UNIVERSIDAD DE MURCIA

ESCUELA INTERNACIONAL DE DOCTORADO

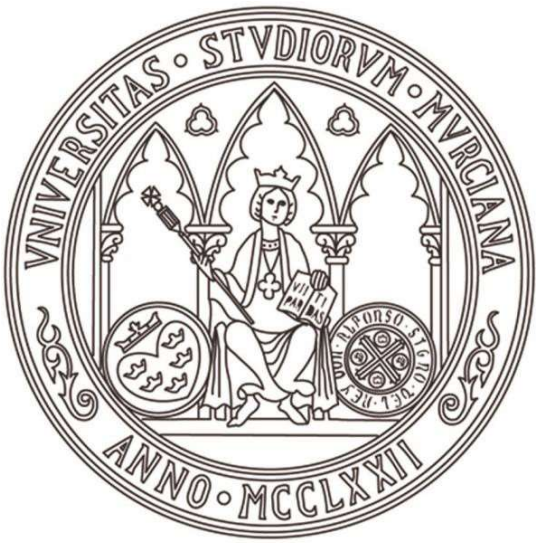
TESIS DOCTORAL

On the modular isomorphism problem

Del problema del isomorfismo modular

D. Diego García Lucas

2024



UNIVERSIDAD DE MURCIA

ESCUELA INTERNACIONAL DE DOCTORADO

TESIS DOCTORAL

On the modular isomorphism problem

Del problema del isomorfismo modular

Autor: D. Diego García Lucas

Director/es: D. Leo Margolis y D. Ángel del Río Mateos

UNIVERSIDAD DE MURCIA

DECLARACIÓN DE AUTORÍA Y ORIGINALIDAD DE LA TESIS PRESENTADA EN MODALIDAD DE COMPENDIO O ARTÍCULOS PARA OBTENER EL TÍTULO DE DOCTOR

Aprobado por la Comisión General de Doctorado el 19-10-2022

D./Dña. Diego García Lucas

doctorando del Programa de Doctorado en

Matemáticas

de la Escuela Internacional de Doctorado de la Universidad Murcia, como autor/a de la tesis presentada para la obtención del título de Doctor y titulada:

On the modular isomorphism problem / Del problema del isomorfismo modular

y dirigida por,

D./Dña. Ángel del Río Mateos

D./Dña. Leo Margolis

D./Dña.

DECLARO QUE:

La tesis es una obra original que no infringe los derechos de propiedad intelectual ni los derechos de propiedad industrial u otros, de acuerdo con el ordenamiento jurídico vigente, en particular, la Ley de Propiedad Intelectual (R.D. legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, modificado por la Ley 2/2019, de 1 de marzo, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia), en particular, las disposiciones referidas al derecho de cita, cuando se han utilizado sus resultados o publicaciones.

Además, al haber sido autorizada como compendio de publicaciones o, tal y como prevé el artículo 29.8 del reglamento, cuenta con:

- *La aceptación por escrito de los coautores de las publicaciones de que el doctorando las presente como parte de la tesis.*
- *En su caso, la renuncia por escrito de los coautores no doctores de dichos trabajos a presentarlos como parte de otras tesis doctorales en la Universidad de Murcia o en cualquier otra universidad.*

Del mismo modo, asumo ante la Universidad cualquier responsabilidad que pudiera derivarse de la autoría o falta de originalidad del contenido de la tesis presentada, en caso de plagio, de conformidad con el ordenamiento jurídico vigente.

En Murcia, a 30 de enero de 2024

Fdo.: Diego García Lucas

Esta DECLARACIÓN DE AUTORÍA Y ORIGINALIDAD debe ser insertada en la primera página de la tesis presentada para la obtención del título de Doctor.

Información básica sobre protección de sus datos personales aportados	
Responsable:	Universidad de Murcia. Avenida teniente Flomesta, 5. Edificio de la Convalecencia. 30003; Murcia. Delegado de Protección de Datos: dpd@um.es
Legitimación:	La Universidad de Murcia se encuentra legitimada para el tratamiento de sus datos por ser necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. art. 6.1.c) del Reglamento General de Protección de Datos
Finalidad:	Gestionar su declaración de autoría y originalidad
Destinatarios:	No se prevén comunicaciones de datos
Derechos:	Los interesados pueden ejercer sus derechos de acceso, rectificación, cancelación, oposición, limitación del tratamiento, olvido y portabilidad a través del procedimiento establecido a tal efecto en el Registro Electrónico o mediante la presentación de la correspondiente solicitud en las Oficinas de Asistencia en Materia de Registro de la Universidad de Murcia

Un resumen

Entre las preguntas que surgen en el estudio de los anillos de grupo, una de las más populares es el *problema del isomorfismo*. Y entre las variantes de ésta, la que más tiempo ha resistido a una solución es el *problema del isomorfismo modular*. Éste pregunta si, dados dos p-grupos finitos G y H, la existencia de un isomorfismo entre las álgebras de grupo de G y de H sobre el cuerpo de p elementos (o, alternativamente, sobre algún cuerpo de característica p) implica la existencia de un isomorfismo entre G y H. Este problema ya apareció en el influyente artículo de recopilación de R. Brauer *Representations of finite groups* de 1963, y para el que los primeros resultados parciales se remontan a un trabajo de W. E. Deskins de 1956. A pesar de haber recibido un interés más o menos continuado durante las décadas subsiguientes, este problema sólo había recibido soluciones parciales positivas restringidas a clases de p-grupos finitos específicas, como la clase de los p-grupos abelianos (el mencionado resultado de Deskins), la clase de los p-grupos de clase de nilpotencia 2 y subgrupo derivado elemental abeliano (un resultado debido a R. Sandling de 1989) o la clase de los grupos metacíclicos (debido para p mayor que 3 a C. Bagiński en 1989, y completado por R. Sandling para p un número primo arbitrario en 1996). También es sabido que el problema del isomorfismo modular tiene respuesta positiva para grupos de orden pequeño: Passman demostró en 1965 que el problema tiene respuesta positiva para grupos de orden divisor de p^4 para cualquier primo p, y este resultado fue extendido para grupos de order p^5 por M. A. M. Salim y R. Sandling. Con ayuda de ordenadores, el mismo resultado se ha probado para grupos de orden divisor de 2^8, de 3^7 o, con unas pocas excepciones, de 5^6 (en distintos trabajos de M. Wursthorn, B. Eick, L. Margolis y T. Moede, entre 1993 y 2022).

Nuestra contribución a esta área consiste en un estudio concienzudo del problema del isomorfismo modular para p-grupos finitos 2-generados con subgrupo derivado cíclico, llevado a cabo en las Partes III y IV, con el que demostramos que este problema tiene respuesta positiva para algunas subclases de esta clase de grupos, y demostramos que ciertos invariantes de estos grupos están determinados por sus álgebras de grupo modulares. Un prerrequisito para este estudio era tener clasificados, salvo isomorfismo, los grupos de nuestra clase objetivo, que se realiza en la Parte I. Esta clasificación consiste en en una biyección entre el conjunto de las clases de isomorfía de estos grupos y un cierto conjunto de 12-tuplas de números enteros. Como parte del mencionado estudio del problema del isomorfismo modular para esta clase de grupos, en la Parte II, somos capaces de dar una respuesta negativa al problema del isomorfismo modular, cerrando finalmente los sesenta años de historia de este problema. Más concretamente, encontramos una familia infinita de pares de 2-grupos G y H no isomorfos cuyas álgebras de grupo FG y FH sobre un cuerpo F de característica 2 arbitrario son isomorfas. Sin embargo, el problema del isomorfismo modular sigue siendo una pregunta de interés para algunas clases de grupos, como los p-grupos de orden impar (i.e., con p mayor que 2) o los p-grupos de clase de nilpotencia 2. En la primera dirección destacamos que nuestros esfuerzos en las Partes III y IV muestran que no es posible encontrar, al menos en un sentido naíf, un análogo al contraejemplo de la Parte II cuando p es mayor que 2. En la segunda dirección, en la Parte V damos una respuesta positiva al problema del isomorfismo modular para p-grupos de clase de nilpotencia 2 con centro cíclico. Si además admitimos cuerpos arbitrarios en el enunciado del problema del isomorfismo modular, también damos una respuesta positiva cuando p es impar, pero cuando p es 2 necesitamos hacer una suposición adicional o bien sobre el cuerpo o bien sobre los grupos para obtener una respuesta positiva. Desde un punto de vista más estructural, en la Parte VI demostramos que el problema del isomorfismo modular es equivalente al mismo problema para p-grupos sin factores directos abelianos. Esto nos permite extender de forma no trivial las clases de grupos para las que se conoce que el problema del isomorfismo modular tiene respuesta positiva. En la Parte VII demostramos que, para el problema del isomorfismo modular en su versión para cuerpos arbitrarios, de hecho sólo los cuerpos finitos pueden tener relevancia.

La tesis formalmente consiste en un preámbulo doble y siete partes, cada parte formada por o bien un artículo publicado o bien un *preprint*. El preámbulo se divide en una introducción, donde se presenta el problema del isomorfismo para álgebras de grupo, con especial énfasis en el problema del isomorfismo modular y los resultados conocidos sobre el mismo que no forman parte de esta tesis, y en una sección de resultados, donde los resultados originales que conforman esta tesis se presentan y se ponen en contexto. Las siete partes restantes constituyen el cuerpo principal de la tesis: seis de ellas (las Partes I,II, III, VI y VII) consisten en artículos ya publicados, y aparecen exactamente en el mismo formato en el que lo han sido. La parte restante consiste en un *preprint* no publicado, ya disponible *online* en el mismo formato en que aquí aparece, y en proceso de revisión para ser publicado. A continuación incluimos una lista de estas partes junto con sus resúmenes y sus correspondientes referencias, o, en su caso, su identificador en arXiv.

- Parte I. *A classification of the finite 2-generator cyclic-by-abelian groups of prime-power order*, en colaboración con Osnel Broche Cristo y Ángel del Río Mateos. International Journal of Algebra and Computation, 33 no. 04 (2023) 641-686.

  Resumen: En este artículo clasificamos los grupos finitos cuyo subgrupo derivado es cíclico, que están generados por dos elementos y cuyo orden es potencia de un primo. Para ello, asociamos a cada G en esas condiciones una lista $\mathrm{inv}(G)$ de invariantes númericos que determina la clase de isomorfía del grupo G. A continuación, describimos el conjunto formado por todos los posible valores de $\mathrm{inv}(G)$. Esto nos permite desarrollar algoritmos prácticos que permiten construir todos los grupos finitos no abelianos con subgrupo derivado cíclico generados por dos elementos de orden una potencia de un primo fijada, calcular el vector de invariantes de un grupo tal, y decidir si dos grupos tales dados son o no isomorfos.

- Parte II. *Non-isomorphic 2-groups with isomorphic modular group* , en colaboración con Leo Margolis y Ángel del Río Mateos. Journal fur die Reine und Angewandte Mathematik, 783 (2022) 269-274. doi.org/10.1515/crelle-2021-0074

  Resumen: En este artículo presentamos una familia de 2-grupos finitos no isomorfos que tienen álgebras de grupo isomorfas sobre cada cuerpo de característica 2, dando así respuesta al problema del isomorfismo modular.

- Parte III. *On group invariants determined by modular group algebras: Even versus odd characteristic*, en colaboración con Ángel del Río Mateos y Mima Stanojkovski. Algebras and Representation Theory. doi.org/10.1007/s10468-022-10182-x

  Resumen: Sea p un primo distinto de 2 y sea G un p-grupo finito con subgrupo conmutador cíclico. En este artículo demostramos que el exponente y el abelianizado del centralizador $\mathrm{C}_G(G')$ del subgrupo derivado en G están determinados por el álgebra de grupo de G sobre cualquier cuerpo de característica p. Si, adicionalmente, G está generado por dos elementos, entonces casi todos los invariantes numéricos que determinan G salvo isomorfismos están determinados por las mencionadas álgebras de grupo; como consecuencia, la clase de isomorfía del centralizador en G del subgrupo derivado de G está determinada por el álgebra de grupo. Es sabido que todas estas afirmaciones son falsas para p igual a 2.

- Parte IV. *On the Modular Isomorphism Problem for 2-generated groups with cyclic derived subgroup*, en colaboración con Ángel del Río Mateos. *Preprint* arXiv:2310.02627

  Resumen: En este *preprint* continuamos el análisis del problema del isomorfismo modular para los grupos con subgrupo derivado cíclico, que están generados por dos elementos, y cuyo orden es una potencia de un primo p mayor que dos, iniciado en la Parte III. En él demostramos que si G pertenece a esta clase de grupos, entonces la clases de isomorfía de los cocientes $G/(G')^{p^3}$ y $G/\gamma_3(G)^p$ están determinadas por el álgebra de grupo modular de G. De hecho, obtenemos un resultado más general pero bastante más técnico, en términos de la clasificación de los grupos de la mencionada clase descrita en la Parte I. También mostramos que para los grupos en esta clase de orden no mayor que p^{11}, el problema del isomorfismo modular tiene respuesta positiva. Finalmente, describimos algunas familias de grupos de orden p^{12} cuyas álgebras de grupo sobre el cuerpo de p elementos no pueden ser distinguidas utilizando las técnicas de las que disponemos.

- Parte V *On the modular isomorphism problem for groups of nilpotency class 2 with cyclic center*, en colaboración con Leo Margolis. Forum Mathematicum, 2024. doi.org/10.1515/forum-2023-0237

  Resumen: En este artículo demostramos que el problema del isomorfismo modular tiene respuesta positiva para grupos de clase de nilpotencia 2 con centro cíclico, i.e., que para p-grupos G y H en las mencionadas condiciones, la existencia de un isomorfismo entre las álgebras de grupo FG y FH implica la existencia de un isomorfismo entre los grupos G y H, donde F es el cuerpo de p elementos. Para grupos de orden impar, esta implicación también se demuestra cuando F es un cuerpo arbitrario de característica p. Para grupos de orden par, necesitamos o bien añadir una hipótesis adicional, o bien sobre los grupos o bien sobre el cuerpo.

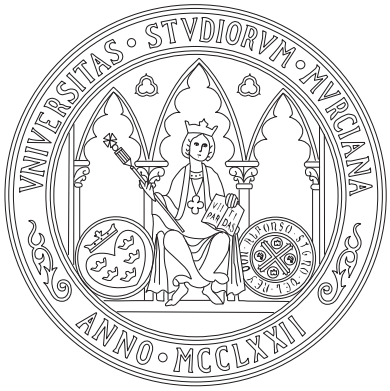
- Parte VI. *The modular isomorphism problem and abelian direct factors.* Mediterranean Journal of Mathematics. 21, 18 (2024). doi.org/10.1007/s00009-023-02557-1

  Resumen: Sea p un número primo y sea G un grupo de orden potencia de p. En este artículo demostramos que tanto la clase de isomorfía el factor directo maximal de G como la clase de isomorfía del álgebra de grupo sobre el cuerpo de p elementos $\mathbb{F}_p$ factor directo no abeliano restante, si existiese, están determinadas por el álgebra de grupo $\mathbb{F}_pG$. Esto generaliza un resultado de L. Margolis, T. Sakurai y M. Stanojkovski (Abelian invariants and a reduction theorem for the modular isomorphism problem, Journal of Algebra 636, 533-559 (2023)) subre el cuerpo primo. Con el fin de lograr esto, abordamos el probleam de encontrar subgrupos característicos de G tales que sus ideales de aumento relativos dependan sólo de la clase ed isomorfía del álgebra de grupo kG, donde k es un cuerpo de característica p arbitrario, y lo relacionamos con el problema del isomorfismo modular, extendiendo y dando pruebas alternativas a algunos resultados ya existentes.

- Parte VII. *A reduction theorem for the Isomorphism Problem of group algebras over fields*, en colaboración con Ángel del Río Mateos. Journal of Pure and Applied Algebra 228 (2024), no. 4, 107511.

  Resumen: En este artículo demostramos que el problema del isomorfismo para álgebras de grupo se reduce al mismo problema restringido a álgebras de grupo sobre extensiones finitas del cuerpo primo. En particular, el problema del isomorfismo modular se reduce al mismo problema sobre álgebras de grupo modulares finitas.

Esta tesis ha sido elaborada durante el periodo de disfrute de una beca de Formación del Profesorado Universitario del Plan Propio de Fomento de la Investigación de la Universidad de Murcia (convocatoria de 2020), además de, durante los primeros dos meses, de una Ayuda de Iniciación de la Investigación del Plan Propio de Fomento de la Investigación de la Universidad de Murcia (convocatoria de 2020). Además, se ha contado con ayudas económicas parciales de la Escuela Internacional de Doctorado de la Universidad de Murcia para la asistencia a congresos y para una estancia corta. Esta investigación también ha estado financiada parcialmente por el proyecto "Methods in noncommutative Algebra and applications " (Proyecto I+D+i PID2020-113206GB-I00 financiado por MCIN/ AEI/10.13039/501100011033/) y por el proyecto "Teoría y aplicaciones del Álgebra no conmutativa"(Proyecto 22004/PI/22 financiado por Fundación Séneca (CARM)).



UNIVERSIDAD DE MURCIA

ESCUELA INTERNACIONAL DE DOCTORADO

TESIS DOCTORAL

On the modular isomorphism problem

or some partial positive solutions, a negative solution,
and a pair of reductions for the question of whether
the isomorphism class of a finite p-group is determined by
its modular group algebra.

Del problema del isomorfismo modular

o algunas soluciones parciales positivas, una solución negativa
y un par de reducciones para la pregunta de si
la clase de isomorfía de un p-grupo finito está determinada por
su álgebra de grupo modular.

Diego García Lucas

Abstract

Among the questions that arise in the study of group rings, one of the most popular is the so called isomorphism problem. And among its variants, the one that remained unsolved the longer is the modular isomorphism problem. It asks whether, given two finite p-groups G and H, the existence of an isomorphism between the group algebras of G and H over the field with p elements (or, alternatively, any field of characteristic p) implies the existence of an isomorphism between G and H themselves. This problem already appeared in R. Brauer's influential 1963 survey *Representations of finite groups*, and the first partial positive result goes back to 1956, to the work of W. E. Deskins.

Our contribution to this issue consists in a thorough study of the modular isomorphism problem for 2-generated p-groups with cyclic derived subgroup, performed in Parts III and IV, in which we prove that this problem has positive answer for some subclasses of this classes of groups, and we show that certain group theoretical invariants are determined by the group algebra. A prerequisite to this was to have the target class of groups classified up to isomorphism, and this is achieved in Part I. As part of this study, in Part II, we are able to answer the modular isomorphism problem in the negative, finally closing this sixty years old problem. Nevertheless, the modular isomorphism problem remains a question of interest for several classes of p-groups, such as the p-groups of odd order (i.e., with $p > 2$) or the p-groups with nilpotency class 2. In this last direction, in V we give a positive answer to the modular isomorphism problem for p-groups of nilpotency class 2 with cyclic center. From a more structural point of view, in Part VI we show that modular isomorphism problem is equivalent to the same problem for p-groups without abelian direct factors. This allows us to extend non-trivially the classes of groups of which the modular isomorphism problem is known to have positive answer. In Part VII we show that for the modular isomorphism problem in its version for arbitrary fields, actually only finite fields matter.

Formally, the thesis consists in a twofold preamble, and seven parts, each part constituted by a published paper or a preprint. The preamble consists in an introduction, where the isomorphism problem for group rings is presented, with special emphasis on the modular isomorphism problem; and in a section of results, where the original contributions of this thesis are described and put in context. The remaining seven parts constitute the main body of the thesis: six of them (Parts I, II, III, VI, and VII) consist in already published papers, and they appear in exactly the same format they were published. The remaining part consists in an unpublished preprint, already submitted for publication and made available online exactly in the same format it appears here. Next we include a list of these parts together with the corresponding journal references, or in its case the arXiv identification.

- Part I. *A classification of the finite 2-generator cyclic-by-abelian groups of prime-power order*, joint with Osnel Broche and Ángel del Río. International Journal of Algebra and Computation, 33 no. 04 (2023) 641-686. dx.doi.org/10.1142/S0218196723500297
- Part II. *Non-isomorphic 2-groups with isomorphic modular group*, joint with Leo Margolis and Ángel del Río. Journal fur die Reine und Angewandte Mathematik, 783 (2022) 269-274. doi.org/10.1515/crelle-2021-0074
- Part III. *On group invariants determined by modular group algebras: Even versus odd characteristic*, joint with Ángel del Río and Mima Stanojkovski. Algebras and Representation Theory. doi.org/10.1007/s10468-022-10182-x
- Part IV. *On the Modular Isomorphism Problem for 2-generated groups with cyclic derived subgroup*, joint with Ángel del Río. arXiv:2310.02627

- Part V *On the modular isomorphism problem for groups of nilpotency class 2 with cyclic center*, joint with Leo Margolis. Forum Mathematicum, 2024. doi.org/10.1515/forum-2023-0237
- Part VI. *The modular isomorphism problem and abelian direct factors.* Mediterr. J. Math. 21, 18 (2024). doi.org/10.1007/s00009-023-02557-1
- Part VII. *A reduction theorem for the isomorphism problem of group algebras over fields*, joint with Ángel del Río. Journal of Pure and Applied Algebra 228 (2024), no. 4, 107511. doi.org/10.1016/j.jpaa.2023.107511

Prolegomena

I feel compelled to say a word about the choice of format of this thesis: namely, this is a thesis by compendium (i.e., that consists in a short introduction and several published papers or preprints), instead of a thesis in the traditional sense. The main reason of this choice is, of course, that it was an option, and I was lucky enough to fulfill the requisites by the time I had to make the decision. Other reason is that most of the background content that should be included in any thesis that addresses the modular isomorphism, e.g., the theory Jennings for modular group algebras of finite p-groups, or a detailed account of the pre-existing results and techniques related to this problem, is already contained in my master's thesis. Though unfortunately this thesis is written in Spanish, and contains a number of typos and mistakes, as well as a certain lack of insight, its existence made much less appealing to me to rewrite and translate all that material, and more attractive to focus on obtaining new results. And a thesis by compendium was the ideal choice for this goal. Moreover, the contents of the different papers actually fit as chapters of a single work: Part II, Part III, and its direct continuation Part IV, provide a thorough study of the modular isomorphism problem for the class of p-groups described in Part I. Part V gives positive answer to this problem for other reasonably nice class of groups (also with cyclic derived subgroup). Finally, Parts VI and VII provide reductions to the modular isomorphism problem from two different points of view.

However, this format of thesis comes with some unpleasant unavoidable features: each paper or preprint comes with its own format and numeration (if the paper is published, the one of the corresponding journal). In an attempt to mitigate the confusion that a double page numeration entails, the page number correspondent to the pagination of the thesis will always be situated at the bottom-center of the page, and preceded by the word page, anti-aesthetic as it might be. Moreover, each paper comes with an introduction, and, when read in a row, they become quite repetitive and discouraging for the reader. I apologize for that.

I would like to express my gratitude to my advisors Ángel del Río and Leo Margolis, for their guidance, support and patience during these years. Without them this thesis would not be, and almost surely I would never had developed any interest in group rings. I read recently in the preface of *Modules and group algebras*, by J. F. Carlson, that "There is a legendary story that Brauer, himself, used to advise his students to try to study the representation theory of p-groups. The subject seemed to be too difficult with little or no promise of productive results." And this thesis can act as a witness of this difficulty: the initial goal was to study the modular isomorphism problem for 2-generated finite p-groups with cyclic derived subgroup, and despite the intense work these years and some major advances in Part III and Part IV, for $p > 2$ this question remains far from being answered. However, other interesting projects appeared and some fortuitous and fortunate results were obtained (all of them related to the modular isomorphism problem), and I can say that I am satisfied with the final configuration (from the third title-page onward) of this thesis. So, I am glad they did not follow His lead.

Aside from Ángel and Leo, I am specially grateful to the other two coauthors of the papers that form this thesis: Osnel Broche and Mima Stanojkovski. It is tautological to say that without them this thesis would not be as it is. I am also grateful to Sofia Brenner, with whom I recently found some results on the topic of this thesis, mentioned in the introduction, but that could not be properly included as an eighth part.

I am grateful to Benjamin Sambale and the Institut für Algebra, Zahlentheorie und Diskrete Mathematik at Leibniz Universität Hannover, for their hospitality during my three months visit in 2022, as well to the Instituto de Ciencias Matemáticas (ICMAT) for its hospitality during my two short visits to work with Leo Margolis. Also to Jon González Sánchez, and rest of the members of the Groups, Toplogy and Applications research group at the University of the Basque Country University for their hospitality and generosity during my one month visit there. I am grateful too to the members of the Algebra group of the University of Murcia,

specially Àngel García Blàzquez and Sara C. Debón, for the shared travels and paperwork.

Finally, I am grateful to the external evaluators of this thesis, Czesław Bagiński and Bettina Eick, for taking the time to read it and for their reports, and to the members of the tribunal: Florian Eisele, Sergio Estrada Domínguez, and Gustavo Fernández Alcober.

Contents

Introduction

1 The isomorphism problem for group algebras

Let G be a group and let R be a commutative ring. The *group algebra* of G over R, denoted RG, is the R-algebra whose elements are formal linear combinations of elements of G with coefficients in R, i.e., elements of the form

$$\sum_{g\in G} a_g g, \qquad (a_g \in R,\ a_g = 0 \text{ for each } g \in G \text{ except for a finite amount of them}),$$

with the obvious sum and R-action, and the multiplication given by the operation in the group and the multiplication in the ring, $(rg)\cdot(sh) = (rs)\cdot gh$ for $r, s \in R$ and $g, h \in G$, extended by linearity. Then G is a basis of RG as a free RG-module. This structure plays a fundamental rôle in the study of the representation theory of the group G over the ring R, and has raised considerable, and consistent thorough time, interest, with several books like [Pas77, Seh78, Pas79, Seh93, PMS02, JdR16] devoted to its study. One of the most natural questions about group rings, and arguably the most popular, is the-so called isomorphism problem. It asks whether the isomorphism type of the group G is determined by that of the group algebra RG as an R-algebra. Formally:

Problem 1.1 (Isomorphism problem)**.** *Let R be a commutative ring and G and H finite groups. Does $RG \cong RH$ imply $G \cong H$?*

Throughout this thesis we use standard notation: $RG \cong RH$ means that RG is isomorphic to RH as an R-algebra, and $G \cong H$ means that G is isomorphic to H as a group. Furthermore, we will only consider group algebras of finite groups. Let $\tilde{G}$ be a subgroup of the group of unit of RG that is at the same time a basis of RG as a free R-module. Then $\tilde{G}$ is called a *group basis* of RG. Since G and $\tilde{G}$ have the same cardinality, by the universal property of the group ring there is an isomorphism $R\hat{G} \cong RG$. Thus Problem 1.1 is equivalent to the question: Is every group basis of RG isomorphic to G?

Problem 1.1, under the additional hypothesis that R is a field, appears in R. Brauer's survey on representations of finite groups [Bra63] as Problem 2. A version of this question can be traced back to the decade of 1940, when, according to [PW50], the problem "given a finite group G and a field R, determine all the groups H such that $RG \cong RH$" was proposed by R. M. Thrall at the Michigan Algebra Conference in the summer of 1947. Examples of groups and rings for which Problem 1.1 has negative answer are easy to find: take $R = \mathbb{C}$ and G and H two non-isomorphic abelian groups of the same order. Then $\mathbb{C}G \cong \mathbb{C}H$. Thus, the problem becomes more a problem about finding the right combination of chosen ring and extra properties to impose on the groups, for which Problem 1.1 has positive answer. In this sense, if one chooses not to impose additional conditions on the groups, it is natural to make the ring vary on a nice class of rings. For example, for R varying in the class of all fields, the problem is Problem 2^* in [Bra63]:

Problem 1.2 (Isomorphism problem for all fields)**.** *Let G and H be finite groups. Does $kG \cong kH$ for every field k imply that $G \cong H$?*

Despite the apparently strong antecedent in the implication of Problem 1.2, less than a decade since Brauer's survey, E. Dade found couples of metabelian groups of order p^3q^6, for p and q two different primes, with isomorphic group algebras over every field [Dad71]. Then, if one still wants not to impose extra condition on the group, a wider class of commutative rings than the class of all fields is needed. This leads to the following:

Problem 1.3 (Isomorphism problem for all rings)**.** *Let G and H be finite groups. Does $RG \cong RH$ for every commutative ring R imply that $G \cong H$?*

Since every commutative ring R can be seen as a $\mathbb{Z}$-module, tensorizing we obtain that $RG \cong R \otimes_{\mathbb{Z}} \mathbb{Z}G$. Therefore $\mathbb{Z}G \cong \mathbb{Z}H$ if and only if $RG \cong RH$ for every commutative ring R. This implies that Problem 1.3 is equivalent to:

Problem 1.4 (Integral isomorphism problem)**.** *Let G and H be finite groups. Does $\mathbb{Z}G \cong \mathbb{Z}H$ imply that $G \cong H$?*

This version of the question is mentioned in G. Higman's thesis [Hig40] in the following terms: "Whether it is possible for two non-isomorphic groups to have isomorphic integral group rings I do not know; but the results of section 5 suggest that it is unlikely". Since then, it has attracted a lot of interest, and lead to a number of significant positive partial results, which we summarize in the following theorem:

Theorem 1.5. *Problem 1.4 has positive answer provided that G and H belong to one of the following classes of groups:*

(1) Abelian groups [Hig40].

(2) Metabelian groups [Whi68]

(3) Abelian-by-nilpotent groups [RS87].

(4) Supersolvable groups [Kim91].

(5) Frobenius groups and 2-Frobenius groups [Kim91].

(6) Nilpotent-by-abelian groups [RT92].

Observe that the different items in the previous theorem are not independent. For example, the class of abelian groups is contained in the class of metabelian groups. We include all of them to illustrate the progress on the problem throughout time.

Despite these considerable advances, M. Herweck [Her01] found two non-isomorphic groups of order $2^{21}97^{28}$ with isomorphic group algebras over the integers (and hence over every commutative ring) in 2001, sixty years after G. Higman's thesis. Many other interesting problems raised in the study of group algebras of finite groups over the integers, such as the Zassenhaus conjectures, or weakened versions of the isomorphism problem, such as the spectrum problem (we suggest the surveys [Md19, PM22] for an overview on these questions).

2 The modular isomorphism problem

More than twenty years before M. Hertweck's examples were found, in [Pas77] D. Passman wrote about Problem 1.1, and apropos E. Dade's counterexamples mentioned above, that "There are, however, two glimmers of hope. The first concerns integral group rings, and the second concerns p-groups over $GF(p)$." This second glimmer of hope (and the only one remaining after M. Hertweck faded away the first) is the modular isomorphism problem, the main topic of this thesis:

Problem 2.1 (Modular isomorphism problem)**.** *Let p be a prime, let k be the field with p elements, and let G and H finite p-groups. Does $kG \cong kH$ imply $G \cong H$?*

Some authors (e.g. [Dre89]) considered a version of this problem substituting the field of p elements by an arbitrary field of characteristic p, raising the question:

Problem 2.2 (k-modular isomorphism problem)**.** *Let p be a prime, let k be a field of characteristic p and let G and H be finite p-groups. Does $kG \cong kH$ imply $G \cong H$?*

We shall sometimes refer to these problem also by the initials MIP and k-MIP, respectively. Since every field k of characteristic p is a vector space over its prime field k_0, there is an isomorphism $kG \cong k \otimes_{k_0} k_0 G$. Therefore, a positive answer to Problem 2.2 for some field k implies a positive answer to Problem 2.1.

The history of Problem 2.1 starts in [Des56], where W. E. Deskins answers the question in the positive for finite abelian p-groups. In the "Supplements" of [Bra63], R. Brauer writes "Jennings' results allow us to define many numerical invariants of p-groups over the prime fields of characteristic p by counting the number of elements of a power of the radical which satisfy given conditions. This suggests that it may be much easier to study Problem 2 for this particular case." These results of S. A. Jennings [Jen41] consist, mainly, in a method to construct bases $\mathscr{B}$ of kG, where k is a field of characteristic p and G a finite p-group, which are compatible with the filtration of ideals $I \supseteq I^2 \supseteq I^3 \supseteq \dots$, where I is the Jacobson radical of kG. That is, $\mathscr{B} \cap I^n$ is a basis of I^n, for each n. The construction of these bases relies in a series of normal subgroups $(\mathrm{D}_n(G))_{n\geq 1}$ of G called the *Jennings series*, or *the Brauer-Jennings-Zassenhaus series*, of G, defined as follows. Given an arbitrary group G, we set

$$\begin{aligned} \mathrm{D}_1(G) &= G, \\ \mathrm{D}_{n+1}(G) &= [G, \mathrm{D}_n(G)]\mathfrak{V}_1(\mathrm{D}_i(G)), \qquad \text{for } n \geq 2, \end{aligned}$$

where in each step i is the smallest integer greater or equal than n/p. Here $\mathfrak{V}_j(G)$ denotes the subgroup of G generated by the p^j-powers of the elements of G for each $j \geq 0$, and given two subgroups N_1 and N_2 of G, $[N_1, N_2]$ denotes the subgroup of G generated by the elements of the form $[n_1, n_2] = n_1^{-1} n_2^{-1} n_1 n_2$, with $n_1 \in N_1$ and $n_2 \in N_2$. These series of subgroups admit the alternative characterization, due to M. Lazard [Laz54],

$$\mathrm{D}_n(G) = \prod_{ip^j \geq n} \mathfrak{V}_j(\gamma_i(G))$$

for each $n \geq 1$, where $\gamma_i(G)$ denotes the i-th term of the lower central series of G. If G is a p-group, then the second term of the Jenning series is the Frattini subgroup $\Phi(G) = \mathrm{D}_2(G) = \mathfrak{V}_1(G)\gamma_2(G)$ of G, and the series coincide with the series of dimension subgroups of G, i.e., for each $n \geq 1$,

$$\mathrm{D}_n(G) = G \cap (1 + I^n).$$

This last result is also due to S. A. Jennings [Jen41]. A detailed account of these topics can be found in [Pas77, Section 11.1].

Despite R. Brauer's initial optimism, Problem 2.1 turned out to be considerably difficult, and only partial positive results were obtained, limited to very restrictive classes of p-groups. In the next two theorems we list all the partial results that are not part of this thesis. An almost identical list can be found in [Mar22, Section 3].

Theorem 2.3. *Problem 2.2 has positive answer provided that G belongs to at least one of the following classes of finite p-groups:*

(1) Abelian p-groups [Des56].

(2) 2-groups of maximal class [Car77][1]*.*

(3) Groups with center of index p^2 [Dre89].

(4) Metacyclic groups [Bag88, San96][2]*.*

(5) Groups of order 32 [NS18].

[1] J. F. Carlson gave a module theoretic proof in [Car77]; years later C. Bagiński provided an alternative proof working inside the modular group algebra. A third proof appeared in [RV13]

[2] C. Bagiński proved this result for $p > 2$, and R. Sandling gave a general proof for every prime p. Both results are stated for the prime field, but the arguments of the later work for every base field of the same characteristic. Some other results in these lists were originaly stated only for the prime field, but with the same arguments, or a very slight variation of them, are valid for arbitrary fields of the same characteristic. We present them in the most general version without further comment.

(6) 2*-generated groups of class* 2 *for* p *odd [BdR21].*

(7) 2*-groups of nilpotency class* 3 *such that* $|G : \mathcal{Z}(G)| = |\Phi(G)| = 8$*. [MSS23].*

(8) 2*-groups with cyclic center such that* $G/\mathcal{Z}(G)$ *is dihedral [MSS23].*

In this theorem (and for the rest of the thesis) $\mathcal{Z}(G)$ denotes the center of the group G. Moreover, for any integer $n \geq 0$, $\Omega_n(G)$ denotes the subgroup of G generated by the elements g of G such that $g^{p^n} = 1$.

Theorem 2.4. *Problem 2.1 has positive answer provided that* G *belongs to at least one of the following classes of finite* p*-groups:*

(1) Groups of order dividing p^5 *[Pas65, SS96a].*

(2) Groups of order 2^6 *[HS06].*

(3) Groups with $\mathrm{D}_3(G) = 1$ *[PS72].*

(4) Groups with $\mathrm{D}_4(G) = 1$*, if* $p > 2$ *[Her07].*

(5) Groups of maximal class and order at most p^{p+1} *which contain a maximal subgroup which is abelian [BC88].*

(6) 3*-groups of maximal class, except for a single family of groups [BK19].*

(7) Groups containing a cyclic subgroup of index p^2 *[BK07].*

(8) 2*-generated groups of nilpotency class* 2 *[BdR21].*

(9) Groups of nilpotency class 2 *with elementary abelian derived subgroup [San89].*

(10) 2*-generated groups of nilpotency class* 3 *and elementary abelian derived subgroup [MM22].*

(11) Groups of nilpotency class 3 *with elementary abelian derived subgroup and such that* $C_G(\gamma_2(G))$*, the centralizer in* G *of the derived subgroup* $\gamma_2(G)$*, is abelian and maximal in* G *[MS22].*

(12) Groups of order dividing 2^8 *or* 3^7 *[Wur93, BKRW99, Eic08, MM22].*

(13) Groups of order 5^6*, except for six families of groups, each one of size at most* 4 *[MM22].*

(14) Groups of the form F/N*, where* F *is a free group of finite rank and* $\mathrm{D}_{i+2}(F) \subseteq N \subseteq \mathrm{D}_{i+1}(F)$ *for some integer* $i \geq 1$ *[Rö90] (see also [HS07, Theorem 5.8]).*

There exist two main strategies (cf. the introduction of [Her07]) to attack the modular isomorphism problem, both of them with strong limitations. The first one consists in attacking the problem for a concrete class of groups which is already classified, i.e., there exists a non-redundant list of the isomorphism types groups in the class, maybe parametrized somehow. Then the problem consists in proving that the group algebra of each of the groups in the list is not isomorphic to the group algebra of the others. This is the approach followed in the aforesaid result of W. E. Deskins, and also in the positive answer of D. S. Passman for groups of order dividing p^4 [Pas65]. The remainder of the results in Theorem 2.3 can also be seen as a result of this approach. Moreover, all the results obtained with computational help lie in this category. Of course, this approach entails the need of a deep knowledge of the groups one is working with. Since a classification of all finite p-groups is hopelessly out of question, this strategy was never meant to provide a definitive positive answer to Problem 2.1, but, at best, to isolate possible counterexamples.

Recall that a group theoretical invariant of a group G is a feature of G depending only on the isomorphism type of G. A group theoretical invariant of a p-group is *determined by its modular group algebra in a class of groups* $\mathcal{C}$, or simply *determined* in the class $\mathcal{C}$, if any two p-groups belonging to $\mathcal{C}$ with isomorphic group algebras share this invariant. When $\mathcal{C}$ is the class of all finite p-groups, we just say that the invariant is *determined*. Finding and using invariants of this type has been key in the success of this approach, which, usually, reduces to show that the isomorphism type of a group is determined by a set of apparently weaker group-theoretical invariants that, in turn, are determined by the modular group algebra. We give a list of invariants of this kind that are not part of the results of the thesis in the following theorem (cf. [MM22, Theorem 2.1]).

Theorem 2.5. *Let p be prime, k a field of characteristic p, and let G be a finite p-group. The following group theoretical invariants of G are determined by the group algebra kG.*

(1) The isomorphism type of $G/\gamma_2(G)$ [Col64].

(2) The isomorphism type of $\mathcal{Z}(G)$. [War61].

(3) The isomorphism type of $\mathrm{D}_i(G)/\mathrm{D}_{i+1}(G)$ for each $i \geq 1$ [PS72]
(See [Pas77, Lemma 2.7] for the first three invariants).

(4) The isomorphism type of $\gamma_2(G) \cap \mathcal{Z}(G)$ [San89, Theorem 6.11].

(5) The isomorphism type of $\mathcal{Z}(G)/\mathcal{Z}(G) \cap \gamma_2(G)$ [San89, Theorem 6.11].

(6) The isomorphism type of $\mathrm{D}_i(\gamma_2(G))/\mathrm{D}_{i+1}(\gamma_2(G))$ for each $i \geq 1$ [San85, Lemma 6.26].

(7) The isomorphism type of $G/\mathcal{Z}(G)$, if G has nilpotency class 2 [San85, Theorem 6.23].

(8) The isomorphism type of G', in the class of metabelian groups.

(9) The isomorphism type of $G/\gamma_2(G)\Omega_i(\mathcal{Z}(G))$, for each $i \geq 0$ [MSS23, Theorem B].

(10) The isomorphism type of $\gamma_2(G)\Omega_i(\mathcal{Z}(G))/\gamma_2(G)$, for each $i \geq 0$ [MSS23, Theorem B].

(11) The isomorphism type of $\mathcal{Z}(G) \cap (\mho_i(G)\gamma_2(G))$ for each $i \geq 0$ [MSS23, Theorem B].

(12) The isomorphism type of $\mathcal{Z}(G)/\mathcal{Z}(G) \cap (\mho_i(G)\gamma_2(G))$, for each $i \geq 0$ [MSS23, Theorem B].

(13) The smallest possible size of a set of generators of G.

(14) The smallest possible size of a set of generators of $\gamma_2(G)$.

(15) For $n \geq 0$, the number of conjugacy classes of G containing an element of the form g^{p^n}, with $g \in G$ [Kü82].

(16) The number of conjugacy classes of p n-th powers which have the same order as a class which powers to them [PPM81] (see also [HS06, Corollary 2.4]).

(17) $\sum_{g^G} \log_p |C_G(g)|/|\Phi(C_G(g))|$ (called the "Roggenkamp parameter").

(18) The exponent of G [Kü82].

(19) The nilpotency class of G, if $\gamma_2(G)$ is cyclic [BK07, Theorem 2].

(20) The nilpotency class of G, if G has exponent p [BK07, Theorem 2].

(21) Whether G has nilpotency class 2 or not [BK07, Theorem 2].

(22) The order of largest cyclic subgroup containing G', in the class of groups with cyclic derived subgroup [San96, Proposition 4].

When the base field is prime, some stronger invariants can be obtained.

Theorem 2.6. *Let p be a prime, k the field of p elements, and G a finite p-group. The following group theoretical invariants of G are determined by the group algebra kG.*

(1) The isomorphism type of $\mathrm{D}_i(G)/\mathrm{D}_{i+2}(G)$ for each $i \geq 1$ [PS72].

(2) The isomorphism type of $\mathrm{D}_i(G)/\mathrm{D}_{2i+1}(G)$ for each $i \geq 1$ [RS83].

(3) The isomorphism type of $G/\mho_1(\gamma_2(G))\gamma_3(G)$ for each $i \geq 1$ [San89].

(4) The isomorphism type of $G/\mathrm{D}_4(G)$, if $p > 2$ [Her07].

(5) The isomorphism type $G/\mathcal{U}_1(\gamma_2(G))\gamma_4(G)$, if G is 2-generated [Bag99, MM22][3].

(6) The isomorphism type of $\Phi(G)$, in the class of abelian-by-(elementary abelian) groups.

(7) The isomorphism type of $\Phi(G)$, in the class of (elementary abelian)-by-abelian groups with $\gamma_{2p}(G) = 1$ [HS06, p. 16].

(8) The number of conjugacy classes of maximal elementary abelian subgroups of G (called "Quillen parameter").

(9) The nilpotency class of $G/\Phi(\gamma_2(G))$ [BC88].

(10) Whether G is of maximal class or not [BK19].

In Theorems 2.3, 2.4, 2.5 and 2.6, the non-referenced results are folklore (or I have not been able to track the original source). Observe that the condition "if G satisfies certain property" is different from the condition "in the class of groups with certain property", since the former means that if G satisfies the property and H is any other group such that $kG \cong kH$, then G and H agree in the considered invariant.

The second approach consists in some canonical ideal J of kG such that G (and hence every group basis of kG) embeds naturally into the quotient kG/I, and furthermore the structure of kG/I is simple enough to allow the identification of the isomorphism type of G. The inconvenience of this method is obvious: the bigger the ideal I is, the simpler has to be G to embed naturally into kG/I, and the smaller the ideal I is, the less probable is that kG/I can be properly understood. Moreover this strategy has been applied successfully only when the base field is prime. In the bright side, this strategy allows us to obtain positive answers for the modular isomorphism problem for classes of groups that are not classified up to isomorphism. Moreover, it has proved to be very useful to deal with classes of groups under strong constraints, mainly in the nilpotency class and the exponent of the derived subgroup (e.g., items (3), (4), (5) and (9) in Theorem 2.4), which led to some optimism about the further success of this approach. M. A. M. Salim and R. Sandling write in [SS96b] that "One can chart a progression in recent papers on the modular isomorphism problem. Each sets out to deduce as much as possible from a quotient algebra of FG. The ideals which are divided out have become smaller and smaller, resulting in larger and larger sections of FG susceptible to purposeful analysis. At each stage a more complicated group basis becomes embeddable in the quotient algebra and thence its structure made accessible." (For them F stands for the field with p elements.) However, after this, only a few papers applied successfully this strategy: [Bag99], [Her07] and [MS22]. This suggests that this approach is almost exhausted, but some modest new results can still be obtained. In a recent preprint [BGL], via this approach we show the following:

Theorem 2.7 (Brenner, —)**.** *Let p be an odd prime, let k be the field with p elements, and let G and be a finite p-group such that $|G/\Phi(G)\mathcal{Z}(G)| = p^d$ for some positive integer d. Suppose that*

(1) $\mathcal{U}_1(G) \cap \gamma_2(G) \subseteq \mathcal{U}_1(\gamma_2(G))\gamma_3(G)$ and

(2) $|\gamma_2(G)/\mathcal{U}_1(\gamma_2(G))\gamma_3(G)| = p^{\binom{d}{2}}$.

If $kG \cong kH$ for some group H, then $G/\mathcal{U}_1(\gamma_2(G))\gamma_4(G) \cong H/\mathcal{U}_1(\gamma_2(H))\gamma_4(H)$.

A corollary of this theorem is a generalization of Theorem 2.6(5) for odd primes:

Corollary 2.8 (Brenner, —)**.** *Let p be an odd prime, let k be the field with p elements and let G and be a finite p-group such that $G/\mathcal{Z}(G)$ is 2-generated. If $kG \cong kH$ for some group H, then*

$$G/\mathcal{U}_1(\gamma_2(G))\gamma_4(G) \cong H/\mathcal{U}_1(\gamma_2(H))\gamma_4(H).$$

Combining the former with Theorem 2.4(9), we are able to solve the modular isomorphism problem for finite p-groups G such that the index of $\mathcal{Z}(G)$ in G is at most p^3 for p odd, an improvement over Theorem 2.3(3) for the prime field. This also delves into the difference between the cases $p = 2$ and $p > 2$, in the light of Part II (observe that the groups in Theorem 3.2 have center of index 2^3).

[3] It was mentioned without proof in the last lines of [Bag99]. A proof was provided in [MM22].

Theorem 2.9 (Brenner, —)**.** *Let p be an odd prime, let k be the field of p elements, and let G be a finite p-group such that $|G : \mathcal{Z}(G)| \leq p^3$. If $kG \cong kH$ for some group H, then $G \cong H$.*

As the reader would expect, both approaches usually interact. For example, when dealing with the modular isomorphism problem for a well understood class of groups, the techniques of the second approach might be useful to distinguish their group algebras. As well as the application of the second strategy might be combined with the use of the invariants in Theorems 2.5 and 2.6.

There is a third way to approach the modular isomorphism problem, that consists in proving that to solve the problem for the class of all finite p-groups is equivalent to solve this problem for groups in a smaller class. This approach is relatively novel, the first result appearing in 2020. We introduce the necessary notation to present this result. Given a finite p-group G, one can take subgroups $\mathrm{El}(G)$ and $\mathrm{NEl}(G)$ of G such that $G = \mathrm{El}(G) \times \mathrm{NEl}(G)$, $\mathrm{El}(G)$ is elementary abelian, and NEl does not have elementary abelian direct factors. By the Krull-Schmidt theorem for finite groups, the isomorphism types of $\mathrm{El}(G)$ and $\mathrm{NEl}(G)$ are completely determined by the isomorphism type of G.

Theorem 2.10. *[MM22, Theorem A] Let p be a prime, let k be a field of characteristic p, and let G and H be finite p-groups. The following are equivalent:*

(1) $kG \cong kH$.

(2) $k\,(NEl(G)) \cong k\,(NEl(H))$ and $El(G) \cong El(H)$.

In other words, Theorem 2.10 reduces the modular isomorphism problem for the same problem only for groups without elementary abelian direct factors. This reduction approach, *per se*, does not aim to give a definitive answer in any sense to the modular isomorphism problem, but combined with the pre-existing results, it leads to answer MIP in the positive for some new classes of groups extending the known ones. For example, the positive answer for the classes (7) and (8) in Theorem 2.3 were obtained as applications of Theorem 2.10.

A result that does not fit in none of the previous categories is the following criterion due to T. Sakurai. Its proof, in contrast to the previous results, does not consists in studying the internal structure of kG, nor its module category, but in exploiting the adjunction between the functor *group of units*, from the category of k-algebras to the category of groups, and the functor *group algebra*, from the category of groups to the category of k-algebras. The statement requires a quite technical definition:

Definition 2.11. *[Sak20, Definition 1.4] Set $M = \{[G] : G \text{ is a finite group}\}$, where the symbol $[G]$ denotes the isomorphism type of a group G. M becomes a commutative monoid with the operation $[G]+[H] = [G\times H]$. Thus we can construct its Groethendieck group $K(M)$. As it is $\mathbb{Z}$-module, we can extend scalars and obtain a $\mathbb{Q}$-vector space $L(M) = \mathbb{Q} \otimes_{\mathbb{Z}} K(M)$. Given a finite commutative ring k, the subspace $S(k)$ of $L(M)$ is defined by*

$$S(k) = \sum_{\substack{A \text{ is a finite} \\ \text{unital } k\text{-algebra}}} \mathbb{Q}[\,\mathcal{U}(A)],$$

where $\mathcal{U}(A)$ denotes the group of units of A. Namely, $S(k)$ is the subspace of $L(M)$ spanned by all the isomorphism types of groups of units of finite unital k-algebras. A finite group is called hereditary over k *if for each subgroup K of G, one has $[K] \in S(k)$.*

Theorem 2.12. *[Sak20, Criterion 1.6] Let G and H be finite groups, and let k be a commutative ring. Suppose that G is hereditary over k. If $kG \cong kH$, then $G \cong H$.*

This criterion provides an alternative proof of Theorem 2.3(1) restricted to the prime field, and of Theorem 2.4(3).

Results

Now we give an overview of the results that form this thesis.

3 2-generated finite p-groups with cyclic derived subgroup

We start mentioning that our initial goal was to study the modular isomorphism problem for 2-generated finite p-groups with cyclic derived subgroup, inspired by the success of [BdR21]. We devote to these groups Parts I, II, III and IV.

A classification

Following the first approach described in Section 2, an initial step to study the modular isomorphism problem for a concrete class of groups is to classify those groups up to isomorphism. Two different classifications of the 2-generated finite p-groups with cyclic derived subgroup for $p > 2$ already existed in the literature: [Mie75] and [Son13]. The first one contains some mistakes and missing groups, while the second was not suitable for our purposes, since the group-theoretical meaning of some of the parameters that configure her classification is sometimes obscure — and this is a key aspect, since our goal is to recover those parameters not only from the group, but from the k-algebra structure of kG. For these reasons, added up to the lack of a classification for $p = 2$, the first result in this thesis consists in a complete —and suitable for the study of the modular isomorphism problem— classification of these groups. This is achieved in Part I ([BGLdR23]).

To give a meaningful statement of the classification theorem, we first fix some notation. Let $\mathcal{A}$ be the set of tuples

$$(p, m, n_1, n_2, \sigma_1, \sigma_2, o_1, o_2, o_1', o_2', u_1, u_2)$$

satisfying the following conditions:

(1) p is prime and $n_1 \geq n_2 \geq 1$.

(2) $\sigma_i = \pm 1$, $0 \leq o_i < \min(m, n_i)$ and $p \nmid u_i$ for $i = 1, 2$.

(3) If $p = 2$ and $m \geq 2$ then $o_i < m - 1$ for $i = 1, 2$.

(4) $0 \leq o_i' \leq m - o_i$ for $i = 1, 2$ and $o_1' \leq m - o_2$.

(5) One of the following conditions holds:

  (a) $o_1 = 0$.

  (b) $0 < o_1 = o_2$ and $\sigma_2 = -1$.

  (c) $o_2 = 0 < o_1$ and $n_2 < n_1$.

  (d) $0 < o_2 < o_1 < o_2 + n_1 - n_2$.

(6) Suppose that $\sigma_1 = 1$. Then the following conditions hold:

  (a) $\sigma_2 = 1$ and $o_2 + o_1' \leq m \leq n_1$.

  (b) Either $o_1 + o_2' \leq m \leq n_2$ or $2m - o_1 - o_2' = n_2 < m$ and $u_2 \equiv 1 \bmod p^{m-n_2}$.

(c) If $o_1 = 0$ then either
  (i) $o_1' \le o_2' \le o_1' + o_2 + n_1 - n_2$ and $\max(p-2, o_2', n_1 - m) > 0$, or
  (ii) $p = 2$, $m = n_1$, $o_2' = 0$ and $o_1' = 1$.

(d) If $o_2 = 0 < o_1$ then $o_1' + \min(0, n_1 - n_2 - o_1) \le o_2' \le o_1' + n_1 - n_2$ and $\max(p-2, o_1', n_1 - m) > 0$.

(e) If $0 < o_2 < o_1$ then $o_1' \le o_2' \le o_1' + n_1 - n_2$.

(f) $1 \le u_1 \le p^{a_1}$, where
$$a_1 = \min(o_1', o_2, o_2 + n_1 - n_2 + o_1' - o_2').$$

(g) One of the following conditions holds:
  (i) $1 \le u_2 \le p^{a_2}$.
  (ii) $o_1 o_2 \ne 0$, $n_1 - n_2 + o_1' - o_2' = 0 < a_1$, $1 + p^{a_2} \le u_2 \le 2p^{a_2}$, and $u_1 \equiv 1 \bmod p$,

  where
$$a_2 = \begin{cases} 0, & \text{if } o_1 = 0; \\ \min(o_1, o_2', o_2' - o_1' + \max(0, o_1 + n_2 - n_1)), & \text{if } o_2 = 0 < o_1; \\ \min(o_1 - o_2, o_2' - o_1'), & \text{otherwise.} \end{cases}$$

(7) Suppose that $\sigma_1 = -1$. Then the following conditions hold:

(a) $p = 2$, $m \ge 2$, $o_1' \le 1$ and $u_1 = 1$.

(b) If $\sigma_2 = 1$ then $n_2 < n_1$ and the following conditions hold:
  (i) If $m \le n_2$ then $o_2' \le 1$, $u_2 = 1$ and either $o_1' \le o_2'$ or $o_2 = 0 < n_1 - n_2 < o_1$
  (ii) If $m > n_2$ then $m + 1 = n_2 + o_2'$, $u_2(1 + 2^{m-o_1-1}) \equiv -1 \bmod 2^{m-n_2}$, $1 \le u_2 \le 2^{m-n_2+1}$, either $o_1' = 1$ or $o_1 + 1 \ne n_1$, and at least one of the following conditions holds:
    - $o_1' = 0$ and either $o_1 = 0$ or $o_2 + 1 \ne n_2$.
    - $o_1' = 1$, $o_2 = 0$ and $n_1 - n_2 < o_1$.
    - $u_2 \le 2^{m-n_2}$.

(c) If $\sigma_2 = -1$ then $o_2' \le 1$, $u_2 = 1$ and the following conditions hold:
  (i) If $o_1 \le o_2$ and $n_1 > n_2$ then $o_1' \le o_2'$.
  (ii) If $o_1 = o_2$ and $n_1 = n_2$ then $o_1' \ge o_2'$
  (iii) If $o_2 = 0 < o_1 = n_1 - 1$ and $n_2 = 1$ then $o_1' = 1$ or $o_2' = 1$.
  (iv) If $o_2 = 0 < o_1$ and $n_1 \ne o_1 + 1$ or $n_2 \ne 1$ then $o_1' + \min(0, n_1 - n_2 - o_1) \le o_2'$.
  (v) If $o_1 o_2 \ne 0$ and $o_1 \ne o_2$ then $o_1' \le o_2'$.

Now we are ready to state the classification theorem (the Main Theorem of Part I):

Theorem 3.1 (Broche, —, del Río)**.** *For each $I = (p, m, n_1, n_2, \sigma_1, \sigma_2, o_1, o_2, o_1', o_2', u_1, u_2) \in \mathcal{A}$, we define the group*

$$\mathcal{G}_I = \left\langle b_1, b_2 \mid [b_2, b_1]^{p^m} = 1, \quad [b_2, b_1]^{b_i} = [b_2, b_1]^{r_i}, \quad b_i^{p^{n_i}} = [b_2, b_1]^{u_i p^{m - o_i'}}, \quad (i = 1, 2) \right\rangle,$$

where r_1 and r_2 are the unique integers $1 < r_i \le 1 + p^m$ satisfying

$$r_1 \equiv \sigma_1(1 + p^{m-o_1}) \bmod p^m \quad \text{and} \quad \begin{cases} r_2 \equiv \sigma_2(1 + p^{m-o_2}) \bmod p^m, & \text{if } o_1 o_2 = 0; \\ r_2 \equiv \sigma_2(1 + p^{m-o_1})^{p^{o_1 - o_2}} \bmod p^m, & \text{otherwise.} \end{cases}$$

The map $I \mapsto [\mathcal{G}_I]$, where $[\mathcal{G}_I]$ is the isomorphism type of $\mathcal{G}_I$, is a bijection between $\mathcal{A}$ and the set of isomorphism types of the 2-generated groups of prime power order with cyclic derived subgroup.

We denote the inverse of the map in the theorem by $\mathrm{inv}(\cdot)$. This inverse is described in Part I. Moreover, this description together with the proof of the theorem provides an algorithm to compute this inverse efficiently, and hence to check whether two given 2-generated finite p-groups with cyclic derived subgroup are isomorphic or not. This algorithm, together with the set $\mathcal{A}$ and an efficient method to construct the groups have been implemented in a GAP program, available at [BCGLdR22]

A negative answer

Part II([GLMdR22]) consists in the description of a series of pairs of 2-generated finite 2-groups with cyclic derived subgroup with isomorphic group algebras over each field of characteristic 2, solving the modular isomorphism problem in its generality, more than sixty years since W. E. Deskins initial result.

Let $n_1 > n_2 > 2$, and let G and H be the 2-generated groups with cyclic derived commutator satisfying

$$\begin{aligned}\mathrm{inv}(G) &= (2, 2, n_1, n_2, -1, -1, 0, 0, 0, 0, 1, 1);\\ \mathrm{inv}(H) &= (2, 2, n_1, n_2, -1, \quad 1, 0, 0, 0, 0, 1, 1).\end{aligned}$$

Presentations for these groups are:

$$\begin{aligned}G &= \left\langle b_1, b_2 : [b_2, b_1]^4 = 1,\ [b_2, b_1]^{b_1} = [b_2, b_1]^{b_2} = [b_2, b_1]^{-1},\ b_1^{p^{n_1}} = b_2^{p^{n_2}} = 1 \right\rangle;\\ H &= \left\langle \tilde{b}_1, \tilde{b}_2 : [\tilde{b}_2, \tilde{b}_1]^4 = 1,\ [\tilde{b}_2, \tilde{b}_1]^{\tilde{b}_1} = [\tilde{b}_2, \tilde{b}_1]^{-1},\ [\tilde{b}_2, \tilde{b}_1]^{\tilde{b}_2} = [\tilde{b}_2, \tilde{b}_1]\ \tilde{b}_1^{p^{n_1}} = \tilde{b}_2^{p^{n_2}} = 1 \right\rangle\end{aligned}$$

Theorem 3.1 yields that G and H are non-isomorphic, since $\mathrm{inv}(G) \neq \mathrm{inv}(H)$. Then the following theorem answers Problem 2.1 (and hence Problem 2.2) in the negative for $p = 2$:

Theorem 3.2 (—, Margolis, del Río)**.** *Let k be a field of characteristic 2. Then $kG \cong kH$.*

The proof is not complicated, and simply consists in showing that the subgroup

$$\left\langle \tilde{b}_1,\ \ \tilde{b}_2(\tilde{b}_1 + \tilde{b}_2 + \tilde{b}_1\tilde{b}_2)[\tilde{b}_2, \tilde{b}_1] \right\rangle$$

of the group of units of kH is isomorphic to G, and its elements generate all of kH as a k-algebra.

On the modular isomorphism problem for $p > 2$

Once settled the modular isomorphism problem in the negative for $p = 2$, in Part III ([GLdRS22]), and later in Part IV ([GLdR23]), we attack this question for 2-generated finite p-groups with cyclic derived subgroup for $p > 2$. The following result encompass Theorem B of Part III and Theorem 2 of Part IV, and states that if G is 2-generated with cyclic derived subgroup, then so is H and almost all the entries of $\mathrm{inv}(G)$ are determined by kG.

Theorem 3.3 (—, del Río, Stanojkovski)**.** *Let p be an odd prime, let k be a field of characteristic p, and let G be a 2-generated finite p-group with cyclic derived subgroup with*

$$\mathrm{inv}(G) = (p, m, n_1, n_2, \sigma_1, \sigma_2, o_1, o_2, o_1', o_2', u_1, u_2).$$

If $kG \cong kH$ for some group H, then H is 2-generated, $\gamma_2(H)$ is cyclic and

$$\mathrm{inv}(H) = p, m, n_1, n_2, \sigma_1, \sigma_2, o_1, o_2, o_1', o_2', v_1, v_2)$$

for some integers v_1 and v_2. If additionally k is the field of p elements, then $u_2 \equiv v_2 \mod p$ and one of the following holds:

(1) $u_1 \equiv v_1 \mod p$.

(2) $o_1 o_2 > 0$, $n_1 + o_1' = n_2 + o_2'$ *and at least one of the following conditions fails:*

- $u_2 \equiv v_2 \equiv 1 \mod p^{o_1+1-o_2}$,
- $n_2 = 2m - o_1 - o_2'$,

As a consequence, corresponding to Theorem A of Part III we obtain a number of group theoretical invariants that are determined by the modular group algebra for groups with cyclic derived subgroup (not necessarily 2-generated).

Theorem 3.4 (—, del Río, Stanojkovski)**.** *Let p be an odd prime, let k be a field of characteristic p, and let G be finite p-group with cyclic derived subgroup. If $kG \cong kH$ for some group H, then the following hold:*

(1) $\mathrm{C}_G(\gamma_2(G))$ *and* $\mathrm{C}_H(\gamma_2(H))$ *have the same exponent.*

(2) $\mathrm{C}_G(\gamma_2(G))/\gamma_2(G) \cong \mathrm{C}_H(\gamma_2(H))/\gamma_2(H)$.

(3) $\mathrm{C}_G(\gamma_2(G))/\gamma_2(\mathrm{C}_G(\gamma_2(G))) \cong \mathrm{C}_H(\gamma_2(H))/\gamma_2(\mathrm{C}_H(\gamma_2(H)))$.

A corollary of the previous theorem is that the isomorphism type of the centralizer of the derived subgroup is determined by the modular group algebra for this class of groups.

Corollary 3.5 (—, del Río, Stanojkovski)**.** *Let p be an odd prime, let k be a field of characteristic p, and let G be a finite 2-generated p-group with cyclic derived subgroup. If $kG \cong kH$ for some group H, then $C_G(\gamma_2(G)) \cong C_H(\gamma_2(H))$.*

Another consequence, corresponding to Theorem 1.1 of Part IV, and involving only group algebras of 2-generated groups with cyclic derived subgroup over the prime field, is the following:

Theorem 3.6 (—. del Río)**.** *Let p be an odd prime, let k be the field with p elements and let G be a 2-generated finite p-group with cyclic derived subgroup. If $kG \cong kH$ for some group H, then*

(1) $G/\mathfrak{V}_1(\gamma_3(G)) \cong H/\mathfrak{V}_1(\gamma_3(H))$.

(2) $G/\mathfrak{V}_3(\gamma_2(G)) \cong H/\mathfrak{V}_3(\gamma_2(H))$.

Moreover, we can also provide a positive answer to Problem 2.1 for 2-generated group with cyclic derived subgroup with order dividing p^{11}, and for groups with order p^{12} but for $p-2$ families of groups, each one of size p.

Theorem 3.7 (—, del Río)**.** *Let G be a finite 2-generated group with cyclic derived subgroup and order dividing p^{12}. If $kG \cong kH$ for some group H, then one of the following holds:*

(1) $G \cong H$.

(2) $|G| = p^{12}$ *and one has that*

$$\mathrm{inv}(G) = (p, 4, 4, 4, 0, 2, 2, 2, u_1, 1);$$
$$\mathrm{inv}(H) = (p, 4, 4, 4, 0, 2, 2, 2, v_1, 1),$$

with $\{u_1, v_1\} \subseteq \mathcal{J}_i$ *for some* $1 \leq i \leq p-2$*, where* $\mathcal{J}_i = \{i + jp : 0 \leq j \leq p-1\}$.

4 Groups of nilpotency class 2 with cyclic center

In his 1985 survey [San85], R. Sandling writes "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." And almost forty years later, the situation is not very different. Aside for a few of partial positive results (e.g., Theorem 2.3(6) and Theorem 2.4(8)) an answer for the modular isomorphism problem for groups of class 2 still remains unknown.

Our contribution to this issue is Part V ([GLM24]), where we solve Problem 2.1 in the positive for p-groups of nilpotency class 2 with cyclic center. Moreover, we pay special attention to the base field, being able to solve Problem 2.2 in the positive for every field of odd characteristic, and for every field k of characteristic 2 such that the polynomial $X^2 + X + 1 \in k[X]$ is irreducible over k. These are the following two theorems.

Theorem 4.1 (—, Margolis)**.** *Let p be an odd prime, let k be a field of characteristic p and let G be a finite p-group of nilpotency class 2 with cyclic center. If $kG \cong kH$ for some group H, then $G \cong H$.*

Theorem 4.2 (—, Margolis)**.** *Let k be a field of characteristic 2 and let G be a finite p-group of nilpotency class 2 with cyclic center. Assume moreover that the polynomial $X^2 + X + 1$ is irreducible in the polynomial ring $k[X]$. If $kG \cong kH$ for some group H, then $G \cong H$.*

For the rest of fields of characteristic 2, we solve Problem 2.2 except for a sequence of pairs of groups. To state this last result, we need some notation. For a 2-group G of class 2, let $m(G)$ be the rank of the homocyclic component of $G/\mathcal{Z}(G)$ of maximal exponent, i.e. the number of cyclic direct factors of maximal order of this group. This is the same as the rank of the elementary abelian group $G/\Omega_{\log_2(\exp(G))-1}(G)$.

Theorem 4.3 (—, Margolis)**.** *Let k be a field of characteristic p, let G be a finite 2-group of nilpotency class 2 with cyclic center.*

(1) If $kG \cong kH$ for some group H and $m(G) \leq 2$, then $G \cong H$.

(2) Suppose that $m(G) > 2$. Then there exists at most one isomorphism class of groups C not containing G such that the following implication holds: If $kG \cong kH$ for some group H, either $G \cong H$ or $H \in C$.

The results in this part follow closely the first strategy, and are based on the classification of the finite p-groups of class 2 with cyclic centre due to Y. K. Leong [Leo74, Leo79].

5 Reduction theorems

In Part VI ([GL24]), Theorem 2.10 is generalized by dropping the 'elementary' hypothesis, i.e., proving that the modular isomorphism problem can be reduced to the same problem over groups without abelian direct factors, with no restrictions on the exponent. We formalize this as follows. Given a finite p-group G, consider the subgroups $\mathrm{Ab}(G)$ and NAb(G) of G such that $G = \mathrm{Ab}(G) \times \mathrm{NAb(G)}$, $\mathrm{Ab}(G)$ is abelian and NAb(G) has no abelian direct factors. By the Krull-Remak-Schmidt theorem, the isomorphism types of $\mathrm{Ab}(G)$ and NAb(G) do not depend on the chosen decomposition, so they are group-theoretical invariants of the group G. Then we can disregard the direct factor $\mathrm{Ab}(G)$ in the study of the modular isomorphism problem. Formally:

Theorem 5.1. *Let p be a prime, let k be the field of p elements and let G and H be finite p-groups. The following are equivalent:*

(1) $kG \cong kH$.

(2) $k\,(\mathrm{NAb}(G)) \cong k\,(\mathrm{NAb}(H))$ and $\mathrm{Ab}(G) \cong \mathrm{Ab}(H)$.

As an immediate corollary, we can extend non-trivially some of the classes of groups for which the modular isomorphism problem is known to have a positive answer.

Corollary 5.2. *Let p be a prime, let k be the field of p elements and let A and G be finite p-groups such that A is abelian and G belongs to at least one of the classes in Theorem 2.3 or in Theorem 2.4. If H is another group such that $kH \cong k(G \times A)$, then $H \cong G \times A$.*

The primality of the field is important in the proof of Theorem 5.1. However, for an arbitrary field of characteristic p we can still recover the isomorphism type of the maximal abelian direct factor.

Proposition 5.3. *Let p be a prime, let G and H be finite p-groups and k be a field of characteristic p. Then $kG \cong kH$ implies that $\mathrm{Ab}(G) \cong \mathrm{Ab}(H)$.*

We do not have an analogue of the proof of the other implication in Theorem 5.1 ($kG \cong kG$ implies that $k\,(\mathrm{NAb}(G)) \cong k\,(\mathrm{NAb}(H))$), but it seems reasonable that the result will extend to arbitrary fields of the same characteristic.

This extra difficulty when one increases the size of the field in the same characteristic, together with the curious behaviour of certain fields of characteristic 2 observed in Theorem 4.2 and Theorem 4.3, made us wonder how the field k of characteristic p influences the answer to Problem 2.2. Part VII ([GLdR24]) is an initial attempt to attack this problem. There we show that only finite extensions of prime fields matter for the isomorphism problem.

Theorem 5.4 (—, del Río)**.** *Let k be a field, let k_0 be the prime field of k, and let G and H be finite groups. If $kG \cong kH$, then there exists a finite extension k_1 of k_0 such that $k_1G \cong k_1H$.*

If the characteristic of k is coprime with the order of the group G, then a finite extension of k_0 split k_0G and k_0H and hence, in this case, a proof of Theorem 5.4 is straightforward. However, we present a unified proof for any characteristic. The application of Theorem 5.4 to the Problem 2.2 shows that this question can be regarded as exclusively about finite objects. Formally:

Corollary 5.5 (—, del Río)**.** *Let p be a prime, and let G and H finite p-groups such that $kG \cong kH$ for some field k of characteristic p. Then there exists a finite field k_1 of characteristic p such that $k_1G \cong k_1H$.*

We highlight that this reduction makes possible to apply R. Brauer's suggestion to attack Problem 2.1 "by counting the number of elements of a power of the radical which satisfy a given condition" also to attack Problem 2.2, since these counting arguments are available only for finite fields. This strategy is applied successfully in the proof Theorem 4.3.

6 Desiderata and open questions

Despite Theorem 3.2 gives a negative answer to the modular isomorphism questions in its general form, many interesting questions on this topic remain unanswered. Some of these questions appear in the recent survey [Mar22]. The most natural (and interesting) class of groups for which the modular isomorphism problem is still open is the class of p-groups of odd order.

Problem 6.1. *Settle the modular isomorphism problem for $p > 2$.*

The groups of Theorem 3.2 have nilpotency class 3, and another natural class of groups for which there is still hope to obtain a positive answer to the modular isomorphism problem is the class of groups with nilpotency class 2.

Problem 6.2. *Settle the modular isomorphism problem for groups of nilpotency class 2.*

In the other extreme of the duality complexity of the p-power map/complexity of the commutator map, we find the groups with exponent p, for which the modular isomorphism problem is still open.

Problem 6.3. *Settle the modular isomorphism problem for groups of exponent p.*

These being the most natural and general open questions on the modular isomorphism problem, some others, more specific —and hence maybe easier to approach— can be the following. In spite of all the work in Parts III and IV, the modular isomorphism problem remains open for 2-generated p-groups with cyclic derived subgroup for $p > 2$.

Problem 6.4. *Settle the modular isomorphism problem for 2-generated p-groups with cyclic derived subgroup for $p > 2$.*

About this last problem, we observe that the groups in Theorem 3.2 are 2-generated with cyclic derived subgroup of order p^2. However, for $p > 2$, MIP has positive answer for the subclass of groups with this property (Theorem 3.6). Similarly, the groups of Theorem 3.2 have center of index p^3, and again for the class of groups with this property MIP has positive answer (Theorem 2.9). Thus, apparently, groups providing a negative answer to MIP for $p > 2$ will be (in case they exist) quite different from examples for $p = 2$. We pose one last, and extremely specific, question about 2-generated groups with cyclic derived subgroups.

Problem 6.5. *Settle the modular isomorphism problem for the groups in Theorem 3.7(2).*

Now we focus on more general questions, not specialized to any class of finite p-groups. We already mentioned that we do not know whether Theorem 5.1 generalizes to arbitrary fields of characteristic p. In order to do so, it suffices to solve the following problem in the positive.

Problem 6.6. *Decide whether $kG \cong kH$ implies $k\,(NAb(G)) \cong k\,(NAb(H))$ or not.*

Furthermore, regarding these "changes of field", we can simply ask the following.

Problem 6.7. *Let k be a field of characteristic p, let k_0 be its prime field, and let G and H be finite p-groups. Decide whether $kG \cong kH$ implies $k_0G \cong k_0H$ or not.*

We conclude with a few structural questions, related to the structure of the modular group algebras of finite p-groups, as well to the reduction results for the modular isomorphism problem. One of the most natural features of a finite p-group G is its nilpotency class, but how it relates to the algebra structure of kG is still mysterious, and not understood in general.

Problem 6.8. *Decide whether the nilpotency class of a finite p-group is determined by its modular group algebra.*

While whether a p-group has nilpotency class 2 or not is determine by the group algebra Theorem 2.5(21), it is still unknown whether being metabelian is determined. This shows that the relation between the modular group algebra and the derived length is less understood, making the following problem even harder.

Problem 6.9. *Decide whether the derived length of a finite p-group is determined by its modular group algebra.*

Given a finite group G, we can consider an *indecomposable decomposition* $G = G_1 \times G_2 \times \cdots \times G_n$, where each G_i is indecomposable as a direct product of proper subgroups. Then both the number n are the list of isomorphism types of the G_i's (up to reordering) are group theoretical invariants of G, by the Krull-Schmidt theorem for finite groups. Settling in the positive the following problem would widely generalize Theorem 2.10 and Theorem 5.1:

Problem 6.10. *Let k be the field of p elements, let G and H finite p-groups, and let $G = G_1 \times G_2 \times \cdots \times G_n$ be an indecomposable decomposition of G. Decide whether $kG \cong kH$ implies that H has an indecomposable decomposition $H = H_1 \times H_2 \times \cdots \times H_n$ such that $kG_i \cong kH_i$ for each i, or not.*

Observe that this problem is considerably weaker than the modular isomorphism problem. A positive answer to Problem 6.10 would imply that the modular isomorphism problem can be reduced to the same problem over p-groups which are indecomposable as direct product of proper subgroups. This would take the reduction strategy (at least in the sense of direct products) to its optimal outcome.

The group algebra of a direct product of groups is isomorphic to the tensor product (over the base field) of the group algebras of each group; formally,

$$k(G \times H) \cong kG \otimes_k kH,$$

for each pair of finite groups G and H and each field k. However, under the assumptions that G is a finite p-group and k is a field of characteristic p, it is unknown whether a non-trivial decomposition of the group algebra as a tensor product of proper subalgebras implies the existence of a decomposition of the group as a direct product of proper subgroups. Here by *non-trivial decomposition as tensor product* we mean a decomposition $A = A_1 \otimes_k A_2$ such that the dimension of A_i over k is strictly greater than 1 for $i = 1, 2$. This appears as a question in [CK95].

Problem 6.11. *Decide whether the group algebra of an indecomposable finite p-group over a field of characteristic p is indecomposable as non-trivial tensor product of k-algebras or not.*

In the spirit of Problem 6.10, A. Jaikin asked the author, during a seminar in the ICMAT, whether a tensor product version of the Krull-Schmidt theorem could hold for local augmented algebras with nilpotent Jacobson radical. Formally:

Problem 6.12. *Let k be a field of characteristic p and let A be a local k-algebra with nilpotent Jacobson radical of codimension 1 (e.g., the group algebra of a finite p-group over a field of characteristic p). Suppose that $A = A_1 \otimes_k \cdots \otimes_k A_n = B_1 \otimes_k \cdots \otimes_k B_m$, for subalgebras A_i and B_j that are indecomposable as a tensor product of proper subalgebras. Decide whether $n = m$ and $A_i \cong B_i$ for each i (up to a possible reordering of the B_i's) or not.*

The author has tackled this problem during a great part of the last year, in the concrete case where A is the group algebra of a finite p-group, together Problem 6.10, with (excluding a couple of fleeting moments of mathematical self-delusion) scarce success. It is to be noted that positive answer to Problem 6.12, under the additional hypothesis that A is the group algebra of a finite abelian p-group over a field of characteristic p, has existed for more than twenty years [CK95].

Bibliography

[Bag88] C. Bagiński, *The isomorphism question for modular group algebras of metacyclic p-groups*, Proc. Amer. Math. Soc. **104** (1988), no. 1, 39–42.

[Bag99] ———, *On the isomorphism problem for modular group algebras of elementary abelian-by-cyclic p-groups*, Colloq. Math. **82** (1999), no. 1, 125–136.

[BC88] C. Bagiński and A. Caranti, *The modular group algebras of p-groups of maximal class*, Canad. J. Math. **40** (1988), no. 6, 1422–1435.

[BCGLdR22] O. Broche-Cristo, D. García-Lucas, and Á. del Río, *CbA2Gen. A classification of 2-generated cyclic-by-abelian finite p-groups*, https://github.com/angeldelriomateos/CbA2Gen, 2022.

[BdR21] O. Broche and Á. del Río, *The Modular Isomorphism Problem for two generated groups of class two*, Indian J. Pure Appl. Math. **52** (2021), 721–728.

[BGL] S. Brenner and D. García-Lucas, *On the modular isomorphism problem for groups with large centre*, arXiv:2311.06666.

[BGLdR23] O. Broche, D. García-Lucas, and Á. del Río, *A classification of the finite 2-generator cyclic-by-abelian groups of prime-power order*, International Journal of Algebra and Computation **33** (2023), no. 04, 641–686.

[BK07] 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.

[BK19] C. Bagiński and J. Kurdics, *The modular group algebras of p-groups of maximal class II*, Comm. Algebra **47** (2019), no. 2, 761–771.

[BKRW99] F. M. Bleher, W. Kimmerle, K. W. Roggenkamp, and M. Wursthorn, *Computational aspects of the isomorphism problem*, Algorithmic algebra and number theory (Heidelberg, 1997), Springer, Berlin, 1999, pp. 313–329.

[Bra63] R. Brauer, *Representations of finite groups*, Lectures on Modern Mathematics, Vol. I, Wiley, New York, 1963, pp. 133–175.

[Car77] J. F. Carlson, *Periodic modules over modular group algebras*, J. London Math. Soc. (2) **15** (1977), no. 3, 431–436.

[CK95] J. F. Carlson and L. G. Kovács, *Tensor factorizations of group algebras and modules*, J. Algebra **175** (1995), no. 1, 385–407 (English).

[Col64] D. B. Coleman, *On the modular group ring of a p-group*, Proc. Am. Math. Soc. **15** (1964), 511–514 (English).

[Dad71] E. Dade, *Deux groupes finis distincts ayant la même algèbre de groupe sur tout corps*, Math. Z. **119** (1971), 345–348.

[Des56] W. E. Deskins, *Finite Abelian groups with isomorphic group algebras*, Duke Math. J. **23** (1956), 35–40. MR 77535

[Dre89] V. Drensky, *The isomorphism problem for modular group algebras of groups with large centres*, Representation theory, group rings, and coding theory, Contemp. Math., vol. 93, Amer. Math. Soc., Providence, RI, 1989, pp. 145–153.

[Eic08] B. Eick, *Computing automorphism groups and testing isomorphisms for modular group algebras*, J. Algebra **320** (2008), no. 11, 3895–3910.

[GL24] D. García-Lucas, *The modular isomorphism problem and abelian direct factors*, Mediterr. J. Math. **21** (2024), Article 18.

[GLdR23] D. García-Lucas and Á. del Río, *On the modular isomorphism problem for 2-generated groups with cyclic derived subgroup*, arXiv:2310.02627 (2023).

[GLdR24] ———, *A reduction theorem for the Isomorphism Problem of group algebras over fields*, Journal of Pure and Applied Algebra **228** (2024), no. 4, 107511.

[GLdRS22] D. García-Lucas, Á. del Río, and M. Stanojkovski, *On group invariants determined by modular group algebras: even versus odd characteristic*, Algebr. Represent. Theory. https://doi.org/10.1007/s10468-022-10182-x (2022).

[GLM24] D. García-Lucas and L. Margolis, *On the modular isomorphism problem for groups of nilpotency class 2 with cyclic center*, Forum Mathematicum (2024), doi.org/10.1515/forum–2023–0237.

[GLMdR22] 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.

[Her01] M. Hertweck, *A counterexample to the isomorphism problem for integral group rings*, Ann. of Math. (2) **154** (2001), no. 1, 115–138.

[Her07] ———, *A note on the modular group algebras of odd p-groups of M-length three*, Publ. Math. Debrecen **71** (2007), no. 1-2, 83–93.

[Hig40] G. Higman, *Units in group rings*, 1940, Thesis (Ph.D.)–Univ. Oxford.

[HS06] 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.

[HS07] ———, *Parametrization of central Frattini extensions and isomorphisms of small group rings*, Israel J. Math. **157** (2007), 63–102.

[JdR16] E. Jespers and Á. del Río, *Group ring groups. Volume 1: Orders and generic constructions of units.*, De Gruyter Textb., Berlin: De Gruyter, 2016 (English).

[Jen41] S. A. Jennings, *The structure of the group ring of a p-group over a modular field*, Trans. Amer. Math. Soc. **50** (1941), 175–185.

[Kim91] W. Kimmerle, *Beiträge zur ganzzahligen Darstellungstheorie endlicher Gruppen*, Bayreuth. Math. Schr. (1991), no. 36, 139.

[Kü82] B. Külshammer, *Bemerkungen über die Gruppenalgebra als symmetrische Algebra. II*, J. Algebra **75** (1982), no. 1, 59–69.

[Laz54] M. Lazard, *Sur les groupes nilpotents et les anneaux de Lie*, Annales scientifiques de l'École Normale Supérieure **3e série, 71** (1954), no. 2, 101–190 (fr). MR 19,529b

[Leo74] Y. K. Leong, *Odd order nilpotent groups of class two with cyclic centre*, Journal of the Australian Mathematical Society **17** (1974), 142 – 153.

[Leo79] ———, *Finite 2-groups of class two with cyclic centre*, Journal of the Australian Mathematical Society **27** (1979), 125 – 140.

[Mar22] L. Margolis, *The Modular Isomorphism Problem: A Survey*, Jahresber. Dtsch. Math. Ver. (2022).

[Md19] L. Margolis and Á. del Rio, *Finite subgroups of group rings: A survey*, Advances in Group Theory and Applications **8** (2019), 1–37 (English).

[Mie75] R. J. Miech, *On p-groups with a cyclic commutator subgroup*, J. Austral. Math. Soc. **20** (1975), no. 2, 178–198.

[MM22] L. Margolis and T. Moede, *The modular isomorphism problem for small groups – revisiting eick's algorithm*, Journal of Computational Algebra **1-2** (2022), 100001.

[MS22] L. Margolis and M. Stanojkovski, *On the modular isomorphism problem for groups of class* 3 *and obelisks*, J. Group Theory **25** (2022), no. 1, 163–206.

[MSS23] L. Margolis, T. Sakurai, and M. Stanojkovski, *Abelian invariants and a reduction theorem for the modular isomorphism problem*, Journal of Algebra **636** (2023), 533–559.

[NS18] G. Navarro and B. Sambale, *On the blockwise modular isomorphism problem*, Manuscripta Math. **157** (2018), no. 1-2, 263–278.

[Pas65] 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

[Pas77] ———, *The algebraic structure of group rings*, Pure and Applied Mathematics, Wiley-Interscience [John Wiley & Sons], New York-London-Sydney, 1977.

[Pas79] I. B. S. Passi, *Group rings and their augmentation ideals*, Lect. Notes Math., vol. 715, Springer, Cham, 1979 (English).

[PM22] C. Polcino Milies, *Units of group rings and a conjecture of H. J. Zassenhaus*, São Paulo J. Math. Sci. **16** (2022), no. 1, 43–61 (English).

[PMS02] C. Polcino Milies and S. K. Sehgal, *An introduction to group rings*, Algebr. Appl., vol. 1, Dordrecht: Kluwer Academic Publishers, 2002 (English).

[PPM81] M. M. Parmenter and C. Polcino Milies, *A note on isomorphic group rings*, Bol. Soc. Bras. Mat. **12** (1981), no. 2, 57–59 (English).

[PS72] I. B. S. Passi and S. K. Sehgal, *Isomorphism of modular group algebras*, Math. Z. **129** (1972), 65–73.

[PW50] S. Perlis and G. L. Walker, *Abelian group algebras of finite order*, Trans. Amer. Math. Soc. **68** (1950), 420–426.

[RÖ90] F. Röhl, *On automorphisms of complete algebras and the isomorphism problem for modular group rings*, Canad. J. Math. **42** (1990), no. 3, 383–394.

[RS83] J. Ritter and S. Sehgal, *Isomorphism of group rings*, Arch. Math. **40** (1983), 32–39 (English).

[RS87] K. W. Roggenkamp and L. Scott, *Isomorphisms of p-adic group rings*, Ann. of Math. (2) **126** (1987), no. 3, 593–647.

[RT92] K. W. Roggenkamp and M. J. Taylor, *Group rings and class groups. Notes of talks, given at the DMV-seminar, held in Günzburg, Germany, September 1990*, DMV Semin., vol. 18, Basel etc.: Birkhäuser Verlag, 1992 (English).

[RV13] A. Ruíz and A. Viruel, *Cohomological uniqueness, massey products and the modular isomorphism problem for 2-groups of maximal nilpotency class*, Transactions of the American Mathematical Society **365** (2013), no. 7, 3729–3751.

[Sak20] T. Sakurai, *The isomorphism problem for group algebras: a criterion*, J. Group Theory **23** (2020), no. 3, 435–445.

[San85] R. Sandling, *The isomorphism problem for group rings: a survey*, Orders and their applications (Oberwolfach, 1984), Lecture Notes in Math., vol. 1142, Springer, Berlin, 1985, pp. 256–288.

[San89] ———, *The modular group algebra of a central-elementary-by-abelian p-group*, Arch. Math. (Basel) **52** (1989), no. 1, 22–27.

[San96] ———, *The modular group algebra problem for metacyclic p-groups*, Proc. Amer. Math. Soc. **124** (1996), no. 5, 1347–1350.

[Seh78] S. K. Sehgal, *Topics in group rings*, Monographs and Textbooks in Pure and Applied Math., vol. 50, Marcel Dekker, Inc., New York, 1978.

[Seh93] ———, *Units in integral group rings*, Pitman Monographs and Surveys in Pure and Applied Mathematics, vol. 69, Longman Scientific & Technical, Harlow; copublished in the United States with John Wiley & Sons, Inc., New York, 1993, With an appendix by Al Weiss.

[Son13] Q. Song, *Finite two-generator p-subgrous with cyclic derived group*, Comm. Algebra **41** (2013), no. 4, 1499–1513.

[SS96a] 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.

[SS96b] ———, *The modular group algebra problem for small p-groups of maximal class*, Can. J. Math. **48** (1996), no. 5, 1064–1078 (English).

[War61] H. N. Ward, *Some results on the group algebra of a p-group over a prime field*, Seminar on finite groups and related topics., Mimeographed notes, Harvard Univ., 1960-61, pp. 13–19.

[Whi68] A. Whitcomb, *The Group Ring Problem*, ProQuest LLC, Ann Arbor, MI, 1968, Thesis (Ph.D.) – The University of Chicago.

[Wur93] M. Wursthorn, *Isomorphisms of modular group algebras: an algorithm and its application to groups of order 2^6*, J. Symbolic Comput. **15** (1993), no. 2, 211–227. MR 1218760

Part I

in which we try to understand the 2-generated groups with cyclic derived subgroup, in the hope we would later understand their group algebras.

This empty page stands for the following article:

Title: *A classification of the finite 2-generator cyclic-by-abelian groups of prime-power order.*
Authors: Osnel Broche, Diego García-Lucas and Ángel del Río.
Reference: International Journal of Algebra and Computation, 33 no. 04 (2023) 641-686.
DOI: dx.doi.org/10.1142/S0218196723500297
Abstract: We classify the finite 2-generator cyclic-by-abelian groups of prime-power order. We associate to each such group G a list $\mathrm{inv}(G)$ of numerical group invariants which determines the isomorphism type of G. Then we describe the set formed by all the possible values of $\mathrm{inv}(G)$. This allows us to develop practical algorithms to construct all finite non-abelian 2-generator cyclic-by-abelian groups of a given prime-power order, to compute the invariants of such a group, and to decide whether two such groups are isomorphic.

Part II

in which we solve the modular isomorphism problem.

This empty page stands for the following article:

Title: *Non-isomorphic 2-groups with isomorphic modular group.*
Authors: Diego García-Lucas, Leo Margolis and Ángel del Río.
Reference: Journal fur die Reine und Angewandte Mathematik, 783 (2022) 269-274.
DOI: doi.org/10.1515/crelle-2021-0074
Abstract: We provide non-isomorphic finite 2-groups which have isomorphic group algebras over any field of characteristic 2, thus settling the Modular Isomorphism Problem.

Part III

in which we start the study of the modular isomorphism problem
over the groups described in Part I, for $p > 2$.

This empty page stands for the following article:

Title: *On group invariants determined by modular group algebras: Even versus odd characteristic.*
Authors: Diego García-Lucas, Ángel del Río and Mima Stanojkovski.
Reference: Algebras and Representation Theory.
DOI: doi.org/10.1007/s10468-022-10182-x
Abstract: Let p be a an odd prime and let G be a finite p-group with cyclic commutator subgroup G'. We prove that the exponent and the abelianization of the centralizer of G' in G are determined by the group algebra of G over any field of characteristic p. If, additionally, G is 2-generated then almost all the numerical invariants determining G up to isomorphism are determined by the same group algebras; as a consequence the isomorphism type of the centralizer of G' is determined. These claims are known to be false for $p = 2$.

Part IV

in which we continue the study of the modular isomorphism problem over the groups of Part I started in Part III.

This empty page should stand for the following preprint:

Title: *On the Modular Isomorphism Problem for 2-generated groups with cyclic derived subgroup.*
Authors: Diego García-Lucas and Ángel del Río.
Reference: arXiv:2310.02627
Abstract: We continue the analysis of the Modular Isomorphism Problem for 2-generated p-groups with cyclic derived subgroup, $p > 2$, started in [GLdRS22]. We show that if G belongs to this class of groups, then the isomorphism type of the quotients $G/(G')^{p^3}$ and $G/\gamma_3(G)^p$ are determined by its modular group algebra. In fact, we obtain a more general but technical result, expressed in terms of the classification [BGLdR23]. We also show that for groups in this class of order at most p^{11}, the Modular Isomorphism Problem has positive answer. Finally, we describe some families of groups of order p^{12} whose group algebras over the field with p elements cannot be distinguished with the techniques available to us.

But, still, a copy of such preprint can be found in the following pages.

ON THE MODULAR ISOMORPHISM PROBLEM FOR 2-GENERATED GROUPS WITH CYCLIC DERIVED SUBGROUP

DIEGO GARCÍA-LUCAS AND ÁNGEL DEL RÍO

ABSTRACT. We continue the analysis of the Modular Isomorphism Problem for 2-generated p-groups with cyclic derived subgroup, $p > 2$, started in [8]. We show that if G belongs to this class of groups, then the isomorphism type of the quotients $G/(G')^{p^3}$ and $G/\gamma_3(G)^p$ are determined by its modular group algebra. In fact, we obtain a more general but technical result, expressed in terms of the classification [4]. We also show that for groups in this class of order at most p^{11}, the Modular Isomorphism Problem has positive answer. Finally, we describe some families of groups of order p^{12} whose group algebras over the field with p elements cannot be distinguished with the techniques available to us.

The class of 2-generated finite p-groups with cyclic derived subgroup, despite its apparent simplicity, has proven to be a rich class of p-groups, specially regarding the Modular Isomorphism Problem: the only known indecomposable groups to fail to satisfy the statement of this problem are 2-groups that belong to this class (see [7]), while for $p > 2$, the situation being quite different, the problem is still to be decided. Our main result settles the Modular Isomorphism Problem in the positive for groups of this class under additional constraints on the size of the initial terms of the lower central series:

Theorem A. *Let p be an odd prime, let k be the field with p elements and let G be a 2-generated finite p-group with cyclic derived subgroup. If $kG \cong kH$ for some group H, then*

(1) $G/\gamma_3(G)^p \cong H/\gamma_3(H)^p$ and
(2) $G/(G')^{p^3} \cong H/(H')^{p^3}$.

This result fails for $p = 2$ because the counter-example in [7] is formed by groups with derived subgroup of order 4. The proof of Theorem A is based upon a more technical result in terms of the invariants described in [4], that resumes the work started in [8]. Namely, with the notation in Section 2, we prove the following theorem.

Theorem B. *Let p be an odd prime, let k be the field with p elements and let G be a 2-generated finite p-group with cyclic derived subgroup and*

$$\mathrm{inv}(G) = (p, m, n_1, n_2, o_1, o_2, o_1', o_2', u_1^G, u_2^G).$$

If $kG \cong kH$ for some group H, then H is also a 2-generated finite p-group with cyclic derived subgroup and

$$\mathrm{inv}(H) = (p, m, n_1, n_2, o_1, o_2, o_1', o_2', u_1^H, u_2^H)$$

such that

$$u_2^G \equiv u_2^H \mod p,$$

and one of the following holds:

(1) $u_1^G \equiv u_1^H \mod p$.
(2) $o_1 o_2 > 0$, $n_1 + o_1' = n_2 + o_2'$ and at least one of the following conditions fails:
- $u_2^G \equiv u_2^H \equiv 1 \mod p^{o_1+1-o_2}$,
- $n_2 + o_2' = 2m - o_1$.

Date: October 3, 2023.
2020 *Mathematics Subject Classification.* 20D15.
Key words and phrases. Finite p-groups, modular group algebra, invariants, Modular Isomorphism Problem.
Partially supported by Grant PID2020-113206GB-I00 funded by MCIN/AEI/10.13039/501100011033 and by Grant Fundación Séneca 22004/PI/22.

Observe that if G and H are as in the previous theorems, then $G \cong H$ if and only if $\mathrm{inv}(G) = \mathrm{inv}(H)$, so Theorem B is another step towards a solution of the Modular Isomorphism Problem for our target class of groups. As an application we obtain a positive answer for the Modular Isomorphism Problem for 2-generated p-groups with $p > 2$ having cyclic derived subgroup and order at most p^{11}. Moreover, for groups of order p^{12} we also obtain a positive solution except for $p - 2$ families of containing p groups each.

The paper is organized as follows. In Section 1 we establish the notation and prove some general auxiliary results. In the remainder of the paper, p is an odd prime and all the groups are 2-generated finite p-groups with cyclic derived subgroup. In Section 2 we recall the classification of such groups from [4] and establish some basic facts for these groups and their group algebras. In Section 3 we prove Theorems A and B. Finally, in Section 4 we prove the mentioned results about groups of small order.

1. Preliminaries

Throughout the paper, p denotes an odd prime number, k is the field with p elements, G is a finite p-group and N is a normal subgroup of G. The group algebra of G over k is denoted by kG and its *augmentation ideal* is denoted by $\mathrm{I}(G)$. It is a classical result that $\mathrm{I}(G)$ is also the Jacobson ideal of kG. If C is a subset of G then $\hat{C} = \sum_{c \in C} c \in kG$. It is well known that the center $\mathrm{Z}(kG)$ is the k-span of the class sums $\hat{C}$ with C running on the set $\mathrm{Cl}(G)$ of conjugacy classes of G. The rest of group theoretical notation is mostly standard: $[g, h] = g^{-1}h^{-1}gh$ for $g, h \in G$, $|G|$ denotes the order of G, $\mathrm{Z}(G)$ its center, $\{\gamma_i(G)\}_{i \geq 1}$ its lower central series and $G' = \gamma_2(G)$ its commutator subgroup. For $n \geq 1$, we denote by C_n the cyclic group of order n. Moreover, if $g \in G$ and $X \subseteq G$ then $|g|$ denotes the order of g and $\mathrm{C}_G(X)$ the centralizer of X in G. For a subgroup A of G, we denote $A^n = \langle a^n : x \in A \rangle$. If A is normal cyclic subgroup of G, then $\mathrm{I}(A^{p^n}) = \mathrm{I}(A)^{p^n}$ and hence $(\mathrm{I}(A)kG)^{p^n} = \mathrm{I}(A)^{p^n}kG = \mathrm{I}(A^{p^n})kG$.

We take the following the following notation from [4] for integers s, t and n with $n \geq 0$:

$$\mathcal{S}(s \mid n) = \sum_{i=0}^{n-1} s^i.$$

We will use the following elementary lemma.

Lemma 1.1. *If G is a finite p-group with cyclic derived subgroup and $p > 2$, then every conjugacy class of G is a coset modulo a subgroup of G'.*

Proof. Let C be a conjugacy class of G, let $g \in C$ and $H = \{[x, g^{-1}] : x \in G\}$. Then $C = Hg$ and hence it is enough to prove that H is a subgroup of G'. As G' is cyclic and $H \subseteq G'$, it is enough to prove that if $h \in H$ then $h^i \in H$ for every non-negative integer i. Let $h = [x, g^{-1}]$ with $x \in G$. Then $h^x = h^r$ for some integer r with $r \equiv 1 \mod p$. Therefore, using [4, Lemma 2.1], we have $[x^i, g^{-1}] = x^{-i}(x^i)^{g^{-1}} = x^{-i}(x^{g^{-1}})^i = x^{-i}(xh)^i = h^{\mathcal{S}(r|i)}$. This proves that H contains all the elements of the form $h^{\mathcal{S}(r|i)}$ with $i \geq 0$. By [8, Lemma 2.2] we deduce that H contains h^i for every non-negative integer. □

Let n be a positive integer. We set

$$\Omega_n(G) = \left\langle g \in G : g^{p^n} = 1 \right\rangle \quad \text{and} \quad \Omega_n(G : N) = \left\langle g \in G : g^{p^n} \in N \right\rangle.$$

Observe that $\Omega_n(G : N)$ is the only subgroup of G containing N such that

$$\Omega_n(G : N)/N = \Omega_n(G/N).$$

The next lemma collects some well-known results about the Modular Isomorphism Problem which will be used throughout the paper.

Lemma 1.2. *The Modular Isomorphism Problem has a positive solution for G if one of the following holds:*

(1) G is abelian [5].
(2) G is metacyclic [1, 13].
(3) G is 2-generated of class 2 [3].

1.1. **The Jennings series.** We denote $\mathrm{D}_n(G)$ the n-th term of the *Jennings series* of G, i.e.

$$\mathrm{D}_n(G) = \{g \in G : g-1 \in \mathrm{I}(G)^n\} = \prod_{ip^j \geq n} \gamma_i(G)^{p^j}.$$

It is straightforward (see [6, Lemma 4.10]) that

$$G \cap (1 + \mathrm{I}(G)^n + \mathrm{I}(N)kG) = \mathrm{D}_n(G)N. \tag{1.1}$$

Each quotient $\mathrm{D}_n(G)/\mathrm{D}_{n+1}(G)$ is elementary abelian and, if t is the smallest non-negative integer with $\mathrm{D}_{t+1}(G) = 1$, then a *Jennings set* of G is a subset $\{g_{11}, \ldots, g_{1d_1}, g_{21}, \ldots, g_{2d_2}, \ldots | g_{t1}, \ldots, g_{td_t}\}$ of G such that $g_{i1}\mathrm{D}_{i+1}(G), \ldots, g_{id_i}\mathrm{D}_{i+1}(G)$ is a basis of $\mathrm{D}_n(G)/\mathrm{D}_{n+1}(G)$ for each i. Observe that $|G| = p^{\sum_{i=1}^{t} d_i}$. If $x_1, \ldots, x_n$ are the elements of a Jennings set of G, in some order, then

$$\mathscr{B} = \{(x_1-1)^{e_1} \cdots (x_n-1)^{e_n} : 0 \leq e_i \leq p-1 \text{ and } \sum_{i=1}^{n} e_i > 0\}$$

is a basis of $\mathrm{I}(G)$, called a *Jennings basis* of $\mathrm{I}(G)$ associated to the given Jennings set. We denote $\mathscr{B}^n = \mathscr{B} \cap \mathrm{I}(G)^n$, which is a basis of $\mathrm{I}(G)^n$.

Lemma 1.3. *There is a Jennings set $\mathscr{S}$ of G such that $N \cap \mathscr{S}$ is a Jennings set of N.*

Proof. We argue by induction on $|N|$. If $|N| = 1$, then there is nothing to prove. Now suppose that the result holds for normal subgroups of order p^n, and assume that N has order p^{n+1}. Since G is a p-group, the center of G intersects N non-trivially, so we can choose a subgroup $L \subseteq N \cap \mathrm{Z}(G)$ of order p. By the induction hypothesis, we can choose a Jennings set $\bar{\mathscr{S}}$ of G/L such that $\bar{\mathscr{S}} \cap (N/L)$ is a Jennings set of N/L. Let $\mathscr{S}$ be a set of representatives of the elements of $\bar{\mathscr{S}}$ in G. Clearly, the representatives of elements in N/L are in N. For some i we have that $L \subseteq D_i(G)$ but $L \not\subseteq D_{i+1}(G)$, and for some j, that $L \subseteq \mathrm{D}_j(N)$ but $L \not\subseteq \mathrm{D}_{j+1}(N)$. Observe that $\mathscr{S}$ is almost a Jennings basis of G except it does not contain representatives of a basis of $\mathrm{D}_i(G)/\mathrm{D}_{i+1}(G)$, only of a maximal linear subspace which is a direct complement of L. Similarly, $\mathscr{S} \cap N$ is almost a Jennings basis of N except it does not contain representatives of a basis of $\mathrm{D}_j(N)/\mathrm{D}_{j+1}(N)$, only of a maximal linear subspace which is a direct complement of L. Hence it suffices to take the Jennings set $\mathscr{S} \cup \{l\}$, where l is a generator of L. □

The following equality is [14, Theorem A] and its symmetric analogue:

$$\mathrm{D}_{n+1}(N) = G \cap (1 + \mathrm{I}(N)^n\mathrm{I}(G)) = G \cap (1 + \mathrm{I}(G)\mathrm{I}(N)^n). \tag{1.2}$$

It can be generalized as follows.

Lemma 1.4. *If n and m are positive integers, then*

$$(1 + \mathrm{I}(G)^n + \mathrm{I}(N)^m\mathrm{I}(G)) \cap G = \mathrm{D}_n(G)\mathrm{D}_{m+1}(N) = (1 + \mathrm{I}(G)^n + \mathrm{I}(G)\mathrm{I}(N)^m) \cap G.$$

Proof. We prove only the first identity, the second being analogous. Since $(1 + \mathrm{I}(G)^n) \cap G = \mathrm{D}_n(G)$ and $(1 + \mathrm{I}(N)^m\mathrm{I}(G)) \cap G \supseteq (1 + \mathrm{I}(N)^{m+1}) \cap G = \mathrm{D}_{m+1}(N)$, the right-to-left inclusion is clear. Thus it suffices to prove the converse. Taking quotients modulo $\mathrm{D}_n(G)\mathrm{D}_{m+1}(N)$, it is enough to prove that

$$\mathrm{D}_n(G)\mathrm{D}_{m+1}(N) = 1 \qquad \text{implies} \qquad (1 + \mathrm{I}(G)^n + \mathrm{I}(N)^m\mathrm{I}(G)) \cap G = 1. \tag{1.3}$$

By Lemma 1.3, there is a Jennings set $\mathscr{S}$ of G such that $N \cap \mathscr{S}$ is a Jennings set of N. Ordering the elements of $\mathscr{S}$ so that those in N are placed first we obtain a Jennings basis $\mathscr{B}$ of $\mathrm{I}(G)$ associated to $\mathscr{S}$ containing a Jennings basis $\mathscr{B}_0$ of $\mathrm{I}(N)$ associated to $N \cap \mathscr{S}$. Recall that the set $\mathscr{B}^n = \mathscr{B} \cap \mathrm{I}(G)^n$ is a basis of $\mathrm{I}(G)^n$. Moreover, the set $\mathscr{B}_0^m = \mathscr{B} \cap \mathrm{I}(N)^m\mathrm{I}(G)$ is a basis of $\mathrm{I}(N)^m\mathrm{I}(G)$, and coincides with the set of elements of $\mathscr{B}$ of the form xy with $x \in \mathscr{B}_0 \cap \mathrm{I}(N)^m$ and $y \in \mathrm{I}(G)$. Then the following implication is clear: if $y \in \mathscr{B}$ occurs in the support in the basis $\mathscr{B}$ of an element $x \in \mathrm{I}(G)^n + \mathrm{I}(N)^m\mathrm{I}(G)$, then $y \in \mathscr{B}^n \cup \mathscr{B}_0^m$.

Moreover, it is clear $(1 + \mathscr{B}^n) \cap G \subseteq (1 + \mathrm{I}(G)^n) \cap G = \mathrm{D}_n(G)$ and $(1 + \mathscr{B}_0^m) \cap G \subseteq (1 + \mathrm{I}(N)^m\mathrm{I}(G)) \cap G = \mathrm{D}_{m+1}(N)$ by (1.2). Thus $(1 + \mathscr{B}^n \cup \mathscr{B}_0^m) \cap G \subseteq \mathrm{D}_n(G)\mathrm{D}_{m+1}(N)$.

We prove (1.3) by induction on m. Suppose first that $m = 1$ and that $\mathrm{D}_n(G)\mathrm{D}_2(N) = 1$, so (1.1) yields

$$(1 + \mathrm{I}(G)^n + \mathrm{I}(N)\mathrm{I}(G)) \cap G \subseteq (1 + \mathrm{I}(G)^n + \mathrm{I}(N)kG) = \mathrm{D}_n(G)N = N.$$

So, if $1 \neq g \in (1 + \mathrm{I}(G)^n + \mathrm{I}(N)\mathrm{I}(G)) \cap G$, then $g \in N$. Since N is elementary abelian, $g - 1 \in \mathrm{I}(N) \setminus \mathrm{I}(N)^2$. Thus the support of $g-1$ in the basis $\mathscr{B}_0$ contains an element of the form $h-1$, with $1 \neq h \in N$. Then, by the two previous paragraphs, $h \in (1 + \mathscr{B}^n \cup \mathscr{B}_0^1) \cap G \subseteq \mathrm{D}_n(G)\mathrm{D}_2(N) = 1$, a contradiction.

For $m > 1$, the induction step is similar. Suppose that $\mathrm{D}_n(G)\mathrm{D}_{m+1}(N) = 1$, so $\mathrm{D}_m(N)$ is elementary abelian. Take

$$1 \neq g \in (1 + \mathrm{I}(G)^n + \mathrm{I}(N)^m\mathrm{I}(G)) \cap G \subseteq (1 + \mathrm{I}(G)^n + \mathrm{I}(N)^{m-1}\mathrm{I}(G)) = \mathrm{D}_n(G)\mathrm{D}_m(N) = \mathrm{D}_m(N).$$

Since $\mathscr{B}_0 \cap \mathrm{I}(\mathrm{D}_m(N))$ is a Jennings basis of $\mathrm{I}(\mathrm{D}_m(N))$ and $g - 1 \in \mathrm{I}(\mathrm{D}_m(N)) \setminus \mathrm{I}(\mathrm{D}_m(N))^2$, we have that the support of $g - 1$ in this basis (and hence in the basis $\mathscr{B}$) contains an element of the form $h - 1$, with $1 \neq h \in \mathrm{D}_m(N)$. However, $h \in (1 + \mathscr{B}^n \cup \mathscr{B}_0^m) \subseteq \mathrm{D}_n(G)\mathrm{D}_{m+1}(N) = 1$, a contradiction. □

1.2. **The relative lower central series.** The *lower central series of N relative to G* is the series defined recursively by

$$\gamma_1^G(N) = G \quad \text{and} \quad \gamma_{n+1}^G(N) = [\gamma_n^G(N), N].$$

We consider also the sequence of ideals of kG defined recursively by setting

$$\mathrm{J}^1(N, G) = \mathrm{I}(N)\mathrm{I}(G) \quad \text{and} \quad \mathrm{J}^{+1}(N, G) = \mathrm{I}(N)\mathrm{J}^i(N, G) + \mathrm{J}^i(N, G)\mathrm{I}(N).$$

This can be also defined with a closed formulae:

$$\mathrm{J}^n(N, G) = \mathrm{I}(N)^n\mathrm{I}(G) + \sum_{i=1}^{n-1} \mathrm{I}(N)^{n-i}\mathrm{I}(G)\mathrm{I}(N)^i. \tag{1.4}$$

From $\mathrm{I}(N)kG = kG\mathrm{I}(N)$ and (1.4) it easily follows that

$$\mathrm{I}(N)^n\mathrm{I}(G) \subseteq \mathrm{J}^n(N, G) \subseteq \mathrm{I}(N)^n kG. \tag{1.5}$$

Lemma 1.5. *The following is a well defined map:*

$$\Lambda_N^n = \Lambda_{N,G}^n : \frac{\mathrm{I}(N)kG}{\mathrm{I}(N)\mathrm{I}(G)} \longrightarrow \frac{\mathrm{I}(N)^{p^n}kG}{\mathrm{J}^{p^n}(N, G)}, \qquad x + \mathrm{I}(N)\mathrm{I}(G) \mapsto x^{p^n} + \mathrm{J}^{p^n}(N, G).$$

Proof. Let $x \in \mathrm{I}(N)kG$ and $y \in \mathrm{I}(N)\mathrm{I}(G)$. Then $(x + y)^{p^n} - x^{p^n} = \sum_i a_i$ where each a_i is a product of p elements of $\{x, y\}$ with at least one equal to y. Hence each $a_i \in I_1 \dots I_{p^n}$, where each I_i is either $\mathrm{I}(N)kG$ or $\mathrm{I}(N)\mathrm{I}(G)$, and at least one of the I_i's is of the second type. Since $\mathrm{I}(N)\mathrm{I}(G) \subseteq \mathrm{I}(N)kG$, $I_1 \dots I_{p^n} \subseteq I(N)^{p^n-j}I(G)I(N)^j$ for some $0 \leq j \leq p^n$, and hence, by (1.4), $I_1 \dots I_{p^n} \subseteq \mathrm{J}^{p^n}(N, G)$. Therefore $(x+y)^{p^n} - x^{p^n} \in \mathrm{J}^{p^n}(N, G)$, so Λ_N^n is well defined. □

The ambient group G will be always clear from the context so we just write Λ_N^n. In particular,

$$\Lambda_G^n : \frac{\mathrm{I}(G)}{\mathrm{I}(G)^2} \to \frac{\mathrm{I}(G)^{p^n}}{\mathrm{I}(G)^{p^n+1}}$$

is the usual map used in the *kernel size* computations (see [9]).

The first statement of the next lemma is just a slight modification of a well-known identity (see [12, Lemma 2.2]), while the second one is inspired, together with the definition of the ideals $\mathrm{J}^i(N, G)$, by the first section of [2]. For the convenience of the reader we include a proof.

Lemma 1.6. *Let L and N be normal subgroups of G. Then the following equations hold*

$$\mathrm{I}(L)\mathrm{I}(N)kG + \mathrm{I}(N)\mathrm{I}(L)kG = \mathrm{I}([L, N])kG + \mathrm{I}(N)\mathrm{I}(L)kG, \tag{1.6}$$

$$\mathrm{J}^n(N, G) = \sum_{i=1}^{n} \mathrm{I}(N)^{n+1-i}\mathrm{I}(\gamma_i^G(N))kG. \tag{1.7}$$

Proof. Since the terms at both sides of (1.6) are two-sided ideals of kG, the equation follows from

$$(g - 1)(h - 1) = hg([g, h] - 1) + (h - 1)(g - 1) \qquad \text{for } g, h \in G.$$

In order to prove (1.7) we proceed by induction on n. For $n = 1$ there is nothing to prove, and the following chain of equations

$$\begin{aligned}
\mathrm{J}^{n+1}(N,G) &= \mathrm{J}^n(N,G)\mathrm{I}(N) + \mathrm{I}(N)\mathrm{J}^n(N,G)\\
&= \sum_{i=1}^{n} \mathrm{I}(N)^{n+1-i}\mathrm{I}(\gamma_i^G(N))kG\mathrm{I}(N) + \mathrm{I}(N)\sum_{i=1}^{n} \mathrm{I}(N)^{n+1-i}\mathrm{I}(\gamma_i^G(N))kG\\
&= \sum_{i=1}^{n} \mathrm{I}(N)^{n+1-i}\left[\mathrm{I}(\gamma_i^G(N))\mathrm{I}(N)kG + \mathrm{I}(N)\mathrm{I}(\gamma_i^G(N))kG\right]\\
\text{(by (1.6) with } L=\gamma_i^G(N)) &= \sum_{i=1}^{n} \mathrm{I}(N)^{n+1-i}\left(\mathrm{I}(\gamma_{i+1}^G(N))kG + \mathrm{I}(N)\mathrm{I}(\gamma_i^G(N))kG\right)\\
&= \sum_{i=1}^{n+1} \mathrm{I}(N)^{n+2-i}\mathrm{I}(\gamma_i^G(N))kG
\end{aligned}$$

completes the induction argument. □

Lemma 1.7. *Let N be a normal subgroup of G.*

(1) If $\gamma_i^G(N) \subseteq \mathrm{D}_i(N)$ for every $i \geq 2$ then for every $n \geq 1$ we have $\mathrm{J}^n(N,G) = \mathrm{I}(N)^n\mathrm{I}(G)$.
(2) If $[G,N] \subseteq N^p$ then $\gamma_i^G(N) \subseteq \mathrm{D}_i(N)$ for every $i \geq 2$.

Proof. (1) Suppose that $\gamma_i^G(N) \subseteq \mathrm{D}_i(N)$ for $i \geq 2$. Since $\mathrm{D}_i(N) \subseteq 1 + \mathrm{I}(N)^i$, it follows that if $i \geq 2$ then $\mathrm{I}(\gamma_i^G(N)) \subseteq \mathrm{I}(N)^i$ and hence, using (1.7) we have

$$\mathrm{J}^s(N,G) = \mathrm{I}(N)^s\mathrm{I}(G) + \sum_{i=2}^{s} \mathrm{I}(N)^{s+i-1}\mathrm{I}(\gamma_i^G(N))kG \subseteq \mathrm{I}(N)^s\mathrm{I}(G) + \mathrm{I}(N)^{s+1}kG \subseteq \mathrm{I}(N)^s\mathrm{I}(G).$$

This, together with (1.5), completes the proof.

(2) Suppose that $[G,N] \subseteq N^p$. Then $\gamma_2^G(N) = [G,N] \subseteq N^p \subseteq \mathrm{D}_2(N)$. Then arguing by induction on i, for every $i \geq 3$ we obtain $\gamma_i^G(N) = [\gamma_{i-1}^G(N), N] \subseteq [\mathrm{D}_{i-1}(N), \mathrm{D}_1(N)] \subseteq \mathrm{D}_i(N)$, because $(\mathrm{D}_i(N))_i$ is an N_p-series. □

1.3. **Canonical subquotients and maps.** Let $\mathcal{G}$ be a class of groups. Roughly speaking, we say that a certain assignation defined on $\mathcal{G}$ is canonical if it "depends only on the isomorphism type of kG as k-algebra". More precisely, suppose that for each G in $\mathcal{G}$ we have associated a subquotient U_G of kG as k-space. We say that $G \mapsto U_G$ is canonical in $\mathcal{G}$ if every isomorphism k-algebras $\psi : kG \to kH$, with G and H in $\mathcal{G}$, induces an isomorphism $\tilde{\psi} : U_G \mapsto U_H$ in the natural way. If $(G \mapsto U_G^{(x)})_{x\in X}$ is a family of canonical subquotients in $\mathcal{G}$ then we also say that $G \mapsto \prod_{x\in X} U_G^{(x)}$ is canonical in $\mathcal{G}$. In this case every isomorphism $\psi : kG \to kH$ with G and H in $\mathcal{G}$ induces an isomorphism $\prod_{x\in X} U_G^{(x)} \to \prod_{x\in X} U_H^{(x)}$ in the natural way.

Lemma 1.8. *The following assignations are canonical in the class of p-groups:*

- $G \mapsto \mathrm{I}(\Omega_n(G : G'))kG$.
- $G \mapsto \mathrm{I}(\Omega_n(G : \mathrm{Z}(G)G'))kG$.

Proof. See [8, Proposition 2.3(1) and Lemma 3.6]. □

Lemma 1.9. [8, Theorem 4.2(1)] *The assignation $G \mapsto \mathrm{I}(\mathrm{C}_G(G'))kG$ is canonical in the class of p-groups with cyclic derived subgroup and p odd.*

We note that, if $G \mapsto \mathrm{I}(N_G)kG$ is canonical in $\mathcal{G}$, where N_G is a normal subgroup of G, then an easy induction on n shows that $G \mapsto \mathrm{J}^n(N_G, G))$ is canonical in $\mathcal{G}$ too.

Now suppose that for each G in $\mathcal{G}$ we have associated a map $f_G : U_G \to V_G$, with U and V products of canonical subquotients in $\mathcal{G}$. We say that $G \mapsto f_G$ is *canonical* if for every isomorphism $\psi : kG \to kH$ the

following square is commutative

$$\begin{array}{ccc} U_G & \xrightarrow{f_G} & V_G \\ {\scriptstyle\tilde{\psi}}\downarrow & & \downarrow{\scriptstyle\tilde{\psi}} \\ U_H & \xrightarrow[f_H]{} & V_H \end{array}$$

For example, the assignation $G \mapsto \Lambda^n_G$ described above is canonical in the class of finite p-groups, and so is $G \mapsto \Delta_G$, where Δ_G is the natural projection:

$$\Delta_G : \frac{\mathrm{I}(G')kG}{\mathrm{I}(G')\mathrm{I}(G)} \longrightarrow \frac{\mathrm{I}(G')kG + \mathrm{I}(G)^3}{\mathrm{I}(G)^3}, \quad x + \mathrm{I}(G')\mathrm{I}(G) \mapsto x + \mathrm{I}(G)^3.$$

Observe that Δ_G is well defined homomorphism of k-algebras because $\mathrm{I}(G') \subseteq \mathrm{I}(G)^2$.

In order to simplify notation, instead of writing "$G \mapsto A_G$ is canonical" we just write "A_G is canonical", where A_G is either a product of subquotients or a map between canonical products of subquotients.

For mnemonic purposes we use variations of the symbols Λ^n and Υ^n for maps of the kind $x \mapsto x^{p^n}$. Moreover we will encounter a number of projection maps of the kind $x + I \mapsto x + J$ for ideals $I \subseteq J$, for which we use variations of the symbols Δ, ζ and ν, with the hope they help the reader to recall the domain: Δ refers to derived subgroup, ζ to center and ν to some normal subgroup N. Other projection maps are denoted with variations of π and η.

2. 2-generated finite p-groups with cyclic derived subgroup

The non-abelian 2-generated finite p-groups with cyclic derived subgroup have been classified in [4] in terms of numerical invariants. For the reader's convenience, we include in the following theorem a simplification of this classification for the case $p > 2$.

Theorem 2.1 ([4])**.** *For a list of non-negative integers $I = (p, m, n_1, n_2, o_1, o_2, o_1', o_2', u_1, u_2)$ where $p > 2$ is a prime number, let $\mathcal{G}_I$ be the group defined by*

$$\mathcal{G}_I = \left\langle b_1, b_2, a = [b_2, b_1] \mid a^{p^m} = 1, a^{b_i} = a^{r_i}, b_i^{p^{n_i}} = a^{u_i p^{m-o_i'}} \right\rangle,$$

where

$$r_1 = 1 + p^{m-o_1} \quad \text{and} \quad r_2 = \begin{cases} 1 + p^{m-o_2}, & \text{if } o_2 > o_1; \\ r_1^{p^{o_1-o_2}}, & \text{otherwise.} \end{cases} \tag{2.1}$$

Then $I \mapsto [\mathcal{G}_I]$, where $[\mathcal{G}_I]$ denotes the isomorphism class of $\mathcal{G}_I$, defines a bijection between the set of lists of integers $(p, m, n_1, n_2, o_1, o_2, o_1', o_2', u_1, u_2)$ satisfying conditions (I)-(VI), and the isomorphism classes of 2-generated non-abelian groups of odd prime-power order with cyclic derived subgroup.

- *(I)* *p is prime and $n_1 \geq n_2 \geq 1$.*
- *(II)* *$0 \leq o_i < \min(m, n_i)$, $0 \leq o_i' \leq m - o_i$ and $p \nmid u_i$ for $i = 1, 2$.*
- *(III)* *One of the following conditions holds:*
  - *(a)* *$o_1 = 0$ and $o_1' \leq o_2' \leq o_1' + o_2 + n_1 - n_2$.*
  - *(b)* *$o_2 = 0 < o_1$, $n_2 < n_1$ and $o_1' + \min(0, n_1 - n_2 - o_1) \leq o_2' \leq o_1' + n_1 - n_2$.*
  - *(c)* *$0 < o_2 < o_1 < o_2 + n_1 - n_2$ and $o_1' \leq o_2' \leq o_1' + n_1 - n_2$.*
- *(IV)* *$o_2 + o_1' \leq m \leq n_1$ and one of the following conditions hold:*
  - *(a)* *$o_1 + o_2' \leq m \leq n_2$.*
  - *(b)* *$2m - o_1 - o_2' = n_2 < m$ and $u_2 \equiv 1 \mod p^{m-n_2}$.*
- *(V)* *$1 \leq u_1 \leq p^{a_1}$, where $a_1 = \min(o_1', o_2 + \min(n_1 - n_2 + o_1' - o_2', 0))$.*
- *(VI)* *One of the following conditions holds:*
  - *(a)* *$1 \leq u_2 \leq p^{a_2}$.*
  - *(b)* *$o_1 o_2 \neq 0$, $n_1 - n_2 + o_1' - o_2' = 0 < a_1$, $1 + p^{a_2} \leq u_2 \leq 2p^{a_2}$, and $u_1 \equiv 1 \mod p$;*

  where

$$a_2 = \begin{cases} 0, & \text{if } o_1 = 0; \\ \min(o_1, o_2', o_2' - o_1' + \max(0, o_1 + n_2 - n_1)), & \text{if } o_2 = 0 < o_1; \\ \min(o_1 - o_2, o_2' - o_1'), & \text{otherwise.} \end{cases}$$

For every non-abelian 2-generated finite p-group Γ with cyclic derived subgroup and p odd, let $\mathrm{inv}(\Gamma)$ denote the unique list satisfying the conditions of the previous theorem such that Γ is isomorphic to $\mathcal{G}_{\mathrm{inv}(\Gamma)}$. An explicit description of $\mathrm{inv}(\Gamma)$ can be found in [4] and also in [8]. In these references the list $\mathrm{inv}(\Gamma)$ has two additional entries σ_1 and σ_2 which for $p > 2$ always equal 1, so we drop them.

In this section Γ is a 2-generated finite p-group with cyclic derived subgroup, and we set

$$\mathrm{inv}(\Gamma) = (p, m, n_1, n_2, o_1, o_2, o_1', o_2', u_1, u_2).$$

Hence Γ is given by the following presentation

$$\Gamma = \left\langle b_1, b_2 \mid a = [b_2, b_1], a^{b_i} = a^{r_i}, b_i^{p^{n_i}} = a^{u_i p^{m-o_i'}} \right\rangle,$$

where r_1 and r_2 are as in (2.1). By [8, Lemma 3.5],

$$\gamma_n(\Gamma) = \left\langle a^{p^{(n-2)(m-\max(o_1,o_2))}} \right\rangle, \text{ for } n \geq 2. \tag{2.2}$$

In particular $[\Gamma, \Gamma'] = \gamma_3(\Gamma) \subseteq \langle a^p \rangle = (\Gamma')^p$, and hence, by Lemma 1.7,

$$\mathrm{J}^n(\Gamma', \Gamma) = \mathrm{I}(\Gamma')^n \mathrm{I}(\Gamma) \text{ for every } n \geq 1.$$

By [8, Lemma 2.2], there is a unique integer δ satisfying

$$1 \leq \delta \leq p^{o_1} \quad \text{and} \quad \mathcal{S}\left(r_2 \mid \delta p^{m-o_1}\right) \equiv -p^{m-o_1} \mod p^m. \tag{2.3}$$

Moreover, $p \nmid \delta$. By [8, Lemma 3.7]

$$\mathrm{Z}(\Gamma) = \left\langle b_1^{p^m}, b_2^{p^m}, c \right\rangle, \quad \text{where } c = \begin{cases} b_1^{\delta p^{m-o_2}} a, & \text{if } o_1 = 0; \\ b_1^{-\delta p^{m-o_2}} b_2^{\delta p^{m-o_1}} a, & \text{otherwise.} \end{cases} \tag{2.4}$$

Observe that

$$n < n_i \quad \text{implies} \quad b_i^{p^n} \notin \mathrm{D}_{p^n+1}(\Gamma)\Gamma', \text{ for } i = 1, 2. \tag{2.5}$$

Furthermore, for every $n \geq 0$,

$$\mathrm{D}_{p^n}(\Gamma) = \Gamma^{p^n}. \tag{2.6}$$

To prove this t suffices to show that $ip^j \geq p^n$ implies $\gamma_i(\Gamma)^{p^j} \subseteq \Gamma^{p^n}$. This is clear if $j \geq n$. Otherwise, $j < n$, $i \geq 2$ and $i - 2 \geq p^{n-j} - 2 \geq n - j$, since $p \geq 3$. Using (2.2) we obtain that $\gamma_i(\Gamma)^{p^j} = \left\langle a^{p^{j+(i-2)(m-\max(o_1,o_2))}} \right\rangle \subseteq \left\langle a^{p^n} \right\rangle \subseteq \Gamma^{p^n}$. Thus (2.6) follows.

Moreover,

$$n_1 = m \qquad \text{implies} \qquad o_1 o_2 = 0. \tag{2.7}$$

To see this, observe that if $o_1 o_2 > 0$ and $n_1 = m$ then $m > n_2$ by condition *(III)*, so $n_2 = 2m - o_1 - o_2'$ by condition *(IV)*. Thus, by conditions *(II)* and *(III)*, $o_1 - o_2 < n_1 - n_2 = o_1 + o_2' - m \leq o_1 - o_2$, a contradiction.

In the rest of this section we assume the following:

$$o_1 \neq o_2, \quad 0 < \max(o_1', o_2') < m \quad \text{and} \quad n_2 \geq 2. \tag{2.8}$$

In the next section we will see that this is the only case of interest, as if any of these conditions fails, then the Modular Isomorphism Problem has a positive solution for Γ.

Observe that if $n < m - 1$ then $\mathrm{I}(\Gamma')^{p^n} k\Gamma / \mathrm{I}(\Gamma')^{p^n} \mathrm{I}(\Gamma)$ is a one-dimensional k-space generated by the class of $a^{p^n} - 1$. Moreover the image of Δ_Γ is spanned by $a - 1 + \mathrm{I}(\Gamma)^3$. As p is odd, $\Gamma^p = \mathrm{D}_3(\Gamma)$, and as $\max(o_1', o_2') < m$, $a \notin \Gamma^p$. Thus $a - 1 \notin \mathrm{I}(\Gamma)^3$. Then, we have the following

Lemma 2.2. *Δ_Γ is an isomorphism.*

Lemma 2.3. *$\hat{C} \in \mathrm{I}(\Gamma)^{(p-1)p^m}$ for each non-central conjugacy class C of Γ.*

Proof. By hypothesis $o_i' > 0$ for some $i \in \{1,2\}$. In that case $m \leq n_i + o_i' - 1$, by condition *(IV)*. Thus, it is enough to show that if $o_i' > 0$, then $\hat{C} \in \mathrm{I}(\Gamma)^{(p-1)p^{n_i+o_i'-1}}$.

If x is an indeterminate over k and $n \geq 1$ then we have

$$\sum_{i=1}^{p^n-1} x^i = \frac{x^{p^n}-1}{x-1} = (x-1)^{p^n-1}.$$

Hence, using Lemma 1.1 for each $C \in \mathrm{Cl}(\Gamma)$ such that $|C| > 1$, and $g \in C$, there exists $0 \leq n < m$ such that

$$\begin{aligned}\hat{C} = \sum_{i=0}^{p^{m-n}-1} a^{ip^n} g = (a^{p^n}-1)^{p^{m-n}-1} g &= (a^{p^n}-1)^{(p-1)p^{m-n-1}} (a^{p^n}-1)^{p^{m-n-1}-1} g \\ &= (a^{p^{m-1}}-1)^{(p-1)} (a^{p^n}-1)^{p^{m-n-1}-1} g,\end{aligned}$$

and this element belongs to $\mathrm{I}(\Gamma)^{(p-1)p^{n_i+o_i'-1}}$, as the hypothesis $o_i' > 0$ implies

$$a^{p^{m-1}} = b_i^{p^{n_i+o_i'-1}} \in \mathrm{D}_{p^{n_i+o_i'-1}}(\Gamma).$$

□

In the remainder of the section we consider a series of subquotients of $k\Gamma$ and maps which, by construction, are canonical in the class of 2-generated finite p-groups with cyclic derived subgroup satisfying (2.8), and will play a central rôle in the proof of our main results.

Recall from [11, Lemma 6.10] that

$$\mathrm{Z}(\mathrm{I}(\Gamma)) = \mathrm{I}(\mathrm{Z}(\Gamma)) \oplus \left(\bigoplus_{C \in \mathrm{Cl}(\Gamma), |C|>1} k\hat{C} \right). \tag{2.9}$$

Observe that as $o_i < m$ for $i = 1, 2$, $c \in \mathrm{D}_2(\Gamma)$, where c is as in (2.4), hence $c-1 \in \mathrm{I}(\Gamma)^2$. Then Lemma 2.3 and (2.9) yield

$$\begin{aligned}\frac{\mathrm{Z}(I(\Gamma)) + \mathrm{I}(\Gamma)^{p^m}}{\mathrm{I}(\Gamma)^{p^m}} &= \frac{\mathrm{I}(\mathrm{Z}(\Gamma)) + \mathrm{I}(\Gamma)^{p^m}}{\mathrm{I}(\Gamma)^{p^m}} \\ &= \frac{k(c-1) + k(c-1)^2 + \cdots + k(c-1)^{\frac{p^m-1}{2}} + \mathrm{I}(\Gamma)^{p^m}}{\mathrm{I}(\Gamma)^{p^m}}.\end{aligned} \tag{2.10}$$

Hence,

$$\frac{\mathrm{Z}(\mathrm{I}(\Gamma)) + \mathrm{I}(\Gamma)^3}{\mathrm{I}(\Gamma)^3} = \frac{k(a-1) + \mathrm{I}(\Gamma)^3}{\mathrm{I}(\Gamma)^3}$$

since $c - a \in \mathrm{I}(\Gamma)^3$, and, for $o = \max(o_1, o_2)$,

$$\frac{\mathrm{Z}(\mathrm{I}(\Gamma)) + \mathrm{I}(\Gamma)^{p^{m-o}+1} + \mathrm{I}(\Gamma')k\Gamma}{\mathrm{I}(\Gamma)^{p^{m-o}+1} + \mathrm{I}(\Gamma')k\Gamma} = \begin{cases} \frac{k(b_1^{p^{m-o_2}}-1) + \mathrm{I}(\Gamma)^{p^{m-o_2}+1} + \mathrm{I}(\Gamma')k\Gamma}{\mathrm{I}(\Gamma)^{p^{m-o_2}+1} + \mathrm{I}(\Gamma')k\Gamma}, & \text{if } o_1 = 0; \\ \frac{k(b_2^{p^{m-o_1}}-1) + \mathrm{I}(\Gamma)^{p^{m-o_1}+1} + \mathrm{I}(\Gamma')k\Gamma}{\mathrm{I}(\Gamma)^{p^{m-o_1}+1} + \mathrm{I}(\Gamma')k\Gamma}, & \text{if } o_1 \neq 0. \end{cases} \tag{2.11}$$

This subquotient of $k\Gamma$ is one-dimensional by (2.5) and [6, Lemma 4.10].

Then we consider the canonical maps

$$\zeta_\Gamma^1 : \frac{\mathrm{Z}(\mathrm{I}(\Gamma)) + \mathrm{I}(\Gamma)^{p^m}}{\mathrm{I}(\Gamma)^{p^m}} \to \frac{\mathrm{Z}(\mathrm{I}(\Gamma)) + \mathrm{I}(\Gamma)^3}{\mathrm{I}(\Gamma)^3},\ w + \mathrm{I}(\Gamma)^{p^m} \mapsto w + \mathrm{I}(\Gamma)^3,$$

and

$$\zeta_\Gamma^2 : \frac{\mathrm{Z}(\mathrm{I}(\Gamma)) + \mathrm{I}(\Gamma)^{p^m}}{\mathrm{I}(\Gamma)^{p^m}} \to \frac{\mathrm{Z}(\mathrm{I}(\Gamma)) + \mathrm{I}(\Gamma)^{p^{m-o}+1} + \mathrm{I}(\Gamma')k\Gamma}{\mathrm{I}(\Gamma)^{p^{m-o}+1} + \mathrm{I}(\Gamma')k\Gamma},\ w + \mathrm{I}(\Gamma)^{p^m} \mapsto w + \mathrm{I}(\Gamma)^{p^{m-o}+1} + \mathrm{I}(\Gamma')k\Gamma.$$

It is immediate that for $x_1, \dots, x_{(p^m-1)/2} \in k$,

$$\zeta_\Gamma^1\left(\sum_{i=1}^{\frac{p^m-1}{2}} x_i(c-1)^i + \mathrm{I}(\Gamma)^{p^m}\right) = x_1(a-1) + \mathrm{I}(\Gamma)^3$$

and

$$\zeta_\Gamma^2\left(\sum_{i=1}^{\frac{p^m-1}{2}} x_i(c-1)^i + \mathrm{I}(\Gamma)^{p^m}\right) = \begin{cases} x_1(b_1^{p^{m-o_2}}-1) + \mathrm{I}(\Gamma)^{p^{m-o}+1} + \mathrm{I}(\Gamma')k\Gamma, & \text{if } o_1 = 0; \\ x_1\delta(b_2^{p^{m-o_1}}-1) + \mathrm{I}(\Gamma)^{p^{m-o}+1} + \mathrm{I}(\Gamma')k\Gamma, & \text{if } o_1 \neq 0. \end{cases}$$

The first implies that $\mathrm{Im}\,(\zeta_\Gamma^1) = \mathrm{Im}\,(\Delta_\Gamma)$.

For each $n \geq 1$ let

$$\mathcal{C}_\Gamma = \frac{\mathrm{I}(C_\Gamma(\Gamma'))k\Gamma + \mathrm{I}(\Gamma)^2}{\mathrm{I}(\Gamma)^2} = \begin{cases} \frac{k(b_1-1)+\mathrm{I}(\Gamma)^2}{\mathrm{I}(\Gamma)^2}, & \text{if } o_1 = 0; \\ \frac{k(b_2-1)+\mathrm{I}(\Gamma)^2}{\mathrm{I}(\Gamma)^2}, & \text{if } o_1 \neq 0. \end{cases}$$

Then

$$\Lambda_\Gamma^n(\mathcal{C}_\Gamma) = \begin{cases} \frac{k(b_1-1)^{p^n}+\mathrm{I}(\Gamma)^{p^n+1}}{\mathrm{I}(\Gamma)^{p^n+1}}, & \text{if } o_1 = 0; \\ \frac{k(b_2-1)^{p^n}+\mathrm{I}(\Gamma)^{p^n+1}}{\mathrm{I}(\Gamma)^{p^n+1}}, & \text{if } o_1 \neq 0. \end{cases} \tag{2.12}$$

Let $\tilde{\Lambda}_\Gamma^n : \mathcal{C}_\Gamma \to \Lambda_\Gamma^n(\mathcal{C}_\Gamma)$ be the restriction of Λ_Γ^n to $\mathcal{C}_\Gamma$. By (2.5),

(2.13) if either $o_1 = 0$ and $n < n_1$ or $o_1 \neq 0$ and $n < n_2$, then $\tilde{\Lambda}_\Gamma^n$ is an isomorphism.

Observe that $m - o < n_i$ for $i = 1, 2$. Indeed, if $m - o \geq n_i$ then, as $o > 0$ and $o_2' < m$, by condition (2.8), $i = 2$ and $n_2 = 2m - o_1 - o_2' > m - o_1 \geq m - o$, a contradiction. Thus $\tilde{\Lambda}_\Gamma^{m-o}$ is an isomorphism and hence $\Lambda_\Gamma^{m-o}(\mathcal{C}_\Gamma)$ is one-dimensional. Therefore we have isomorphisms

$$\mathcal{C}_\Gamma \xrightarrow{\tilde{\Lambda}_\Gamma^{m-o}} \Lambda_\Gamma^{m-o}(\mathcal{C}_\Gamma) \xrightarrow{\pi_\Gamma} \frac{\mathrm{Z}(\mathrm{I}(\Gamma)) + \mathrm{I}(\Gamma)^{p^{m-o}+1} + \mathrm{I}(\Gamma')k\Gamma}{\mathrm{I}(\Gamma)^{p^{m-o}+1} + \mathrm{I}(\Gamma')k\Gamma} \tag{2.14}$$

where π_Γ is another natural projection, i.e. $\pi_\Gamma\left(x + \mathrm{I}(\Gamma)^{p^{m-o}+1}\right) = x + \mathrm{I}(\Gamma)^{p^{m-o}+1} + \mathrm{I}(\Gamma')k\Gamma$.

3. Proof of the main results

Recall that p is an odd prime integer and k the field with p elements. For the remainder of the paper, we fix the following notation. Let G denote a 2-generated finite p-group with cyclic derived subgroup, let H denote another group and let $\psi : kG \to kH$ be an isomorphism of k-algebras. By [8, Theorem C], H is 2-generated with cyclic derived subgroup, and $\mathrm{inv}(G)$ and $\mathrm{inv}(H)$ coincide in all but the last entries. So we may write

$$\mathrm{inv}(G) = (p, m, n_1, n_2, o_1, o_2, o_1', o_2', u_1^G, u_2^G) \quad \text{and} \quad \mathrm{inv}(H) = (p, m, n_1, n_2, o_1, o_2, o_1', o_2', u_1^H, u_2^H).$$

To give a positive answer to the Modular Isomorphism Problem in this case we should prove that $G \cong H$, or equivalently that $u_i^G = u_i^H$ for $i = 1, 2$. Unfortunately, we are only able to prove the statement of Theorem B, namely that $u_2^G \equiv u_2^H \mod p$ and, under some extra assumptions, that $u_1^G \equiv u_1^H \mod p$.

By statements (2) and (3) of Lemma 1.2, we may assume that the groups G and H are not metacyclic, and both are of class at least 3. The first is equivalent to $\max(o_1, o_2) > 0$ and the second is equivalent to $\max(o_1', o_2') < m$. In particular, $m \geq 2$. Moreover $n_2 \geq 2$, as otherwise $n_2 < m$ and condition *(IV)* yields $1 = n_2 = 2m - o_1 - o_2'$, but this last quantity is strictly greater than 1 because $\max(o_1, o_2') < m$, by condition *(II)* and since Γ is not metacyclic. We also have that $o_1 \neq o_2$ by condition *(III)*. Finally, if $o_i' = 0$ for some $i \in \{1, 2\}$, then $u_i^G = 1 = u_i^H$ by conditions *(V)* and *(VI)*; therefore we can assume that $\max(o_1', o_2') > 0$. Thus the conditions in (2.8) hold, so we can freely use the statements of the previous section.

In order to deal with G and H simultaneously, in the remainder of the paper Γ denotes a 2-generated finite p-group with cyclic derived subgroup such that

$$\mathrm{inv}(\Gamma) = (p, m, n_1, n_2, o_1, o_2, o_1', o_2', u_1^\Gamma, u_2^\Gamma).$$

3.1. **Proof of Theorem B.** Recall that $o = \max(o_1, o_2)$. We let

$$N_\Gamma = \begin{cases} \Omega_{m-o-1}(\Gamma : Z(\Gamma)\Gamma'), & \text{if either } o_1 = 0 \text{ or } o_2 = 0 \text{ and } o_1' \geq o_2'; \\ \Omega_{n_2-1}(\Gamma : \Gamma'), & \text{otherwise} \end{cases}$$

and

$$\mathcal{N}_\Gamma = \frac{\mathrm{I}(N_\Gamma)k\Gamma \cap \mathrm{I}(\Gamma)^p}{\mathrm{I}(N_\Gamma)\mathrm{I}(\Gamma)}.$$

By Lemma 1.8, the subquotients $\mathrm{I}(N_\Gamma)k\Gamma$, $\mathrm{J}^n(N_\Gamma, \Gamma)$ and $\mathcal{N}_\Gamma$ are canonical. Moreover,

$$N_\Gamma = \langle a, d, e \rangle, \quad \text{where} \quad (d, e) = \begin{cases} (b_1^p, b_2^{p^{o_2+1}}), & \text{if } o_1 = 0; \\ (b_2^p, b_1^{p^{o_1+1}}), & \text{if } o_2 = 0 \text{ and } o_1' \geq o_2'; \\ (b_2^p, b_1^{p^{n_1-n_2+1}}), & \text{otherwise;} \end{cases} \tag{3.1}$$

and $\mathcal{N}_\Gamma$ is spanned by the classes of $d-1$ and $e-1$.

Lemma 3.1. *For every $n \geq 0$, $\mathrm{J}^n(N_\Gamma, \Gamma) = \mathrm{I}(N_\Gamma)^n\mathrm{I}(\Gamma)$.*

Proof. Suppose first that either $o_1 = 0$ or $o_2 = 0$ and $o_1' \geq o_2'$. Then $\gamma_1^\Gamma(N_\Gamma) = \Gamma$, $\gamma_2^\Gamma(N_\Gamma) = (\Gamma')^p$, and $\gamma_i^\Gamma(N_\Gamma) = 1$ for $i \geq 3$. Since $\Gamma' \subseteq N_\Gamma$ and , it follows that

$$\mathrm{I}(N_\Gamma)^{n-1}\mathrm{I}((\Gamma')^p)k\Gamma \subseteq \mathrm{I}(N_\Gamma)^{n-1+p}k\Gamma \subseteq \mathrm{I}(N_\Gamma)^n\mathrm{I}(\Gamma).$$

Then the desired equality follows from (1.7).

Suppose that $o_1 \neq 0$ and either $o_2 \neq 0$ or $o_1' < o_2'$. Then again $\gamma_1^\Gamma(N_\Gamma) = \Gamma$, $\gamma_2^\Gamma(N_\Gamma) = (\Gamma')^p$ and $\mathrm{I}(N_\Gamma)^{n-1}\mathrm{I}((\Gamma')^p)k\Gamma \subseteq \mathrm{I}(N_\Gamma)^n\mathrm{I}(\Gamma)$. For $i \geq 3$, an easy induction argument, using the description of N_Γ in (3.1), shows that $\gamma_i^\Gamma(N_\Gamma) = (\Gamma')^{p^{1+(i-2)k}}$, where $k = n_1 - n_2 + 1 + m - o_1$ if $o_2 = 0$, and $k = 1 + m - o_2$ otherwise. Either way $k \geq 2$ and hence

$$\mathrm{I}(N_\Gamma)^{n+1-i}\mathrm{I}(\gamma_i^\Gamma(N_\Gamma))k\Gamma \subseteq \mathrm{I}(N_\Gamma)^{n+1-i}\mathrm{I}((\Gamma')^{p^{1+(i-2)k}})k\Gamma \subseteq \mathrm{I}(N_\Gamma)^{n+1-i+p^{1+(i-2)k}}k\Gamma \subseteq \mathrm{I}(N_\Gamma)^n\mathrm{I}(\Gamma).$$

Then again (1.7) yields the desired equality. □

Denote

$$\ell = \begin{cases} n_1 + o_1' - 2, & \text{if } o_1 = 0; \\ n_2 + o_2' - 2, & \text{otherwise.} \end{cases}$$

Combining Lemma 3.1 and (1.2) and using regularity it is easy to obtain

$$\Gamma \cap (1 + \mathrm{J}^{p^\ell}(N_\Gamma, \Gamma)) = 1. \tag{3.2}$$

The next lemma covers most cases of Theorem B.

Lemma 3.2. *The following hold:*

(1) $u_2^G \equiv u_2^H \mod p$.
(2) If $o_1 o_2 = 0$ *then* $u_1^G \equiv u_1^H \mod p$.

Proof. Let $t \in \{1, 2\}$ with $t = 2$ in case $o_1 o_2 \neq 0$, and let s be the other element of $\{1, 2\}$, i.e. $\{s, t\} = \{1, 2\}$. We have to prove that $u_t^G \equiv u_t^H \mod p$. If $a_t = 0$ then $u_t^G = u_t^G = 1$, so we assume that $a_t \neq 0$. In particular, $o_t' > 0$ and $o_s > 0$. Therefore

$$t = \begin{cases} 1, & \text{if } o_1 = 0; \\ 2, & \text{otherwise.} \end{cases}$$

So, $\ell = n_t + o_t' - 2$. If $t = 1$ then $n_1 + o_1' + o_2 > n_2 + o_2'$, by condition (V), as $a_1 > 0$. If $t = 2$ and $o_1' \geq o_2'$ then, by condition (VI), $o_2' - o_1' \leq 0 < a_2 \leq o_2' - o_1' + \max(0, o_1 + n_2 - n_1)$ and hence $n_1 + o_1' < n_2 + o_2' + o_1$ and $o_2 = 0$.

We claim that for $x, y \in k$

$$\Lambda_{N_\Gamma}^\ell(x(d-1) + y(e-1) + \mathrm{I}(N_\Gamma)\mathrm{I}(\Gamma)) = xu_t^\Gamma(a^{p^{m-1}} - 1) + \mathrm{J}^{p^\ell}(N_\Gamma, \Gamma). \tag{3.3}$$

Indeed, if $t=1$ then $o_1=0$, $o_1'>0$, $n_1+o_1'+o_2>n_2+o_2'$, $\ell=n_1+o_1'-2$, $d=b_1^p$ and $e=b_2^{p^{o_2+1}}$. Thus

$$\begin{aligned}\Lambda^{\ell}_{N_\Gamma}(x(d-1)+y(e-1)+\mathrm{I}(N_\Gamma)\mathrm{I}(\Gamma)) &= x(b_1^{p^{n_1+o_1'-1}}-1)+y(b_2^{p^{n_1+o_1'+o_2-1}}-1)+\mathrm{J}^{p^\ell}(N_\Gamma,\Gamma)\\ &= xu_1^\Gamma(a^{p^{m-1}-1}-1)+\mathrm{J}^{p^\ell}(N_\Gamma,\Gamma).\end{aligned}$$

Suppose that $t=2$. Then $o_2'>0$, $o_1>0$ and $\ell=n_2+o_2'-2$. If $o_2'\leq o_1'$ then $o_2=0$ and $n_2+o_2'+o_1>n_1+o_1'$, and (3.3) follows as in the previous case. If $o_2'>o_1'$ then

$$\begin{aligned}\Lambda^{\ell}_{N_\Gamma}(x(d-1)+y(e-1)+\mathrm{I}(N_\Gamma)\mathrm{I}(\Gamma)) &= x(b_2^{p^{n_2+o_2'-1}}-1)+y(b_1^{p^{n_1+o_2'-1}}-1)+\mathrm{J}^{p^\ell}(N_\Gamma,\Gamma)\\ &= xu_2^\Gamma(a^{p^{m-1}-1}-1)+\mathrm{J}^{p^\ell}(N_\Gamma,\Gamma).\end{aligned}$$

This finishes the proof of (3.3).

By (3.2) and (3.3), $\Lambda^{\ell}_{N_\Gamma}(\mathcal{N}_\Gamma)$ is one dimensional spanned by the class of $a^{p^{m-1}}-1$. Moreover, as $o_t'>0$, $a^{u_t^\Gamma p^{m-1}}=d^{p^\ell}\in N_\Gamma^{p^\ell}$ and hence the natural projection defines an isomorphism

$$\Delta'_\Gamma:\frac{\mathrm{I}(\Gamma')^{p^{m-1}}k\Gamma}{\mathrm{I}(\Gamma')^{p^{m-1}}\mathrm{I}(\Gamma)}\to\Lambda^{\ell}_{N_\Gamma}(\mathcal{N}_\Gamma).$$

Using (3.1) and (2.12) it is easy to see that the natural projections

$$\eta_\Gamma:\mathcal{N}_\Gamma\to\frac{\mathrm{I}(N_\Gamma)k\Gamma+\mathrm{I}(\Gamma)^{p+1}}{\mathrm{I}(\Gamma')k\Gamma+\mathrm{I}(\Gamma)^{p+1}}\quad\text{and}\quad\Lambda^1_\Gamma(\mathcal{C}_\Gamma)\to\frac{\mathrm{I}(N_\Gamma)k\Gamma+\mathrm{I}(\Gamma)^{p+1}}{\mathrm{I}(\Gamma')k\Gamma+\mathrm{I}(\Gamma)^{p+1}}$$

make sense, their images coincide and the second map is injective. Thus the natural projection induces an isomorphism $\Lambda^1_\Gamma(\mathcal{C}_\Gamma)\to\eta_\Gamma(\mathcal{N}_\Gamma)$. On the other hand, by (2.13), $\tilde{\Lambda}^1_\Gamma:\mathcal{C}_\Gamma\to\Lambda^1_\Gamma(\mathcal{C}_\Gamma)$ is an isomorphism. Composing these isomorphisms we obtain an isomorphism

$$\hat{\Lambda}^1_\Gamma:\mathcal{C}_\Gamma\to\mathrm{Im}\ (\eta_\Gamma),\quad w+\mathrm{I}(\Gamma)^2\mapsto w^p+\mathrm{I}(\Gamma')k\Gamma+\mathrm{I}(\Gamma)^{p+1}.$$

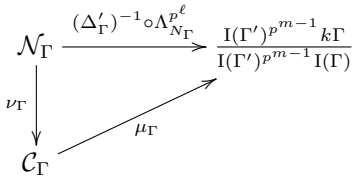
This provides another canonical map

$$\nu_\Gamma=(\hat{\Lambda}^1_\Gamma)^{-1}\circ\eta_\Gamma:\mathcal{N}_\Gamma\to\mathcal{C}_\Gamma,\quad w+\mathrm{I}(N_\Gamma)\mathrm{I}(\Gamma)\mapsto(\hat{\Lambda}^1_\Gamma)^{-1}(w+\mathrm{I}(\Gamma')k\Gamma+\mathrm{I}(\Gamma)^{p+1}).$$

Define the linear map

$$\mu_\Gamma:\mathcal{C}_\Gamma\to\frac{\mathrm{I}(\Gamma')^{p^{m-1}}k\Gamma}{\mathrm{I}(\Gamma')^{p^{m-1}}\mathrm{I}(\Gamma)}$$

sending the class of $x(b_t-1)$ to the class of $xu_t^\Gamma(a^{p^{m-1}}-1)$. A straightforward calculation shows that the following diagram commutes.



As the vertical map is surjective, μ_Γ is the unique map making the previous commutative. Then μ_Γ is canonical, since the other maps in the diagram are so.

Consider the following equation where X stands for an element of k.

$$X\cdot\left(\Lambda^{p^{m-1}}_{\Gamma'}\circ\Delta_\Gamma^{-1}\circ\zeta^1_\Gamma\right)=\mu_\Gamma\circ(\tilde{\Lambda}^{p^{m-o}}_\Gamma)^{-1}\circ\pi_\Gamma^{-1}\circ\zeta^2_\Gamma.\tag{3.4}$$

Here, given a map f with codomain in a vector space over k and $x\in k$, $x\cdot f$ denotes the map given by $(x\cdot f)(w)=xf(w)$, for each w in the domain of f. The unique solution for equation (3.4) is $X=\delta u_t^\Gamma 1_k$. Since all the maps involved are canonical, the solution when $\Gamma=G$ coincides with the solution when $\Gamma=H$. Furthermore, $p\nmid\delta$ and thus $u_t^G\equiv u_t^H \bmod p$, as desired. □

Most of the remaining cases of Theorem B are covered by the next lemma.

Lemma 3.3. *If $n_1+o_1'\neq n_2+o_2'$, then $u_1^G\equiv u_1^H \bmod p$.*

Proof. By Lemma 3.2 we may assume that $o_1o_2 \neq 0$. Hence condition *(III)* and the hypothesis imply $n_1 + o_1' > n_2 + o_2'$. As in the proof of Lemma 3.2 we may assume that $a_1 > 0$ and hence $o_1' > 0$. Consider the subgroup

$$M_\Gamma = \Omega_{n_2-m+o_1}(\Gamma : \Gamma') = \left\langle b_1^{p^{n_1-n_2+m-o_1}}, b_2^{p^{m-o_1}}, a \right\rangle.$$

Recall that $c = b_1^{-\delta p^{m-o_2}} b_2^{\delta p^{m-o_1}} a$ and $\frac{\mathrm{Z}(\mathrm{I}(\Gamma))+\mathrm{I}(\Gamma)^{p^m}}{\mathrm{I}(\Gamma)^{p^m}}$ is spanned by the classes of $c-1, (c-1)^2, \dots, (c-1)^{\frac{p^m-1}{2}}$. The natural projection

$$\zeta_\Gamma^3 : \frac{\mathrm{Z}(\mathrm{I}(\Gamma)) + \mathrm{I}(\Gamma)^{p^m}}{\mathrm{I}(\Gamma)^{p^m}} \to \frac{\mathrm{Z}(\mathrm{I}(\Gamma)) + \mathrm{I}(\Gamma)^{p^{m-o_2+1}} + \mathrm{I}(M_\Gamma)k\Gamma}{\mathrm{I}(\Gamma)^{p^{m-o_2+1}} + \mathrm{I}(M_\Gamma)k\Gamma}$$

maps the class of $x(c-1)+y(c-1)^2+\dots$ to the class of $-x\delta(b_1^{p^{m-o_2}}-1)$, which is non-zero if $x \neq 0$ because $n_1 - n_2 + m - o_1 > m - o_2$. So $\mathrm{Im}\ (\zeta_\Gamma^3)$ is 1-dimensional.

Now consider the composition

$$\hat{\Lambda}_\Gamma^{m-o_2} : \frac{\mathrm{I}(\Gamma)}{\mathrm{I}(\Gamma)^2} \xrightarrow{\Lambda_\Gamma^{m-o_2}} \frac{\mathrm{I}(\Gamma)^{p^{m-o_2}}}{\mathrm{I}(\Gamma)^{p^{m-o_2+1}}} \longrightarrow \frac{\mathrm{I}(\Gamma)^{p^{m-o_2}} + \mathrm{I}(M_\Gamma)k\Gamma}{\mathrm{I}(\Gamma)^{p^{m-o_2+1}} + \mathrm{I}(M_\Gamma)k\Gamma}$$

where the second map is the natural projection. It maps $x(b_1-1)+y(b_2-1)$ to $x(b_1^{p^{m-o_2}}-1)$, so $\mathrm{Im}\ (\hat{\Lambda}_\Gamma^{m-o_1}) = \mathrm{Im}\ (\zeta_\Gamma^3)$.

The image of $\Lambda_\Gamma^{n_1+o_1'-1}$ is the subspace of $\mathrm{I}(\Gamma)^{p^{n_1+o_1'-1}}/\mathrm{I}(\Gamma)^{p^{n_1+o_1'-1}+1}$ spanned by the class of $a^{p^{m-1}} - 1$. It coincides with the image of the natural projection

$$\frac{\mathrm{I}(\Gamma')^{p^{m-1}}k\Gamma}{\mathrm{I}(\Gamma')^{p^{m-1}}\mathrm{I}(\Gamma)} \to \frac{\mathrm{I}(\Gamma)^{p^{n_1+o_1'-1}}}{\mathrm{I}(\Gamma)^{p^{n_1+o_1'-1}+1}}.$$

Thus this natural projection yields an isomorphism $\tilde{\Delta}_\Gamma : \frac{\mathrm{I}(\Gamma')^{p^{m-1}}k\Gamma}{\mathrm{I}(\Gamma')^{p^{m-1}}\mathrm{I}(\Gamma)} \to \mathrm{Im}\ (\Lambda_\Gamma^{n_1+o_1'-1})$.

Let $\mu_\Gamma : \mathrm{Im}\ (\zeta_\Gamma^3) \to \frac{\mathrm{I}(\Gamma')^{p^{m-1}}k\Gamma}{\mathrm{I}(\Gamma')^{p^{m-1}}\mathrm{I}(\Gamma)}$ be the map that sends the class of $x(b_1^{p^{m-o_1}}-1)$ to the class of $xu_1(a^{p^{m-1}}-1)$. Then it is easy to see that the following diagram commutes

$$\begin{array}{ccc} \frac{\mathrm{I}(\Gamma)}{\mathrm{I}(\Gamma)^2} & \xrightarrow{\tilde{\Delta}_\Gamma^{-1}\circ\Lambda_\Gamma^{n_1+o_1'-1}} & \frac{\mathrm{I}(\Gamma')^{p^{m-1}}k\Gamma}{\mathrm{I}(\Gamma')^{p^{m-1}}\mathrm{I}(\Gamma)} \\ {\scriptstyle \hat{\Lambda}_\Gamma^{m-o_2}}\downarrow & \nearrow_{\mu_\Gamma} & \\ \mathrm{Im}\ (\zeta_\Gamma^3) & & \end{array}$$

As the vertical map is surjective, μ_Γ is the unique map making the previous commutative, so μ_Γ is canonical. Then $-\delta u_1^\Gamma 1_k$ is the unique solution of the equation

$$X \cdot (\Lambda_{\Gamma'}^{p^{m-1}} \circ \Delta_\Gamma^{-1} \circ \zeta_\Gamma^1) = \mu_\Gamma \circ \zeta_\Gamma^3.$$

Arguing as at the end of the proof of Lemma 3.2 we conclude that $u_1^G \equiv u_1^H \mod p$. □

The proof of Lemma 3.3 fails if $n_1 + o_1' = n_2 + o_2'$, because in that case $\ker(\hat{\Lambda}_\Gamma^{m-o_2}) \not\subseteq \ker(\Delta_\Gamma^{-1} \circ \Lambda_\Gamma^{n_1+o_1'-1})$, and hence there is no map μ_Γ such that $\mu_\Gamma \circ \hat{\Lambda}_\Gamma^{m-o_2} = \Delta_\Gamma^{-1} \circ \Lambda_\Gamma^{n_1+o_1'-1}$. However, some special subcases can be handled with slight modifications of the previous arguments.

For a non-negative integer n define the map

$$\begin{array}{rcl} \Upsilon_\Gamma^n : \frac{\mathrm{Z}(\mathrm{I}(\Gamma)) + \mathrm{I}(\Gamma)^{p^m}}{\mathrm{I}(\Gamma)^{p^m}} & \longrightarrow & \frac{\mathrm{Z}(\mathrm{I}(\Gamma)) + \mathrm{I}(\Gamma)^{p^{n+m}} + \mathrm{I}(\Gamma')^{p^{m-1}}\mathrm{I}(\Gamma)}{\mathrm{I}(\Gamma)^{p^{n+m}} + \mathrm{I}(\Gamma')^{p^{m-1}}\mathrm{I}(\Gamma)} \\ w + \mathrm{I}(\Gamma)^{p^m} & \mapsto & w^{p^n} + \mathrm{I}(\Gamma)^{p^{n+m}} + \mathrm{I}(\Gamma')^{p^{m-1}}\mathrm{I}(\Gamma). \end{array}$$

It is well defined because the elements of $\mathrm{Z}(\mathrm{I}(\Gamma))$ are central.

Lemma 3.4. *If $o_1o_2 > 0$, $n_1 + o_1' = n_2 + o_2' = 2m - o_1$ and $u_2^G \equiv u_2^H \equiv 1 \mod p^{o_1+1-o_2}$, then $u_1^G \equiv u_1^H \mod p$.*

Proof. As in previous proofs we may assume that $a_1 \neq 0$ and hence $0 < o_1'$. As $o_1 o_2 > 0$ implies $n_1 > n_2$, necessarily $1 \leq o_1' < o_2'$. Recall that $\mathrm{Z}(\Gamma) = \left\langle b_1^{p^m}, b_2^{p^m}, c \right\rangle$, where $c = b_1^{-\delta p^{m-o_2}} b_2^{\delta p^{m-o_1}} a$.

We claim that

$$(\delta u_2^\Gamma + 1) p^{m+o_2-o_1-1} \equiv 0 \bmod p^m. \tag{3.5}$$

To prove this, it suffices to show that $\delta \equiv -1 \mod p^{o_1+1-o_2}$. As $v_p(r_2-1) = m - o_2$, $m - o_1 \geq 1 = m + 1 - o_2 - v_p(r_2)$. Hence [4, Lemma A.2] yields $\mathcal{S}(r_2 \mid \delta p^{m-o_1}) \equiv \delta p^{m-o_1} \mod p^{m+1-o_2}$. Thus (2.3) implies that $\delta \equiv -1 \mod p^{o_1+1-o_2}$. This proves (3.5).

Next we claim that

$$c^{p^{n_1+o_1'-1-m+o_2}} = a^{-\delta u_1^\Gamma p^{m-1}}. \tag{3.6}$$

Indeed, first observe that condition implies

$$n_1 + o_1' - 1 = 2m - o_1 - 1 \geq 2m - o_2 + n_2 - n_1 = 2m - o_2 - o_2' + o_1' \geq 2m - o_2 - o_2' \geq m - o_2. \tag{3.7}$$

Thus the exponent in the left side of (3.6) is a positive integer. Observe that

$$\left\langle b_1^{p^{m-o_2}}, b_2^{p^{m-o_1}}, a \right\rangle$$

is a regular group with derived subgroup $\left\langle a^{p^{2m-o_1-o_2}} \right\rangle$. As $m - o_2' + 2m - o_1 - o_2 = 3m - o_1 - o_2 - o_2' \geq 2m - o_1 > m$ (since $o_2 + o_2' \leq m$), we derive that

$$c^{p^{m-o_2'}} = b_1^{-\delta p^{2m-o_2-o_2'}} b_2^{\delta p^{2m-o_1-o_2'}} a^{p^{m-o_2'}} = b_1^{-\delta p^{2m-o_2-o_2'}} b_2^{\delta p^{n_2}} a^{p^{m-o_2'}} = b_1^{-\delta p^{2m-o_2-o_2'}} a^{(\delta u_2^\Gamma+1)p^{m-o_2'}}.$$

As $b_1^{p^{2m-o_2-o_2'}} \in \mathrm{Z}(\Gamma)$ and recalling (3.7) we get

$$\begin{aligned} c^{p^{n_1+o_1'-1-m+o_2}} &= (c^{p^{m-o_2'}})^{p^{n_1+o_1'-1-(2m-o_2-o_2')}} = b_1^{-\delta p^{n_1+o_1'-1}} a^{(\delta u_2^\Gamma+1)p^{n_1+o_1'-1-m+o_2}} \\ &= a^{-\delta u_1^\Gamma p^{m-1}} a^{(\delta u_2^\Gamma+1)p^{m+o_2-o_1-1}} = a^{-\delta u_1^\Gamma p^{m-1}}, \end{aligned}$$

where the last equality follows from (3.5). This proves (3.6).

Using (3.6) we obtain that $\Upsilon_\Gamma^{n_1+o_1'+o_2-m-1}$ maps the class of $\sum_{i=1}^{\frac{p-1}{2}} x_i(c-1)^i$, with $x_i \in k$, to the class of $-x_1 \delta u_1^\Gamma (a^{p^{m-1}} - 1)$. If $x_1 \neq 0$, then the latter is not the class zero, by Lemma 1.4. Then the natural projection defines an isomorphism $\pi_\Gamma : \frac{\mathrm{I}(\Gamma')^{p^{m-1}} k\Gamma}{\mathrm{I}(\Gamma')^{p^{m-1}} \mathrm{I}(\Gamma)} \to \mathrm{Im}\,(\Upsilon_\Gamma^{n_1+o_1'+o_2-m-1})$. So we have a canonical map

$$\pi_\Gamma^{-1} \circ \Upsilon_\Gamma^{n_1+o_1'+o_2-m-1} : \frac{\mathrm{Z}(\mathrm{I}(\Gamma)) + \mathrm{I}(\Gamma)^{p^m}}{\mathrm{I}(\Gamma)^{p^m}} \to \frac{\mathrm{I}(\Gamma')^{p^{m-1}} k\Gamma}{\mathrm{I}(\Gamma')^{p^{m-1}} \mathrm{I}(\Gamma)},$$

mapping the class of $\sum_{i=1}^{\frac{p-1}{2}} x_i(c-1)^i$ to the class of $x_1(-\delta u_1^\Gamma)(a^{p^{m-1}} - 1)$. But we also have the canonical map

$$\Lambda_{\Gamma'}^{m-1} \circ \Delta_\Gamma^{-1} \circ \zeta_\Gamma^1 : \frac{\mathrm{Z}(\mathrm{I}(\Gamma)) + \mathrm{I}(\Gamma)^{p^m}}{\mathrm{I}(\Gamma)^{p^m}} \to \frac{\mathrm{I}(\Gamma')^{p^{m-1}} k\Gamma}{\mathrm{I}(\Gamma')^{p^{m-1}} \mathrm{I}(\Gamma)}$$

that maps the class of $\sum_{i=1}^{\frac{p-1}{2}} x_i(c-1)^i$ to the class of $x_1(a^{p^{m-1}} - 1)$. Thus the unique element $x \in k$ such that $\pi_\Gamma^{-1} \circ \Upsilon_\Gamma^{n_1+o_1'+o_2-m-1} = x \cdot (\Lambda_{\Gamma'}^{m-1} \circ \Delta_\Gamma^{-1} \circ \zeta_\Gamma^1)$ is $-\delta u_1^\Gamma 1_k$. Since all the maps are canonical, this has to be the same for $\Gamma = G$ and $\Gamma = H$. Hence $u_1^G \equiv u_1^H \mod p$. □

Theorem B follows at once from Lemmas 3.2, 3.3 and 3.4.

3.2. **Proof of Theorem A.** Since $\psi(\mathrm{I}(G')kG) = \mathrm{I}(H')kH$, we have that $\psi(\mathrm{I}((G')^{p^n})kG) = \mathrm{I}((H')^{p^n})kH$ for each $n \geq 1$. Hence ψ induces isomorphims $\psi_n : k(G/(G')^{p^n}) \to k(H/(H')^{p^n})$.

We first proof Theorem A(1). By (2.2), $\gamma_3(G) = (G')^{p^{m-\max(o_1,o_2)}}$. Hence, $\psi_{m-\max(o_1,o_2)+1}$ is an isomorphism $k(G/\gamma_3(G)^p) \cong k(H/\gamma_3(H)^p)$. Hence we can assume that $|\gamma_3(G)| = |\gamma_3(H)| = p$, so necessarily $\max(o_1, o_2) = 1$. This means that $\{o_1, o_2\} = \{0, 1\}$, by condition *(III)*. Thus $a_1 \leq o_2$ and $a_2 \leq o_1$. Then $1 \leq u_i^\Gamma < p$ for $i \in \{1, 2\}$ and $\Gamma \in \{G, H\}$ by conditions *(V)* and *(VI)*. Therefore $u_1^G = u_1^H$ and $u_2^G = u_2^H$ by Theorem B, and the result follows. This proves Theorem A(1).

To prove Theorem A(2) we need one more result, which allows us to recover u_i^Γ modulo a higher power of p in very special situations (see Lemma 3.5). For that, we define

$$q^\Gamma = \min\{n \geq 0 : \Omega_1(\Gamma') \cap \mathrm{D}_{p^n}(\Gamma) = 1\}.$$

We claim that

$$q^\Gamma = \begin{cases} m, & \text{if } o_1' = o_2' = 0; \\ n_2 + o_2', & \text{if } 0 = o_1' < o_2'; \\ \max(n_1 + o_1', n_2 + o_2'), & \text{if } o_1' > 0. \end{cases} \tag{3.8}$$

Indeed, first recall that $n_1 \geq m$ by condition *(IV)*. Moreover, $n_2 + o_2' \geq m$, since otherwise, by the same condition, $n_2 = 2m - o_1 - o_2'$, so $m < 2m - o_1 = n_2 + o_2' \leq m$, a contradiction. Clearly, $m \leq q^\Gamma$, since $1 \neq a^{p^{m-1}} \in \Omega_1(\Gamma') \cap \mathrm{D}_{p^{m-1}}(\Gamma)$. Moreover, using regularity and (2.6) we derive that if $n \geq m$, then $\mathrm{D}_{p^n}(\Gamma) = \left\langle b_1^{p^n}, b_2^{p^n} \right\rangle$. If $o_1' = o_2' = 0$, then $\mathrm{D}_{p^m}(\Gamma) \cap \Omega_1(\Gamma') = 1$, so $q^\Gamma = m$. Suppose that $0 = o_1' < o_2'$. Then $a^{p^{m-1}} \in \mathrm{D}_{p^{n_2+o_2'-1}}(\Gamma)$, but $\mathrm{D}_{p^{n_2+o_2'}}(\Gamma) = \left\langle b_1^{p^{n_2+o_2'}} \right\rangle$, which does not intersect with Γ'. Thus $q^\Gamma = n_2 + o_2'$. Finally suppose that $o_1' > 0$. Then $a^{p^{m-1}} \in \mathrm{D}_{p^{\max(n_1+o_1', n_2+o_2')-1}}(\Gamma)$ because if $n_2 + o_2' > n_1 + o_1'$ then $o_2' > 0$ since $n_1 \geq n_2$. As $\mathrm{D}_{p^{\max(n_1+o_1', n_2+o_2')}}(\Gamma) = 1$, we conclude that $q^\Gamma = \max(n_1 + o_1', n_2 + o_2')$. This finishes the proof of (3.8).

Lemma 3.5. *Let t be a positive integer such that $t \leq 2m - 1 - q^G$.*

(1) Suppose that $o_1 = 0$ and $n_1 = 2m - o_2 - o_1'$. If $u_1^G \equiv u_1^H \equiv -1 \mod p^t$, then $u_1^G \equiv u_1^H \mod p^{t+1}$.
(2) Suppose that $o_2 = 0$ and $n_2 = 2m - o_1 - o_2'$. If $u_2^G \equiv u_2^H \equiv 1 \mod p^t$, then $u_2^G \equiv u_2^H \mod p^{t+1}$.

Proof. Suppose first that the hypotheses of (1) hold. If $a_1 \leq t$ then $u_1^G = u_2^H = -1 + p^{a_1}$. Thus we may assume that $t < a_1$ and in particular $t < o_1'$. Then $q^\Gamma = \max(n_1 + o_1', n_2 + o_2')$. Write $u_1^\Gamma = -1 + v_1^\Gamma p^t$. Recall that $\mathrm{Z}(\Gamma) = \left\langle b_1^{p^m}, b_2^{p^m}, c = b_1^{p^{m-o_2}} a \right\rangle$, by (2.4). As $o_1 = 0$, $[b_1, a] = 1$ and hence

$$(b_1^{p^{m-o_2}} a)^{p^{m-o_1'}} = b_1^{p^{n_1}} a^{p^{m-o_1'}} = a^{(u_1^\Gamma+1)p^{m-o_1'}} = a^{v_1^\Gamma p^{m-o_1'+t}}.$$

Therefore

$$(b_1^{p^{m-o_2}} a)^{p^{m-t-1}} = ((b_1^{p^{m-o_2}} a)^{p^{m-o_1'}})^{p^{o_1'-t-1}} = a^{v_1^\Gamma p^{m-1}}.$$

Then Υ_Γ^{m-t-1} maps the class of $x(c-1) + y(c-1)^2 + \dots$ to the class of $x v_1^\Gamma (a^{p^{m-1}} - 1)$. Observe that $a^{p^{m-1}} \notin \mathrm{D}_{2m-t-1}(\Gamma)$ since $2m - t - 1 \geq q^\Gamma$. Hence $(a^{p^{m-1}} - 1) \notin \mathrm{I}(\Gamma)^{p^{2m-t-1}} + \mathrm{I}(\Gamma')^{p^{m-1}} \mathrm{I}(\Gamma)$, by Lemma 1.4. Thus $\mathrm{Im}\,(\Upsilon_\Gamma^{m-t-1})$ has dimension 1, and the natural projection

$$\omega_\Gamma : \frac{\mathrm{I}(\Gamma')^{p^{m-1}} k\Gamma}{\mathrm{I}(\Gamma')^{p^{m-1}} \mathrm{I}(\Gamma)} \to \mathrm{Im}\,(\Upsilon_\Gamma^{m-t-1})$$

is an isomorphism. If $x \in k$, then

$$(\omega_\Gamma)^{-1} \circ \Upsilon_\Gamma^{m-t-1} = x \cdot (\Lambda_{\Gamma'}^{m-1} \circ \Delta_\Gamma^{-1} \circ \zeta_\Gamma^1)$$

if and only if $x = v_1^\Gamma \cdot 1_k$. As this holds both for $\Gamma = G$ and for $\Gamma = H$ and all the maps are canonical, we conclude that $v_1^G \equiv v_1^H \mod p$, so $u_1^G \equiv u_1^H \mod p^{t+1}$. This finishes the proof of (1).

Under the assumptions of (2), the congruence in (2.3) yields $\delta \equiv -1 \mod p^{o_1}$, and hence $\mathrm{Z}(\Gamma) = \left\langle b_1^{p^m}, b_2^{p^m}, c = b_2^{-p^{m-o_1}} a \right\rangle$. Then setting $u_2^\Gamma = 1 + v_2^\Gamma p^t$ and arguing as above we obtain $(b_2^{-p^{m-o_1}} a)^{p^{m-t^\Gamma-1}} = a^{-v_2^\Gamma p^{m-1}}$. The rest of the proof is completely analogous to the previous case. □

Lemma 3.6. *If $n_2 \leq 2$, then $G \cong H$.*

Proof. Recall that we are assuming that (2.8) holds, so $m \geq 2$ and we may assume that $n_2 = 2$. If $m = 2$ then $|\gamma_3(\Gamma)| = p$, and hence the result follows from Theorem A(1). Thus we assume $m \geq 3$. Then $n_2 < m$, and by condition *(IV)*, $2 = n_2 = 2m - o_1 - o_2'$ and $u_2^\Gamma \equiv 1 \mod p^{m-2}$. Then $2(m-1) = o_1 + o_2'$. Since $o_1 < m$ by condition *(II)*, and $o_2' < m$ by (2.8), we derive that $o_1 = o_2' = m - 1$. As $o_i + o_i' \leq m$ by condition *(II)*, also $o_1' \leq 1$ and $o_2 \leq 1$. Therefore $1 \leq u_1^\Gamma \leq p$. Then Theorem B implies that $u_1^G = u_1^H$ or condition

(2) in the theorem holds. In the latter case $o_1o_2 > 0$ and $n_1 + o_1' = n_2 + o_2' = m + 1$. The former implies $n_1 > m$ by (2.7). Therefore $o_1' = 0$, so $u_1^G = 1 = u_1^H$.

Observe that $1 \leq u_2^\Gamma \leq p^{a_2}$, for otherwise, $o_2 = 1$ and $n_1+o_1'-m-1 = n_1-n_2+o_1'-o_2' = 0 < a_1 \leq o_1' \leq 1$ by condition (VI), so $n_1 = m$ and $o_1o_2 > 0$, in contradiction with (2.7). If $o_2 = 1$, then $a_2 \leq o_1 - o_2 = m-2$, so $1 \leq u_2^\Gamma \leq p^{m-2}$ and hence $u_2^G = u_2^H$. Thus we assume $o_2 = 0$. Suppose that $o_1' = 0$. Then by (3.8) $q^\Gamma = n_2 + o_2' = m + 1$. Thus $m - 2 \leq 2m - 1 - q^\Gamma = m - 2$. Therefore Lemma 3.5(2) with $t = m - 2$ yields that $u_2^G \equiv u_2^H \mod p^{m-1}$, i.e., $u_2^G = u_2^H$. Now suppose that $o_1' = 1$. Since $n_1 \geq m$ by condition (IV), $q^\Gamma = n_1 + 1$. If $n_1 > m$, then by condition (VI) $a_2 = o_2' - o_1 + \max(0, m + 1 - n_1) = m - 2$ and $1 \leq u_2^\Gamma \leq p^{m-2}$, so $u_2^G = u_2^H$. Hence we assume $n_1 = m$. Then $q^\Gamma = m+1$ and $m-2 \leq 2m-1-q^\Gamma = m-2$. Thus, again Lemma 3.5(2) with $t = m - 2$ yields $u_2^G \equiv u_2^H \mod p^{m-1}$, i.e., $u_2^G = u_2^H$. □

Observe that Lemma 3.6 is equivalent to the following proposition which may be of interest by itself. We do not know whether the hypothesis $p > 2$ is needed.

Proposition 3.7. *Let G be a 2-generated finite p-group with cyclic derived subgroup. Suppose that $p > 2$ and $(G/G')^{p^2}$ is cyclic. If $kG \cong kH$ for some group H then $G \cong H$.*

We are finally ready to prove Theorem A(2). Via the isomorphism ψ_3 introduced at the beginning of Section 3.2, we can assume that $(G')^{p^3} = 1 = (H')^{p^3}$, i.e., $m \leq 3$. If $n_2 \leq 2$, then the result follows from Lemma 3.6, so we assume $3 \leq n_2$. If $|\gamma_3(G)| \leq p$, then the result follows from Theorem A(1). Thus we assume $|\gamma_3(G)| = |\gamma_3(H)| = p^2$, so $m = 3$. Then $\gamma_3(G) = (G')^{p^{m-\max(o_1,o_2)}}$, by (2.2), which implies that $\max(o_1, o_2) = 2$. By condition (III), we have three possibilities: $0 = o_1 < o_2 = 2$, $0 = o_2 < o_1 = 2$ and $1 = o_2 < o_1 = 2$.

Suppose that $0 = o_1 < o_2 = 2$. Then $u_2^G = 1 = u_2^H$, by condition (VI). Since $m = 3$ and $o_2 + o_1' \leq m$ by condition (IV), we have that $o_2' \leq 1$, so $1 \leq u_1^\Gamma \leq p$ for $\Gamma \in \{G, H\}$. Thus $u_1^G = u_1^H$, by Theorem B.

Suppose that $0 = o_2 < o_1 = 2$. Then $u_1^G = 1 = u_1^H$ by condition (V). Recall that $m = 3 \leq n_2$. Then $o_2' + 2 = o_2' + o_1 \leq m = 3$ by condition (IV), so $o_2' \leq 1$. Hence $1 \leq u_2^\Gamma \leq p$ for $\Gamma \in \{G; H\}$, by condition (VI). Thus $u_2^G = u_2^H$ by Theorem B.

Finally suppose that $1 = o_2 < o_1 = 2$. By condition (II), $o_1' \leq 1$, and since $n_2 \geq m$, by condition (IV), $o_2' \leq 1$. Then $1 \leq u_1^\Gamma \leq p$. Observe that neither condition (2) in Theorem B nor condition (VI)(b) holds since, by condition (III), in any of these cases $1 = o_1 - o_2 < n_1 - n_2 = o_2' - o_1' \leq 1$, a contradiction. Therefore $1 \leq u_2^\Gamma \leq p$ and, by Theorem B, we derive that $u_1^G = u_1^H$ and $u_2^G = u_2^H$.

4. Applications to groups of small order

Recall that p is an odd prime and k is the field with p elements. We first solve the Modular Isomorphism Problem for our target groups when their order is at most p^{11}.

Proposition 4.1. *Let G be a 2-generated p-group with cyclic derived subgroup such that $|G| \leq p^{11}$. If $kG \cong kH$ for some group H, then $G \cong H$.*

Proof. We may assume that G is neither metacyclic nor of class at most 2. Thus conditions (2.8) are satisfied and hence we can use all the results in previous sections. Let G and H be a 2-generated p-groups ($p > 2$) with cyclic derived subgroup of order at most p^{11}, with $kG \cong kH$ and the usual notation $\mathrm{inv}(\Gamma) = (p, m, n_1, n_2, o_1, o_2, o_1', o_2', u_1^\Gamma, u_2^\Gamma)$ for $\Gamma \in \{G, H\}$. If $m \leq 3$, the result follows from Theorem A(1). Thus we assume $m > 3$. Then $n_1 \geq m > 3$ by condition (IV). We can assume that $n_2 \geq 3$ by Lemma 3.6. Thus $|\Gamma| = p^{n_1+n_2+m} = p^{11}$. Therefore $n_2 = 3$ and $m = n_1 = 4$. As $n_2 < m$, by condition (IV) $u_2^\Gamma \equiv 1 \mod p$ and $8 - o_1 - o_2' = 2m - o_1 - o_2' = n_2 = 3$, so $o_1 + o_2' = 5$. Since $o_1 < m$ and $o_2' < m$ because Γ is not metacyclic, we derive that $\{o_1, o_2'\} = \{3, 2\}$. Then, by (2.7), $o_2 = 0$. Thus $u_1^G = 1 = u_1^H$. It also follows that $a_2 \leq 2$, so $1 \leq u_2^\Gamma \leq p^2$. Since $2 \leq o_1$, by condition (IV), $o_1' \leq 2$. Thus $q^\Gamma \leq \max(n_1 + o_1', n_2 + o_2') \leq 6$. Write $t = 1$, so $t = 1 = 2m - 1 - q^\Gamma$. Therefore, by Lemma 3.5(2), $u_2^G \equiv u_2^H \mod p^2$. Thus $u_2^G = u_2^H$. □

For groups of order p^{12}, we can solve the Modular Isomorphism Problem except for $p-2$ families of groups of size p each one:

Proposition 4.2. *Let G be a 2-generated finite p group with cyclic derived subgroup and $|G| \leq p^{12}$. If $kG \cong kH$ for some group H, then one of the following holds:*

(1) $G \cong H$.

(2) There exist $i \in \{1, \dots, p-2\}$ *and* $u_1^G, u_1^H \in \{i + jp : 0 \leq j \leq p-1\}$ *such that*

$$\mathrm{inv}(G) = (p, 4, 4, 4, 0, 2, 2, 2, u_1^G, 1) \text{ and}$$
$$\mathrm{inv}(H) = (p, 4, 4, 4, 0, 2, 2, 2, u_1^H, 1).$$

Proof. By Theorem A and Proposition 4.1, we may assume that $|G'| > p^3$ and $|G| = p^{12}$. Moreover we can assume that neither G nor H is metacyclic nor of class at most 2. With the notation of Theorem B, $\mathrm{inv}(G)$ equals $\mathrm{inv}(H)$ except the last two entries, (u_1^Γ, u_2^Γ), where $\Gamma \in \{G, H\}$. Moreover, we can assume $n_2 \geq 3$ by Lemma 3.6. Then either $n_2 = 3$, $m = 4$ and $n_1 = 5$, or $n_2 = m = n_1 = 4$.

Suppose that $m = 4$, $n_1 = 5$ and $n_2 = 3$. By condition *(IV)*, $u_2^\Gamma \equiv 1 \mod p$ and $3 = n_2 = 2m - o_1 - o_2'$, so $5 = o_1 + o_2'$, and hence $\{o_1, o_2'\} = \{2, 3\}$ because $o_1 < m$ and $o_2' < m$.

Suppose that $o_2' = 3$. Then $o_1 = 2$, $o_2 \leq m - o_2' = 1$ and $o_1' \leq m - o_1 = 2$. Assume that $o_2 = 1$. Then $a_2 \leq o_1 - o_2 = 1$. If condition *(VI)*(b) does not hold, then Theorem B yields $u_2^G = u_2^H$. Thus suppose this condition holds. Then $u_1^\Gamma \equiv 1 \bmod p$ and $5 + o_1' = n_1 + o_1' = n_2 + o_2' = 6$, so $o_1' = 1$. Hence $1 \leq u_1^\Gamma \leq p$, and we get $u_1^G = u_1^H = 1$. Moreover $a_2 = \min(o_1 - o_2, o_2' - o_1') = 1$. Thus $u_2^\Gamma \in \{1, 1 + p\}$. Summarizing, after exchanging G and H, if necessary,

$$\mathrm{inv}(G) = (p, 4, 5, 3, 2, 1, 1, 3, 1, 1);$$
$$\mathrm{inv}(H) = (p, 4, 5, 3, 2, 1, 1, 3, 1, 1 + p).$$

But then a straightforward computation, using (2.4), shows that $\mathrm{Z}(G)$ has exponent p^2 while the exponent of $\mathrm{Z}(H)$ is p^3, in contradiction with a result of Ward [15] (see [10, Lemma 2.7]). Now assume $o_2 = 0$. Then $a_1 = 0$, so $u_1^G = 1 = u_1^H$. Observe that $a_2 = \min(o_1, 3 - o_1') \leq 2$. Moreover $3 - o_1' = o_2' - o_1' \leq n_1 - n_2 = 2$, so $1 \leq o_1'$. If $o_1' = 1$ then $q^\Gamma = 6$, and setting $t = 1 = 2m - 1 - q^\Gamma$, Lemma 3.5(2) yields $u_2^G = u_2^H$. Otherwise, i.e. if $o_1' \geq 2$, then $a_2 \leq 1$, and $u_2^G = u_2^H$ by Theorem B.

Now suppose that $o_2' = 2$. Then $o_1 = 3$, $o_2 \leq m - o_2' = 2$ and $o_1' \leq m - o_1 = 1$. We claim that $u_1^G = u_1^H$. Indeed, if $o_1' = 0$ then $u_1^G = 1 = u_1^H$, and if $o_1' = 1$ then condition (2) of Theorem B does not hold, and hence that theorem yields the claim. Moreover $a_2 \leq o_2' = 2$ and if condition *(VI)*(b) holds, then $o_2 > 0$ and $o_1' \geq a_1 > 0$ so that $a_2 \leq 1$. Thus $1 \leq u_2^\Gamma \leq 2p < p^2$. Observe that $q^\Gamma = \max(5 + o_1', 5) \leq 6$. Then set $t = 1 \leq 2m - 1 - q^\Gamma$, and Lemma 3.5(2) yields that $u_2^G = u_2^H$.

Finally, suppose that $m = n_1 = n_2 = 4$. By condition *(III)* we have that $o_1 = 0$. Then $u_2^G = 1 = u_2^H$. Moreover $a_1 = \min(o_1', o_2 + o_1' - o_2')$. If $a_1 \leq 1$, then $u_1^G = u_1^H$ by Theorem B. Thus we assume $a_1 \geq 2$, i.e., $2 \leq o_1' \leq 3$ and $2 \leq o_1' + o_2 - o_2'$. If $o_2 \leq 1$ then $|\gamma_3(\Gamma)| \leq p$, and $G \cong H$ by Theorem A(1). Thus we suppose $o_2 \geq 2$. Since $o_1' + o_2 \leq m = 4$, we derive that $o_1' = o_2 = 2$. Hence $a_1 = o_1' = 2$, and $o_2' \geq o_1' = 2$, by condition *(III)*. Since $o_2 + o_2' \leq m = 4$, necessarily $o_2' = 2$. Hence we have that

$$\mathrm{inv}(\Gamma) = (p, 4, 4, 4, 0, 2, 2, 2, u_1^\Gamma, 1)$$

with $1 \leq u_1^\Gamma \leq p^2$. Moreover, by Theorem A(2), we have that $u_1^G \equiv u_1^H \mod p$. Hence there is an integer $1 \leq i \leq p-1$ such that $u_1^\Gamma = i + j^\Gamma p$, for some integers $0 \leq j^G, j^H \leq p-1$. Finally, assume $i = p-1$, so $u_1^\Gamma \equiv -1 \mod p$. Since $q^\Gamma = 6$, setting $t = 1 = 2m - 1 - q^\Gamma$, Lemma 3.5(1) yields that $u_1^G = u_1^H$. □

Remark 4.3. *Observe that Theorem B shows that* $kG \cong kH$ *implies* $u_1^G \equiv u_1^H \mod p$ *in almost all situations. A pair of groups* G *and* H *of minimal size with* $u_1^G \not\equiv u_1^H \mod p$ *and not covered by this theorem (i.e., such that it is still open whether they have isomorphic group algebras or not) consists in groups of order* 3^{17} *and*

$$\mathrm{inv}(G) = (3, 5, 7, 5, 1, 1, 2, 1, 1, 3, 1, 2);$$
$$\mathrm{inv}(H) = (3, 5, 7, 5, 1, 1, 2, 1, 1, 3, 2, 2).$$

Acknowledgements: We are grateful to Mima Stanojkovski, with whom we started the study of the Modular Isomorphism Problem for this class of groups, for useful comments and discussions on early drafts of this paper. Lemma 1.3, if not folklore, was written by Sofia Brenner and the first author for another project: we are grateful to her for allowing us to include it here.

References

[1] C. Bagiński. The isomorphism question for modular group algebras of metacyclic p-groups. *Proc. Amer. Math. Soc.*, 104(1):39–42, 1988.

[2] C. Bagiński and A. Caranti. The modular group algebras of p-groups of maximal class. *Canad. J. Math.*, 40(6):1422–1435, 1988.
[3] O. Broche and Á. del Río. The Modular Isomorphism Problem for two generated groups of class two. *Indian J. Pure Appl. Math.*, 52:721–728, 2021.
[4] O. Broche, D. García-Lucas, and Á. del Río. A classification of the finite 2-generator cyclic-by-abelian groups of prime-power order. *International Journal of Algebra and Computation*, 33(04):641–686, 2023.
[5] W. E. Deskins. Finite Abelian groups with isomorphic group algebras. *Duke Math. J.*, 23:35–40, 1956.
[6] D. García-Lucas. The modular isomorphism problem and abelian direct factors. `arXiv:2209.15128`, 2022.
[7] D. García-Lucas, L. Margolis, and Á. del Río. Non-isomorphic 2-groups with isomorphic modular group algebras. *J. Reine Angew. Math.*, 154(783):269–274, 2022.
[8] D. García-Lucas, Á. del Río, and M. Stanojkowski. On group invariants determined by modular group algebras: even versus odd characteristic. *Algebr. Represent. Theory.* `https://doi.org/10.1007/s10468-022-10182-x`, 2022.
[9] D. S. Passman. The group algebras of groups of order p^4 over a modular field. *Michigan Math. J.*, 12:405–415, 1965.
[10] D. S. Passman. *The algebraic structure of group rings*. Pure and Applied Mathematics. Wiley-Interscience [John Wiley & Sons], New York-London-Sydney, 1977.
[11] R. Sandling. The isomorphism problem for group rings: a survey. In *Orders and their applications (Oberwolfach, 1984)*, volume 1142 of *Lecture Notes in Math.*, pages 256–288. Springer, Berlin, 1985.
[12] R. Sandling. The modular group algebra of a central-elementary-by-abelian p-group. *Arch. Math. (Basel)*, 52(1):22–27, 1989.
[13] R. Sandling. The modular group algebra problem for metacyclic p-groups. *Proc. Amer. Math. Soc.*, 124(5):1347–1350, 1996.
[14] H. Usefi. Identifications in modular group algebras. *J. Pure Appl. Algebra*, 212(10):2182–2189, 2008.
[15] H. N. Ward. Some results on the group algebra of a p-group over a prime field. In *Seminar on finite groups and related topics.*, pages 13–19. Mimeographed notes, Harvard Univ., 1960-61.

Departamento de Matemáticas, Universidad de Murcia, Spain
Email address: `diego.garcial@um.es`

Departamento de Matemáticas, Universidad de Murcia, Spain
Email address: `adelrio@um.es`

Part V

in which we study the modular isomorphism problem
for groups of nilpotency class 2 with cyclic center.

This empty page stands for the following article:

Title: *On the modular isomorphism problem for groups of nilpotency class 2 with cyclic center.*
Authors: Diego García-Lucas and Leo Margolis.
Reference: Forum Mathematicum, 2024.
DOI: doi.org/10.1515/forum-2023-0237
Abstract: We show that the modular isomorphism problem has a positive answer for groups of nilpotency class 2 with cyclic center, i.e. that for such p-groups G and H an isomorphism between the group algebras FG and FH implies an isomorphism of the groups G and H for F the field of p elements. For groups of odd order this implication is also proven for F being any field of characteristic p. For groups of even order we need either to make an additional assumption on the groups or on the field.

Part VI

in which we reduce the modular isomorphism problem
to groups without abelian direct factors.

This empty page stands for the following article:

Title: *The modular isomorphism problem and abelian direct factors.*
Author: Diego García-Lucas.
Reference: Mediterr. J. Math. 21, 18 (2024).
DOI: doi.org/10.1007/s00009-023-02557-1
Abstract: Let p be a prime and let G be a finite p-group. We show that the isomorphism type of the maximal abelian direct factor of G, as well as the isomorphism type of the group algebra over $\mathbb{F}_p$ of the non-abelian remaining direct factor, if existing, are determined by $\mathbb{F}_pG$, generalizing the main result in Margolis et al. (Abelian invariants and a reduction theorem for the modular isomorphism problem, Journal of Algebra 636, 533-559 (2023)) over the prime field. In order to do this, we address the problem of finding characteristic subgroups of G such that their relative augmentation ideals depend only on the k-algebra structure of kG, where k is any field of characteristic p, and relate it to the modular isomorphism problem, extending and reproving some known results.

Part VII

in which we reduce the isomorphism problem
to finite extensions of the prime field.

This empty page stands for the following article:

Title: *A reduction theorem for the isomorphism problem of group algebras over fields.*
Authors: Diego García-Lucas and Ángel del Río.
Reference: Journal of Pure and Applied Algebra 228 (2024), no. 4, 107511.
DOI: doi.org/10.1016/j.jpaa.2023.107511
Abstract: We prove that the Isomorphism Problem for group algebras reduces to group algebras over finite extensions of the prime field. In particular, the Modular Isomorphism Problem reduces to finite modular group algebras.