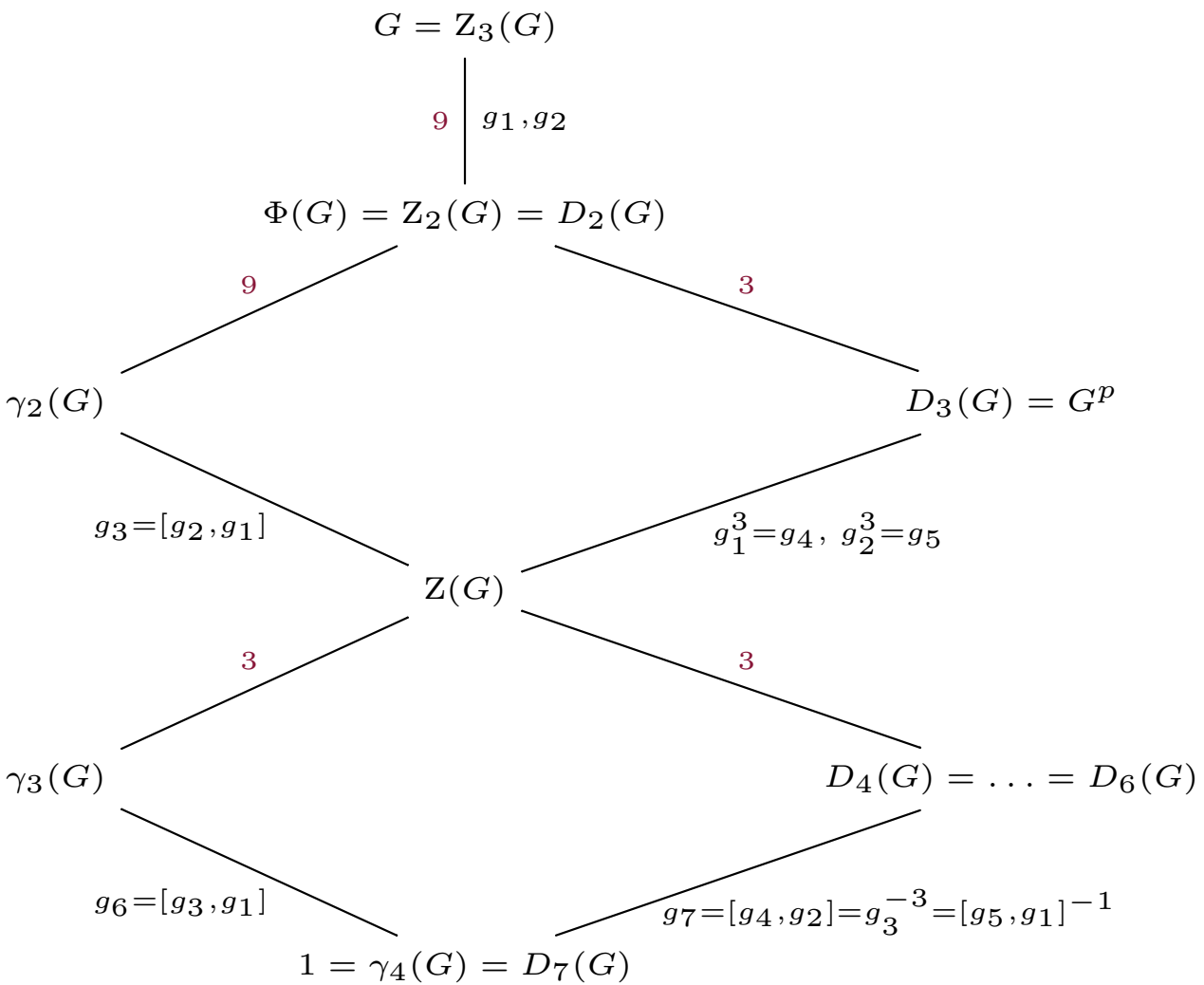
$$D_n(G) = \prod_{ip^j \geq n} \gamma_i(G)^{p^j} = D_{\lceil \frac{n}{p} \rceil}(G)^p \gamma_n(G)$$

and satisfies

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

There exists n such that $D_n(G) = 1$.

$G = \mathrm{SG}(3^7, 19) = \langle g_1, g_2(, g_3, \ldots, g_7) \rangle$ where



The augmentation ideal of kG is

$$I(kG) = \{\sum_{g\in G} \lambda_g g \mid \sum_{g\in G} \lambda_g = 0\} = \langle g-1 : g \in G\rangle \triangleleft kG,$$

which is nilpotent and coincides with the radical of kG.

Reasons to care about this ideal:

- $I(kG)$ is determined by kG and $1 + I(kG) \subseteq U(kG)$
- for each $n \geq 0$, we have $D_n(G) = G \cap (1 + I(kG)^n)$
- we can use bases of the quotients $D_n(G)/D_{n+1}(G)$ to define a Jennings basis of $I(kG)$ respecting the filtration given by the powers of $I(kG)$
- Jennings bases are computationally extremely useful and allow efficient computations in $I(kG)/I(kG)^n$

The Modular Isomorphism Problem

Invariants and positive results

The group G is determined by kG if G:

- has $\gamma_2(G)^p\gamma_3(G) = 1$ (Deskins '56, Coleman '64, Passi, Sehgal '72, Sandling '89)
- has center of index p^2 (Drensky '89)
- is metacyclic (Bagiński '88, Sandling '96)
- is a 2-group of maximal class (Carlson '77, Bagiński '92)
- has odd $|G| \leq p^{p+1}$, max class, and abelian maximal subgroup (Bagiński, Caranti '88)
- is elementary abelian-by-cyclic (Bagiński '99)
- has a cyclic subgroup of index p^2 (Bagiński, Konovalov '05)
- is a 3-group of maximal class, but two families (Bagiński, Kurdics '19)
- is 2-generated of class 2 (Broche, del Rio, '20+)
- is 2-generated with $\gamma_4(G)\gamma_2(G)^p = 1$ (Margolis, Moede '20+)

- has order dividing p^5 (Passman '65, Kovacs, Newman - Salim, Sandling '96)
- has order 2^9 (Makasikis '76, Michler, Newman, O'Brien '87, Wursthorn '93 , Hertweck, Soriano '06, Wursthorn '99, Eick '08, Eick, Konovalov '11)
- has order 3^7 (Eick '08, Margolis, Moede '20+)
- has order 5^6, but a small list (Margolis, Moede '20+)

The group G is determined by kG if G:

- has $\gamma_2(G)^p\gamma_3(G) = 1$ (Deskins '56, Coleman '64, Passi, Sehgal '72, Sandling '89)
- has center of index p^2 (Drensky '89)
- is metacyclic (Bagiński '88, Sandling '96)
- is a 2-group of maximal class (Carlson '77, Bagiński '92)
- has odd $|G| \leq p^{p+1}$, max class, and abelian maximal subgroup (Bagiński, Caranti '88)
- is elementary abelian-by-cyclic (Bagiński '99)
- has a cyclic subgroup of index p^2 (Bagiński, Konovalov '05)
- is a 3-group of maximal class, but two families (Bagiński, Kurdics '19)
- is 2-generated of class 2 (Broche, del Rio, '20+)
- is 2-generated with $\gamma_4(G)\gamma_2(G)^p = 1$ (Margolis, Moede '20+)

- has order p^5 (Passman '65, Kovacs, Newman - Salim, Sandling '96)
- has order 2^9 (Makasikis '76, Michler, Newman, O'Brien '87, Wursthorn '93 , Hertweck, Soriano '06, Wursthorn '99, Eick '08, Eick, Konovalov '11)
- has order 3^7 (Eick '08, Margolis, Moede '20+)
- has order 5^6, but a small list (Margolis, Moede '20+)

A (group) invariant for the (MIP) is a property $\mathcal{P}$ such that

$$kG \cong kH \Longrightarrow \mathcal{P}(G) = \mathcal{P}(H).$$

Some known invariants:

- $|G|$, $\exp(G)$, $[G/\gamma_2(G)]_{\cong}$
- $[G/\Phi(G)]_{\cong} \Longrightarrow \mathrm{d}(G)$
- $[D_n(G)/D_{n+1}(G)]_{\cong}$ (also $n+2$, $2n+1$)
- $[D_n(\gamma_2(G))/D_{n+1}(\gamma_2(G))]_{\cong} \Longrightarrow \mathrm{d}(\gamma_2(G))$
- $[\mathrm{Z}(G)]_{\cong}$, $[\gamma_2(G) \cap \mathrm{Z}(G)]_{\cong}$, $[\mathrm{Z}(G)/(\gamma_2(G) \cap \mathrm{Z}(G))]_{\cong}$
- $[G/\gamma_2(G)^p\gamma_3(G)]_{\cong}$ – the Sandling quotient
- if $\mathrm{d}(G) = 2$, then $[G/\gamma_2(G)^p\gamma_4(G)]_{\cong}$
- ...

Though the class of a p-group is a strong invariant of $[\ldots]_{\cong}$, it is not known whether it is an invariant of kG. Not much is known about the structure of the lower central series either.

Some evidence:

- the class is an invariant, if it is at most 2 or maximal class
- an example suggesting that the lower central series of G does not yield canonical ideals of kG (Bagiński, Kurdics '19)

Example. The groups $G = \mathrm{SG}(3^7, 19)$ and $H = \mathrm{SG}(3^7, 43)$ share all known group theoretical invariants ($\textsc{ModIsomExt}$), but do not satisfy $|\gamma_3(G)| = |\gamma_3(H)|$.

Theorem (Margolis, S. '20+)

Assume p is odd, $\mathrm{d}(G) = 2$, and $\gamma_3(G)^p\gamma_4(G) = 1$. Let H be a p-group such that $kG \cong kH$. Then H has the same class as G and, for each $i \geq 2$, one has $\gamma_i(G) \cong \gamma_i(H)$.

Ingredients of the proof:

- Mix of structural observations and computations
- Argue by contradiction on conveniently chosen Jennings bases coming from G and H
- Identify $kG = kH$ and consider a specific quotient algebra $\mathbb{A}$
- Show that $[\mathbb{A}, \mathbb{A}]\mathbb{A} \cap \mathrm{Z}(\mathbb{A})$ has incompatible properties, when viewed as coming from G or from H.

The small group algebra

Extending techniques of Salim and Sandling

The small group algebra of kG is $kG/I(kG)I(k\gamma_2(G))$.

Applications of the small group algebra:

- Whitcomb's proof for metabelian groups in the integral case
- Determination of Sandling's quotient
- Salim and Sandling's positive solution of the (MIP) for groups of order p^5. It builds upon three main subcases:
  1. groups that are determined by known group theoretical invariants,
  2. groups of maximal class
  3. remaining cases satisfy $\gamma_2(G)^p\gamma_4(G) = 1$ and are determined by the unit group of the small group algebra

We apply similar techniques to positively solve the (MIP) for new classes of groups of order p^6 or p^7.

Theorem (Margolis, S. '20+)

Assume p is odd and $\gamma_2(G)^p\gamma_4(G) = 1$. Then $[G]_{\cong}$ is determined by the small group algebra of kG in the following cases:

- $\mathrm{C}_G(\gamma_2(G))$ *is abelian and maximal in* G,
- $|G : \Phi(G)| = |G : \mathrm{Z}_2(G)| = p^3$ *and one of* $|\gamma_3(G)| = p$ *or* $|\gamma_2(G) : \gamma_2(G) \cap \mathrm{Z}(G)| = p^3$ *holds.*

Comments:

- Relying on James' classification (1980), our result completely covers 5 isoclinism classes of groups of order p^6 (against the 10 covered by previous results).
- Our result covers 68 groups out of 684 groups of order 5^6.
- Also covers 13459 groups out of 34297 groups of order 5^7.

Let S be the subgroup of the normalized units of the small group algebra, i.e. $S \cong (1 + I(kG))/(1 + I(kG)I(k\gamma_2(G)))$.

Let H be another group basis of kG.

- Since $\gamma_2(G)^p\gamma_4(G) = 1$, (a normal copy of) G is complementable in S, i.e. there exists A such that $S = G \rtimes A$,
- show that $S = G \rtimes A = H \rtimes A$
- mod out $\mathrm{Z}(S) \cap A$ and get A elementary abelian
- show that H has a generating set (gotten from a generating set of G via translation by A) satisfying the same relations as a set of generators of G

Example. The groups $G = \mathrm{SG}(5^6, 553)$ and $H = \mathrm{SG}(5^6, 554)$ satisfy $\gamma_2(G)^p\gamma_4(G) = \gamma_2(H)^p\gamma_4(H) = 1$, share all known group theoretical invariants, and the unit groups of the small group algebras of kG and kH are isomorphic.

Other examples in the literature:

- Bagiński '99: groups of order at least p^5, of maximal class with an elementary abelian maximal subgroup
- Hertweck, Soriano '07: groups of order 32 and derived subgroup is cyclic of order 4
- Wursthorn: four groups of order 5^5 and maximal class that have all isomorphic small group algebras

The class of p-obelisks

A new invariant highlighted by computational experiments

A strategy to show that $kG \ncong kH$ is to show that there exists ℓ such that

$$I(kG)/I(kG)^{\ell} \ncong I(kH)/I(kH)^{\ell}.$$

Implementations: Wursthorn '93, Eick '08, Margolis-Moede '20+.

A strategy to show that $kG \ncong kH$ is to show that there exists ℓ such that

$$I(kG)/I(kG)^{\ell} \ncong I(kH)/I(kH)^{\ell}.$$

Implementations: Wursthorn '93, Eick '08, Margolis-Moede '20+.

Question. Let $H \ncong G$ with $|H| = |G|$ and let ℓ be maximal such that $G/D_{\ell}(G) \cong H/D_{\ell}(H)$. Are the following true?

- $I(kG)/I(kG)^{2\ell+1} \ncong I(kH)/I(kH)^{2\ell+1}$
- if p is odd and $m = \max\{\ell, (4\ell - p + 1)/2\}$, then

$$I(kG)/I(kG)^{m+1} \ncong I(kH)/I(kH)^{m+1}$$

A strategy to show that $kG \ncong kH$ is to show that there exists ℓ such that

$$I(kG)/I(kG)^{\ell} \ncong I(kH)/I(kH)^{\ell}.$$

Implementations: Wursthorn '93, Eick '08, Margolis-Moede '20+.

Question. Let $H \ncong G$ with $|H| = |G|$ and let ℓ be maximal such that $G/D_{\ell}(G) \cong H/D_{\ell}(H)$. Are the following true?

- $I(kG)/I(kG)^{2\ell+1} \ncong I(kH)/I(kH)^{2\ell+1}$
- if p is odd and $m = \max\{\ell, (4\ell - p + 1)/2\}$, then

$$I(kG)/I(kG)^{m+1} \ncong I(kH)/I(kH)^{m+1}$$

Question 1 has a negative answer for groups of order 2^8.
Question 2 is open. Family of p-obelisks highlighted by investigation of groups of order 5^6.

Assume that $p > 3$. A p-obelisk is a finite non-abelian p-group $\mathcal{O}$ satisfying $|\mathcal{O} : \gamma_2(\mathcal{O})| = p^2$ and $\mathcal{O}^p = \gamma_3(\mathcal{O})$.

Assume that $p > 3$. A p-obelisk is a finite non-abelian p-group $\mathcal{O}$ satisfying $|\mathcal{O} : \gamma_2(\mathcal{O})| = p^2$ and $\mathcal{O}^p = \gamma_3(\mathcal{O})$.

Some facts:

- there are obelisks of any class.
- for $\omega_i = \log_p |\gamma_i(\mathcal{O}) : \gamma_{i+1}(\mathcal{O})|$, one has $(\omega_i)_{i\geq 1} = (2, 1, \ldots, 2, 1, f, 0, 0, \ldots)$ with $f \in \{0, 1, 2\}$
- normal subgroups of $\mathcal{O}$ are squeezed between elements of the lower central series
- p-obelisks are thin and regular
- for fixed p, there are exactly two infinite limits of p-obelisks

Theorem (Margolis, S. '20+)

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


thank you