UNIVERSIDAD DE MURCIA

ESCUELA INTERNACIONAL DE DOCTORADO

TESIS DOCTORAL

The Isomorphism Problem for Rational Group Rings of Finite Metacyclic Groups.

El Problema del Isomorfismo en Anillos de Grupo Racionales de Grupos Metacíclicos Finitos.

D. Àngel García Blàzquez

2023

UNIVERSIDAD DE MURCIA

ESCUELA INTERNACIONAL DE DOCTORADO

TESIS DOCTORAL

The Isomorphism Problem for Rational Group Rings of Finite Metacyclic Groups.

El Problema del Isomorfismo en Anillos de Grupo Racionales de Grupos Metacíclicos Finitos.

Autor: Àngel García Blàzquez

Director: Ángel del Río Mateos

Dedication

To mom and dad.

Acknowledgements

I want to express my sincerest gratitude to Ángel del Río Mateos for his support, guidance and inestimable help over the course of my research career.

I would also like to thank my friends, family and partner, for being the core of my resilience.

I want to also thank Leo Margolis and Diego García Lucas. Leo for being someone that I could always count on for advice, and Diego for being the greatest travelling partner and Phd fellow that I could ask for.

I want to thank Juan Jacobo Simón Pinero and the members of the algebra department of the University of Murcia, for their assistance and support.

Finally, I want to give my gratitude to my colleagues of the Department of Mathematics of Firenze, for their support and embrace during my 3 months stay there.

Contents

Resumen **vii**

Abstract **xvii**

1 Preliminaries **1**

1.1 Number Theory 1

1.2 Group theory 5

1.3 Group Rings and the Isomorphism Problem 11

1.4 Wedderburn decomposition of rational group algebras 14

2 Finite Metacyclic Groups **19**

2.1 Introduction 19

2.2 Metacyclic factorizations 23

2.3 Proofs of Theorems A, B and C 39

2.4 A GAP implementation 41

3 The Nilpotent Case **49**

3.1 Introduction 49

3.2 ISO for finite metacyclic p-groups 53

3.3 ISO for finite metacyclic nilpotent groups 69

4 The General Case **73**

4.1 Introduction and sketch of the proof 73

4.2 $\mathbb{Q}G$ determines R^G 75

4.3 $\mathbb{Q}G$ determines s^G and ϵ^G 81

4.4 $\mathbb{Q}G$ determines m^G, n^G and r^G 88

4.5 $\mathbb{Q}G$ determines Δ^G 98

List of Symbols **109**

Bibliography **113**

Resumen

El Problema del Isomorfismo para anillos de grupo consiste en la siguiente pregunta: Dados un anillo conmutativo R y dos grupos G y H, si los anillos de grupo RG y RH son isomorfos entonces, ¿son G y H necesariamente isomorfos también? Es decir, ¿es toda la información del grupo inequívocamente recuperable del anillo de grupo? Vemos esto escrito simbólicamente como sigue:

$$RG \cong RH \quad \overset{?}{\Rightarrow} \quad G \cong H$$

De aquí en adelante, cuando decimos que para un anillo dado o para una clase de grupos dada el Problema del Isomorfismo tiene una respuesta positiva (o negativa), nos referimos a que la implicación anterior es lógicamente cierta (respectivamente, falsa) para ese anillo o para esa clase de grupos, es decir, un isomorfismo de álgebras de grupo implica (respectivamente, no implica) un isomorfismo de grupos en ese caso.

Este problema, y su especialización a un caso particular, se ha convertido en la pregunta principal estudiada en esta tesis. Decimos especialización porque afrontar el problema en su forma más general no tiene sentido, pues tomando grupos abelianos pequeños y el cuerpo de los números complejos (ver Example 1.13) podemos encontrar contraejemplos al caso general.

El Problema del Isomorfismo para álgebras de grupo fue propuesto por primera vez como problema durante la Conferencia de Álgebra de Michigan de 1947, por T.M. Thrall, que formuló el problema como sigue (traducido al español):

> *"Dados un grupo finito G y un cuerpo $\mathbb{K}$, encontrar todos los grupos distintos H para los que $\mathbb{K}G \cong \mathbb{K}H$."*

Este problema ha sido estudiado extensivamente, con énfasis especial en grupos finitos y

los casos donde el anillo de coeficientes es o bien un cuerpo o el anillo de enteros. Uno de los primeros resultados viene dado por G. Higman antes incluso de que se planteara el Problema del Isomorfismo para álgebras de grupo como tal. Higman demostró que si G y H son grupos abelianos finitos y $\mathbb{Z}G \cong \mathbb{Z}H$ entonces $G \cong H$ [Hig40a, Hig40b]. El mismo resultado para el cuerpo de números racionales en lugar de el anillo de números enteros fue probado por S. Perlis y G. L. Walker [PW50] (Theorem 1.12). Sin embargo, si G y H son grupos abelianos finitos con el mismo orden, entonces $\mathbb{C}G \cong \mathbb{C}H$ (este resultado se demostró también en el artículo anterior). Con este resultado se obtienen los contraejemplos sencillos que mencionamos anteriormente.

Se tiene un principio general para el Problema del Isomorfismo: “cuanto más pequeño sea el anillo de coeficientes, mayor la probabilidad de una respuesta positiva”. Esto es una consecuencia de que si K es una R-álgebra, entonces $KG \cong K \otimes_R RG$. Así, si $RG \cong RH$, entonces

$$KG \cong K \otimes_R RG \cong K \otimes_R RH \cong KH.$$

De esta forma, no solo $\mathbb{Z}$ es el anillo con mayor probabilidad de conseguir respuestas positivas al Problema del Isomorfismo, si no que si uno encontrara una respuesta negativa al Problema del Isomorfismo para $\mathbb{Z}$, este contraejemplo lo sería para cualquier otra reformulación del problema con distinto anillo R. Esto significó que la mayor parte de la investigación se centrara en este caso y se obtuvieron muchos resultados parciales. A continuación enumeramos una recoleccion no exhaustiva de clases de grupos para los que el Problema del Isomorfismo con coeficientes enteros tiene respuesta positiva:

- Grupos abelianos, por G. Higman en [Hig40a] y [Hig40b],
- Grupos metabelian, por A. Whitcomb en [Whi68],
- p-grupos, por K. W. Roggenkamp y L. Scott en [RS87],
- Grupos nilpotentes, por K. W. Roggenkamp y L. Scott en [RS87],
- Grupos abeliano-por-nilpotente, por K. W. Roggenkamp y L. Scott en [RS87] y unos meses después independientemente por A. Weiss en [Wei88],

- Grupos simples, por W. Kimmerle en [KLST90],
- Grupos superresolubles, por W. Kimmerle en [Kim91], Teorema 5.20
- Grupos de Frobenius y 2-Frobenius, en [Kim91], Teorema 5.17,
- Grupos nilpotente-por-abeliano, un resultado de W. Kimmerle que puede consultarse en [RT92], Capítulo XII.

A finales del siglo XX se pensaba que el resultado positivo definitivo para $\mathbb{Z}$ estaba en camino. Sin embargo, M. Hertweck encontró 2 grupos finitos resolubles no isomorfos con anillos de grupo enteros isomorfos [Her01]. Estos grupos tenían longitud de su serie derivada igual a cuatro y tamaño par, luego el problema sigue vivo para grupos impares y para grupos con longitud de su serie derivada igual a tres (longitud dos, o lo que es lo mismo, grupos metabelianos, tiene respuesta positiva, como hemos mencionado antes).

En un famoso artículo recopilatorio sobre representación de grupos finitos [Bra63], Brauer planteó las siguientes preguntas que pueden verse como variantes del Problema del Isomorfismo para álgebras de grupo sobre cuerpos (traducidas al español):

> “¿Si dos grupos G_1 y G_2 tienen álgebras de grupo isomorfas sobre todo cuerpo Ω, son G_1 y G_2 isomorfos?”.
>
> “¿Cuándo tienen dos grupos no isomorfos álgebras de grupo isomorfas?”,

Desviémonos un minuto en una tangente sobre la primera de las preguntas anteriores. Un teorema de Passman [Pas65] casi da una respuesta negativa a esta pregunta. Este teorema establece que existen

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

p-grupos no isomorfos de tamaño p^n con álgebras de grupo isomorfas sobre todos los cuerpos de característica distinta a p. Poco después, Dade encontró un contraejemplo [Dad71] al problema en cuestión. Encontró dos grupos finitos metabelianos no isomorfos con orden divisible por dos primos distintos, tales que sus álgebras de grupo son isomorfas sobre todo cuerpo.

Como los contraejemplos en el resultado de Dade no eran p-grupos, la pregunta de Brauer seguía abierta para p-grupos. Pero por el resultado de Passman sabemos que, para p-grupos, tener álgebras de grupo isomorfas sobre cuerpos de característica distinta a p no significa mucho, uno puede encontrar tantos p-grupos como se desee con esta propiedad.

Ahora, fijemos G y H dos p-grupos y consideremos la siguiente pregunta:

$$FG \cong FH \text{ para todo cuerpo } F \text{ de característica } p \overset{?}{\Rightarrow} G \cong H \tag{1}$$

Ahora, como sucedía con $\mathbb{Z}$, si denotamos como $\mathbb{F}_p$ al cuerpo finito de p elementos y F es cualquier cuerpo de característica p, tenemos:

$$\mathbb{F}_pG \cong \mathbb{F}_pH \Rightarrow FG \cong F \otimes_{\mathbb{F}_p} \mathbb{F}_pG \cong F \otimes_{\mathbb{F}_p} \mathbb{F}_pH \cong FH$$

Entonces, la pregunta (1) es realmente equivalente a

$$\mathbb{F}_pG \cong \mathbb{F}_pH \overset{?}{\Rightarrow} G \cong H \tag{2}$$

Esta última preunta es la que es conocida comúnmente como el Problema del Isomorfismo Modular (o MIP). Este problema a día de hoy ha sido resuelto para cierto número de casos. El más interesante en relación con la tesis es la demostración de la respuesta positiva al MIP para grupos metacíclicos, por Baginski para $p > 3$ [Bag88] y posteriormente Sandling completó la demostración [San96].

Recientemente se ha encontrado una respuesta negativa al MIP general, en un artículo por D. García-Lucas, L. Margolis y Á. del Río [GLMdR22]. Para más información sobre el Problema del Isomorfismo véase [Pas77, Capítulo 14], [Seh78, Capítulo III] y el reciente artículo recopilatorio [Mar22].

Ahora, el problema al que nos enfrentamos en esta tesis es la variante del Problema del Isomorfismo para $R = \mathbb{Q}$ y considerando grupos metacíclicos finitos:

$$\mathbb{Q}G \cong \mathbb{Q}H \overset{?}{\Rightarrow} G \cong H \tag{3}$$

Cuando mi tutor del doctorado me propuso la idea de trabajar en el Problema del Isomorfismo de álgebras de grupo de grupos metacíclicos finitos, mi intención inicial fue encontrar un contraejemplo. Hay un artículo de 2009 [HOdR09] en el que se probó que los isomorfismos de anillos entre componentes simples de álgebras de grupo racionales de grupos metacíclicos finitos están determinados por su centro, la dimensión sobre $\mathbb{Q}$ y la lista de índices de Schur locales en primos racionales. Esto significa que para cada grupo G teníamos una lista de invariantes para cada componente simple de la descomposición de Wedderburn de $\mathbb{Q}G$, de forma que uno puede tomar la librería de grupos pequeños de GAP [GAP12], recorriendo todos los grupos de tamaños entre 2 y 2000, computando los invariantes y comprobando si hay alguna coincidencia para los invariantes de dos grupos diferentes. En caso de que haya, tenemos un contraejemplo en nuestras manos. Esta estrategia se implantó durante mi primer semestre como estudiante de doctorado y los resultados fueron vacíos. No encontramos un contraejemplo, pero esto significaba que no podíamos negarnos a considerar la posibilidad de que la respuesta fuera positiva en este caso. Si consideramos el Problema del Isomorfismo Modular, en ese caso la respuesta es positiva para metacíclicos, así que esto al menos es un buen indicador de esperanza para el caso de característica cero.

Esto nos lleva a los contenidos de la tesis, que se centra entorno a probar la respuesta positiva. El documento está dividido en cuatro partes: En el primer capítulo introducimos los conceptos principales, la notación y probamos algunos resultados auxiliares básicos. El siguiente capítulo está dedicado a la clasificación de los grupos metacíclicos finitos, recogida en [GBdR23a]. El tercer capítulo consiste en la solución positiva para el Problema del Isomorfismo para anillos de grupo de grupos metacíclicos finitos. El resultado puede encontrarse en [GBdR23b]. El último capítulo está centrado en generalizar el resultado a grupos metacíclicos finitos, apoyándonos en tanto el resultado para grupos nilpotentes como en el la clasificación de grupos metacíclicos. Este resultado para el caso general se encuentra en [GBdR23c].

Como hemos mencionado, la mayor parte del capítulo 1 está dedicado a introducir la notación y los conceptos de la tesis. En la sección 1.1 introducimos un importante lema, Lemma 1.1. Es un resultado que se usa para cálculos y es importante porque será usado frecuentemente a lo largo de la tesis. También es importante que en la sección 1.2 introducimos las definiciones de los parámetros de grupos metacíclicos que en el capítulo 2 se demostrará que son invariantes que determinan cada grupo metacíclico finito. En las secciones 1.3 y 1.4 introducimos formalmente el concepto de anillo de grupo y damos un pequeño resumen de su historia. También damos una construcción que será muy importante en el documento. Vamos a elaborar sobre esta construcción. Al tratar de resolver el Problema del Isomorfismo, es de extrema importancia ser capaces de traducir la información estructural de $\mathbb{Q}G$ a G. En [OdRS04], A. Olivieri, J. J. Simón y Á. del Río introdujeron el concepto de par de Shoda fuerte. Éstos son pares de subgrupos de un grupo que, en otro artículo de los mismos autores [OdRS06], se demuestra que se encuentran en una correspondencia biyectiva con las componentes simples de Wedderburn del álgebra de grupo racional del mismo grupo, al menos en el caso metacíclico. De esta forma, cuando queramos encontrar información sobre un grupo metacíclico, solo tenemos que ver cómo puede reflejarse esta información en pares de Shoda y qué componentes están asociadas a estos pares de Shoda. Esto puede parecer más sencillo de lo que es en la práctica, pero en cualquier caso esta estrategia es clave en los argumentos usados para algunas de las demostraciones en el capítulo 3 y la mayoría de las demostraciones en el capítulo 4.

En el segundo capítulo de esta tesis nos centramos en clasificar los grupos metacíclicos finitos. Esta clasificación se apoya en la clasificación original por C. E. Hempel [Hem00], pero se diferencia en la mayoría de argumentos y el resultado final. Necesitábamos obtener una clasificación que se prestara a un enfoque computacional. También necesitábamos ser capaces de identificar claramente los invariantes del grupo. De esta forma, la sección 2.1 se centra en enunciar los teoremas principales y explicar los detalles de la clasificación. La sección 2.2 está dedicada a probar lemas auxiliares. En particular, el Lemma 2.4 da una idea sobre la estructura del grupo y será usado a menudo en el último capítulo de la tesis. El motivo es que simplifica la obtención de los parametros del grupo que son triviales en el caso nilpotente (el caso estudiado en el capítulo 3) pero necesitan ser considerados en el caso general. En la misma sección, el Lemma 2.6 es relevante porque muestra qué invariante va a ser problemático y en qué caso. La Proposition 2.7 y el Algorithm 1 asociado son el núcleo del enfoque computacional al problema. Con este resultado probamos cómo obtener, numéricamente, una factorización minimal de un grupo metacíclico. Esto es absolutamente necesario para después construir el paquete de software que nos permitirá obtener los invariantes metacíclicos de cualquier grupo metacíclico finito. El Lemma 2.8 muestra de dónde viene el parámetro más intricado (1.4) de los grupos metacíclicos y por qué es necesario. Finalmente, el Theorem 2.9 usa el lema anterior para acabar de determinar cuándo es un invariante el último parámetro. En la sección 2.3 usamos los resultados de las secciones anteriores para demostrar los teoremas principales. La mayoría de las demostraciones son directas, pues la mayor parte del trabajo se realiza en la sección 2.2. La última sección es sobre la implementación computacional. Es una descripción general del paquete de GAP [GAP12], recorriendo las funciones y algoritmos principales, incluyendo una función que computa los invariantes metacíclicos de un grupo metacíclico dado como argumento y una función que computa todos los grupos metacíclicos de un tamaño dado. Esta última función requiere dar condiciones numéricas para comprobar cuándo se tiene que una lista de parámetros se corresponde con un grupo metacíclico existente. La mayoría de estas condiciones numéricas se demuestran a lo largo de las secciones anteriores y en el Lemma 2.12 se compilan y se demuestran las que quedan.

Vamos ahora a centrarnos en el tercer capítulo. Como mencionamos, en el tercer capítulo se demuestra que el Problema del Isomorfismo para anillos de grupo racionales de p-grupos metacíclicos finitos tiene una respuesta positiva. La primera estrategia para resolver este problema se apoyaba en usar 4 invariantes específicos del grupo que pueden encontrarse en el anillo de grupo. Consideremos un grupo G. El primer invariante sería $|G|$. Éste es la dimensión de $\mathbb{Q}G$. Otro invariante es la clase de isomorfía de G/G'. Esto es porque las componentes de Wedderburn de $\mathbb{Q}(G/G')$ son exactamente las componentes conmutativas de la descomposición de Wedderburn de $\mathbb{Q}G$ y porque por un Teorema de Perlis-Walker (Theorem 1.12), $\mathbb{Q}H$ determina H para cualquier grupo abeliano H. En resumen, las componentes conmutativas de $\mathbb{Q}G$ determinan G/G'. Un tercer invariante sería el número de clases de conjugación de G. Es bien sabido que este número es igual a la dimensión del centro de la componente sobre $\mathbb{Q}$. El último invariante es el número de clases de conjugación de subgrupos cíclicos de G. Éste es igual al número de componentes simples de la descomposición de Wedderburn de $\mathbb{Q}G$ (véase Theorem 1.11). Nuestra esperanza era ser capaces de identificar G salvo isomorfismo usando estos 4 invariantes y casi tenemos éxito. Hay casos específicos, en los que el grupo es un 2-grupo, en que estos invariantes no son capaces de determinar el grupo. Un ejemplo de dos 2-grupos metacíclicos que tienen estos cuatro invariantes iguales se da en Example 3.7. Ahora, como estas condiciones están más o menos aisladas, realmente podemos lidiar con los casos restantes buscando componentes específicas en $\mathbb{Q}G$ que diferencien los pares de grupos que tengan invariantes iguales. Esto se hace en el Lemma 3.8 y el Lemma 3.9. Finalmente, el resultado para p-grupos se demuestra en el Theorem 3.10.

La generalización a grupos nilpotentes es sorprendentemente directa. Definimos propiedades para identificar ciertas componentes de la descomposición de Wedderburn del álgebra de grupo. Después probamos en el Lemma 3.15 que la suma de estas componentes es realmente isomorfa a un número determinado de copias del álgebra de grupo sobre un p-subgrupo de Sylow de G, para ciertos primos. En el caso nilpotente los primos para los que sucede esto son todos aquéllos que dividen al orden de G. Esto nos ofrece una manera de obtener un isomorfismo de álgebras de grupo de p-grupos a partir de un isomorfismo de álgebras de grupo de grupos nilpotentes. Llegados a este punto, ya hemos probado que si las álgebras de grupo de dos p-grupos son isomorfas, los grupos también son isomorfos, y en el caso de nilpotentes si todos los p-subgrupos de Sylow son isomorfos entonces los grupos en sí son isomorfos, así que obtenemos el resultado deseado.

Finalmente, en el último capítulo estudiamos la demostración del caso general. En la sección 4.1 simplemente introducimos el teorema principal y fijamos notación para el resto del capítulo. En adelante, el resto de secciones se centran en probar que el álgebra de grupo determina cada uno de los invariantes del grupo. De esta forma, al probar en la última sección que el álgebra de grupo determina el último invariante necesario para describir el grupo, hemos acabado la demostración del resultado positivo para el Problema del Isomorfismo para grupos metacíclicos finitos. En la sección 4.2 comenzamos fijando condiciones sobre cuerpos. Estas condiciones sirven para identificar componentes de Wedderburn del álgebra de grupo con ciertas propiedades. En el Lemma 4.2 se demuestra que existen componentes con estas propiedades. También probamos que si existen entonces tienen que venir de pares de Shoda fuertes muy específicos, de forma que en la estructura de la componente como extensión de Galois de $\mathbb{Q}$ podemos encontrar información sobre el parámetro que estamos buscando. Limitamos las posibilidades para los pares de Shoda en el Lemma 4.3 y el Lemma 4.4. Estos dos lemas, en particular, serán usados de nuevo más adelante en argumentos similares. La estrategia que acabamos de describir se usa varias veces a lo largo del capítulo, con distintas condiciones para los cuerpos y distintas variaciones para lidiar con cada caso. En el inicio de la sección 4.3 usamos argumentos numéricos y resultados del capítulo 2 para probar que un invariante específico puede encontrarse en el álgebra de grupo. En la segunda parte de la sección usamos un argumento similar al usado en la sección anterior para acabar con otro invariante. En la sección 4.4 los argumentos se vuelven más técnicos y necesitamos usar algunos lemas sobre subgrupos cocíclicos (Lemma 1.7 y Lemma 4.13). La estrategia seguida en esta sección es similar a la usada en las secciones anteriores, pero en este caso la parte de determinar qué pares de Shoda pueden corresponderse con las componentes con las condiciones dadas se complica bastante. Finalmente, en la sección 4.5 acabamos la demostración mostrando que $\mathbb{Q}G$ determina el último invariante de G. Esta sección se divide en tres casos, porque para cada caso necesitamos usar diferentes condiciones sobre las componentes de Wedderburn del álgebra de grupo. La estrategia es muy similar a la usada en la sección 4.2: Primero fijamos condiciones sobre las componentes de Wedderburn, a continuación encontramos pares de Shoda para los que las componentes simples asociadas satisfacen las condiciones. Después, restringimos qué pares de Shoda pueden estar asociados a una componente que satisfaga las condiciones. De esta forma, incluso aunque los pares de Shoda no sean exactamente los mismos, probamos que la mera existencia de componentes isomorfas cumpliendo las condiciones en ambas álgebras de grupo significa que el invariante ha de ser igual en los grupos. Para esto usamos la construcción de las componentes de [OdRS06] (véase Theorem 1.19) y Teoría de Galois.

Una vez hemos probado que cada uno de los invariantes está determinado por el álgebra de grupo, como hemos probado en el capítulo 2 que estos invariantes son suficientes para describir el grupo salvo isomorfismo, hemos acabado la demostración del resultado positivo para el Problema del Isomorfismo de álgebras de grupo de grupos metacíclicos finitos.

Abstract

The Isomorphism Problem for group rings asks the following question: Given a commutative ring R and two groups G and H, if the group rings RG and RH are isomorphic then, are G and H necessarily isomorphic as well? i.e. Is all of the information of the group unambiguously recoverable from the group ring? We write this as follows:

$$RG \cong RH \quad \overset{?}{\Rightarrow} \quad G \cong H$$

From now on, when we say that for a given ring or for a given class of groups the Isomorphism Problem has a positive (or negative) answer, we mean that the previous implication is logically true (respectively, false) for that ring or that class of groups, i.e. an isomorphism of group algebras gives (respectively, does not give) an isomorphism for groups in that case.

This problem, and its specialization to a particular case, has become the main question studied in this thesis. We say specialization because tackling the whole problem at once does not make sense, as the most general statement can be proven wrong with small abelian groups and the complex field (see Example 1.13).

The Isomorphism Problem was first proposed as a problem during the Michigan Algebra Conference of 1947, by T.M. Thrall, who formulated the problem as follows:

> *"Given a finite group G and a field $\mathbb{K}$, find all other groups H for which $\mathbb{K}G \cong \mathbb{K}H$."*

This problem has been studied extensively, with special emphasis on finite groups and the cases where the coefficient ring is either a field or the ring of integers. One of the first results is due to G. Higman from before the problem was even stated. He proved that if G and H are finite abelian groups and $\mathbb{Z}G \cong \mathbb{Z}H$, then $G \cong H$ [Hig40a, Hig40b]. The same result for

the field of rationals instead of the ring of integers was proved by S. Perlis and G. L. Walker [PW50] (Theorem 1.12). However, if G and H are finite abelian groups of the same order, then $\mathbb{C}G \cong \mathbb{C}H$ (this result was also proved in the previous article). This leads to the easy counterexamples to the general case that we mentioned before.

This also illustrates a general principle for the Isomorphism Problem: "the smaller the coefficient ring the greater the chances for a positive answer". This is a consequence of the fact that if K is an R-algebra, then $KG \cong K \otimes_R RG$. Hence, if $RG \cong RH$, then

$$KG \cong K \otimes_R RG \cong K \otimes_R RH \cong KH.$$

So, not only $\mathbb{Z}$ is the ring with greatest chances to get positive answers to the Isomorphism Problem, but a negative answer to the Isomorphism Problem for $\mathbb{Z}$ is also a negative answer for every other possible variant of the problem with a different ring. This meant that a lot of the research was focused on this case and many partial results were obtained. Let us list some of the types of groups for which the Isomorphism Problem for integral coefficients was proved to be true:

- Abelian groups, by G. Higman in [Hig40a] and [Hig40b],
- Metabelian groups, by A. Whitcomb in [Whi68],
- p-groups, by K. W. Roggenkamp and L. Scott in [RS87],
- Nilpotent groups, by K. W. Roggenkamp and L. Scott in [RS87],
- Abelian-by-nilpotent groups, by K. W. Roggenkamp and L. Scott in [RS87] and few months later independently by A. Weiss in [Wei88],
- Simple groups, by W. Kimmerle in [KLST90],
- Supersolvable groups, by W. Kimmerle in [Kim91], Theorem 5.20
- Frobenius and 2-Frobenius groups, by [Kim91], Theorem 5.17,
- Nilpotent-by-abelian groups, a result by W. Kimmerle that can be consulted in [RT92], Chapter XII.

For a while it seemed like a definitive positive result for $\mathbb{Z}$ was coming. However, M. Hertweck found two non-isomorphic finite solvable groups with isomorphic integral group rings [Her01]. These groups have derived length 4 and even size, so the problem still continues alive for groups of odd order or derived length 3 (for derived length 2, i.e. metabelian, as we said before the answer to the Isomorphism Problem is positive).

In an influential survey paper on representations of finite groups [Bra63], Brauer posed the following questions that can be seen as variants of the Isomorphism Problem for group algebras over fields:

> “If two groups G_1 and G_2 have isomorphic group algebras over every ground field Ω, are G_1 and G_2 isomorphic?”.
>
> “When two non-isomorphic groups have isomorphic group algebras?”,

Let us go in a tangent about the former question. A theorem by Passman [Pas65] almost gives a negative answer to this one. This theorem proves that there exist

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

non-isomorphic p-groups of order p^n that have isomorphic group algebras over all fields of characteristic not equal to p. This result will be relevant in a minute.

A couple years later, Dade found a counterexample [Dad71] to the problem in question. He found two non-isomorphic metabelian finite groups, with order divisible by two different primes, such that their group algebras were isomorphic over every field.

As the counterexamples in Dade's result were not p-groups, Brauer's question was still open for p-groups. However, by Passman result, we know that for p-groups having isomorphic group algebras over fields of characteristic not equal to p does not mean much, as one can find as many non-isomorphic p-groups as one wants with this property.

Now, fix two p-groups G and H and let us consider the following question:

$$FG \cong FH \text{ for every field } F \text{ of characteristic } p \overset{?}{\Rightarrow} G \cong H \tag{4}$$

Now, as it happened with $\mathbb{Z}$, if we denote $\mathbb{F}_p$ the finite field of p elements and F is any field of characteristic p, we have:

$$\mathbb{F}_pG \cong \mathbb{F}_pH \Rightarrow FG \cong F \otimes_{\mathbb{F}_p} \mathbb{F}_pG \cong F \otimes_{\mathbb{F}_p} \mathbb{F}_pH \cong FH$$

So, the question (4) is actually equivalent to

$$\mathbb{F}_p G \cong \mathbb{F}_p H \overset{?}{\Rightarrow} G \cong H \tag{5}$$

This last question is what is commonly known as the Modular Isomorphism Problem (or MIP). This problem has been solved for a number of cases. The one that is of most interest for us is that it was proved to be true for metacyclic groups, by Baginski for $p > 3$ [Bag88] and Sandling completed the proof [San96].

Recently, the MIP has been given a negative answer, in an article by D. García-Lucas, L. Margolis and Á. del Río [GLMdR22]. For more information on the Isomorphism Problem see [Pas77, Chapter 14], [Seh78, Chapter III] and the recent survey [Mar22].

Now, the problem that we face in this thesis is the variant of the Isomorphism Problem for $R = \mathbb{Q}$ and considering metacyclic finite groups:

$$\mathbb{Q}G \cong \mathbb{Q}H \overset{?}{\Rightarrow} G \cong H \tag{6}$$

When I was proposed by my thesis advisor the idea of going after the Isomorphism Problem for rational group algebras of finite metacyclic groups, my initial intention was to prove it wrong. There is a 2009 article [HOdR09] where it was proved that ring isomorphisms between simple components of the rational group algebras of finite metacyclic groups are determined by the center, the dimension over $\mathbb{Q}$ and the list of local Schur indices at rational primes. This means that for each group G we had a list of invariants for each simple Wedderburn component of $\mathbb{Q}G$ to work with, such that one could go ahead and use the library of small groups of GAP [GAP12], going over all of the groups of sizes between 2 and 2000, and compute these invariants, then check if there were any coincidences for the invariants for two different groups and if so, we had a counterexample in our hands. This strategy was put into place during my first semester as a PhD student and the results were void. We did not find a counterexample, but this meant that we should not easily disregard the possibility of a positive answer existing. When looking at the Modular Isomorphism Problem, the answer is positive for metacyclic, so that is at least an indicator of hope for characteristic zero.

This leads us to the contents of the thesis, which is centered around proving the positive answer. The document is divided in four parts: In the first chapter, we introduce the main concepts, notation and prove some basic auxiliary results. The next chapter is dedicated to a classification of finite metacyclic groups, which is the recollected in [GBdR23a]. The third chapter consists of the positive solution for the Isomorphism Problem for rational group rings of metacyclic nilpotent groups. The result can be found in [GBdR23b]. The last chapter is focused on generalizing the result to general finite metacyclic groups, relying heavily in both the result for nilpotent groups and the classification of finite metacyclic groups. This result is collected in [GBdR23c].

As we said, most of Chapter 1 is dedicated to introducing the notation and the concepts of the thesis. One important lemma, Lemma 1.1 is introduced in Section 1.1. It is a result that is used for computations and it is important because it will be used commonly throughout the thesis. Another remarkable thing from this chapter is that in Section 1.2 we introduce the definitions of the parameters that in Chapter 2 will be proved to be the invariants determining each finite metacyclic group up to isomorphism. In Section 1.3 and Section 1.4 we introduce formally the concept of group ring and we give some history about it, as well as giving a construction that will be very important in the thesis. Let us elaborate for a minute. When trying to solve the Isomorphism Problem, it is of utmost importance to be able to translate structural information from $\mathbb{Q}G$ to G. In [OdRS04], A. Olivieri, J. J. Simón and Á. del Río introduced the concept of strong shoda pair. These are pairs of subgroups of a group which, in another article by the same authors [OdRS06], are shown to be in a bijective correspondence with the Wedderburn components of the rational group algebra of the same group, in the metacyclic case. This way, whenever we want to get information about a metacyclic group G, we just need to see how this information can be reflected in Shoda pairs and what are the components associated to these Shoda pairs. This sound easier than it is in practice but it is the keystone of the arguments used for some of the proofs in Chapter 3 and most of the proofs in Chapter 4.

In the second chapter of this thesis we focus on classifying the finite metacyclic groups. This classification relies on the original classification by C. E. Hempel [Hem00], but differs from it in most of the arguments and the ending result. We needed to obtain a classification that lent itself to a computational approach. We also needed to be able to clearly identify the invariants of the group. This way, Section 2.1 is focused on giving the statements of the

main theorems and explaining the details of the classification. Section 2.2 is dedicated to proving auxiliary lemmas. In particular, Lemma 2.4 gives a lot of insight into the structure of the group and will be used a great deal in the last chapter of the thesis. The reason is that it simplifies obtaining the parameters of the group that are trivial in the nilpotent case (the case in Chapter 3) but which need to be considered in the general case. In the same section, Lemma 2.6 is relevant because shows which of the invariants is going to be problematic and in which cases. Proposition 2.7 and its associated Algorithm 1 are the core of the computational approach to the problem. With this result we prove how to obtain, numerically, a minimal factorization of a metacyclic group. This is absolutely necessary to later make the software package that will allow us to obtain the metacyclic invariants of any finite metacyclic groups. Lemma 2.8 shows where the most intricate parameters for the metacyclic group (1.4) come from and why they are necessary. Finally, Theorem 2.9 uses the previous lemma to finish determining when the last parameter is an invariant. Section 2.3 uses the results of the previous sections to prove the main theorems. Most of the proofs in this section are straightforward, as most of the work has been done in Section 2.2. The last section of Chapter 2 is all about the computer implementation. It is an overview of the GAP [GAP12] package, going over the main functions and algorithms, including a function that computes the metacyclic invariants of a given metacyclic group and a function that computes all metacyclic groups of a given size. The latter function requires giving numerical conditions to check when the list of parameters corresponds to an existing metacyclic group. Most of the conditions have already been explained as their significance affected other results along the chapter. In Lemma 2.12 we compile them and we prove the remaining ones.

Let us focus on the third chapter now. As we said, in the third chapter we prove that the Isomorphism Problem for rational group rings of finite metacyclic p-groups has a positive answer. The first strategy to prove this problem relied heavily on using four specific invariants from the group that can be found in the Wedderburn decomposition of the group ring. Let us consider a group G. The first invariant would be $|G|$, which is the dimension of $\mathbb{Q}G$. Another invariant is the isomorphism class of G/G'. This is because the Wedderburn components of $\mathbb{Q}(G/G')$ are exactly the commutative components of the Wedderburn decomposition of $\mathbb{Q}G$ and because, by a Perlis-Walker Theorem (Theorem 1.12), $\mathbb{Q}H$ determines H for any

abelian group H. In short, the commutative components of the Wedderburn decomposition of $\mathbb{Q}G$ determine G/G'. A third invariant would be the number of conjugacy classes of G. This number is known to be the dimension of the center of $\mathbb{Q}G$ over $\mathbb{Q}$. The final invariant is the number of conjugacy classes of cyclic subgroups of G. This is equal to the number of simple components of $\mathbb{Q}G$ (see Theorem 1.11). Our hope was being able to identify G up to isomorphism using these 4 invariants and we almost succeeded. There are specific cases, when the group is a 2-group and other circumstances arise, in which these invariants are not able to determine the group. An example of two metacyclic 2-groups which have these 4 invariants equal is Example 3.7. Now, as these conditions are fairly isolated, we can actually deal with the few remaining cases by looking for specific components in $\mathbb{Q}G$ that differentiate the pairs of groups which have equal invariants. This is done in Lemma 3.8 and Lemma 3.9. Finally, the result for p-groups is proved in Theorem 3.10.

The generalization to nilpotent groups is surprisingly straightforward. We define properties to identify certain components of the Wedderburn decomposition of the group algebra. Then we prove in Lemma 3.15 that the sum of these components is actually isomorphic to a known number of copies of the group algebra over a Sylow p-subgroup of the group, for certain primes. In the nilpotent case this is true for all primes dividing the order of the group. This gives us a way to obtain an isomorphism of group algebras of p-groups from an isomorphism of groups algebras of nilpotent groups. By this point we have already proved that if the group algebras of p-groups are isomorphic, the groups themselves are isomorphic, and in nilpotent groups if all Sylow p-subgroups are isomorphic, then the groups are isomorphic, so we have our result.

Finally, in the last chapter we go over the prove of the general case. In Section 4.1 we simply introduce the main theorem and fix some notation for the rest of the chapter. From this point on, the rest of the sections focus on proving that the group algebra determines one of the invariants of the group. This way, when we prove in the last section that the group algebra determines the last invariant to describe the group, we have finished the proof of the positive result of the Isomorphism Problem for metacyclic groups. In Section 4.2 we start by fixing some conditions on fields. This conditions are meant to identify Wedderburn components of the group algebra with certain properties. We prove that these components

necessarily exist in Lemma 4.2. We also prove that they have to come from very specific strong Shoda pairs, such that in the structure of the component as a Galois extension of $\mathbb{Q}$ we can find the information about the parameter that we are looking for. We limit the possibilities for the Shoda pairs in Lemma 4.3 and Lemma 4.4. These particular two lemmas will be used again later for similar arguments. The strategy that we have just covered is imitated several times during the chapter, with different conditions for the fields and different variations to deal with each case. At the beginning of Section 4.3 we use numerical arguments and results from Chapter 2 to prove that we can obtain one of the invariants from the group algebra. On the second half of the section we use a similar argument to the one used in the previous section to fix another invariant. In Section 4.4 the arguments get more technical and we need to use a couple of lemmas about cocyclic subgroups (Lemma 1.7 and Lemma 4.13). The strategy followed in this section is similar to the one used in the previous ones, but in this case the part of determining which Shoda pairs can correspond to the components with the given conditions gets pretty convoluted. Finally, in Section 4.5, we finish the proof by showing that $\mathbb{Q}G$ determines the last invariant. This section is divided in three cases, because for each case we need to use different conditions over the Wedderburn components of the group algebra. The strategy is very similar to the one used in Section 4.2: We fix conditions over the Wedderburn components, then we find Shoda pairs for which the associated simple components satisfy the conditions. Next, we restrict which Shoda pairs can be associated to any component that satisfies the conditions. Now, even if the Shoda pairs are not exactly the same, we prove that the mere existence of isomorphic components satisfying the conditions in both group algebras means that the invariant has to be equal in the groups. For this we use the construction of the components taken from [OdRS06] (see Theorem 1.19) and Galois Theory.

Once we have the proof that each of the invariants are determined by the group algebra, as we have proved in Chapter 2 that these invariants are enough to describe the group up to isomorphism, we have finished the proof of the positive result for the Isomorphism Problem of group algebras of finite metacyclic groups.

CHAPTER 1

Preliminaries

In this chapter we are going to present the general concepts and results that will be used throughout the thesis. Along the document we will explain each symbol explicitly but, regardless, at the end of the document (page 112) there will be an exhaustive recollection of the notation.

1.1 Number Theory

In this section we will fixed most of the notation regarding number theory concepts and other concepts related to those. We also prove a lemma that will be used constantly over the course of the document. We adopt the convention that $0 \notin \mathbb{N}$ and prime means prime in $\mathbb{N}$. Let $n \in \mathbb{N}$ and p a prime. Then, we denote

$n_p =$ Greatest power of p dividing n.

$n_\pi = \Pi_{p\in\pi} n_p$, where π is any set of primes.

$v_p(n) =$ Highest positive integer m such that p^m divides n ($n_p = p^{v_p(n)}$).

$\pi(n) =$ Set of primes dividing n.

$\zeta_n =$ A complex primitive n-th root of the unity.

$\mathbb{Q}_n =$ The cyclotomic field $\mathbb{Q}(\zeta_n)$.

$\mathcal{C}_n =$ Cyclic group of order n.

$\mathcal{U}_n =$ Group of units of $\mathbb{Z}/nZ$.

$[t]_n =$ The element of $\mathcal{U}_n$ represented by $t \in \mathbb{Z}$ with $\gcd(t, n) = 1$.

$\langle t\rangle_n =$ Subgroup of $\mathcal{U}_n$ generated by $[t]_n$.

$o_n(t) =$ Order of $[t]_n$ in $\mathcal{U}_n$, this is, the minimal integer m such that $t^m \equiv 1 \mod n$.

$\mathrm{Res}_q =$ Natural map $\mathrm{Res}_q : \mathcal{U}_n \to \mathcal{U}_q$, with $\mathrm{Res}_q([t]_n) = [t]_q$ where q divides n.

We will see more about Res_q later. Now, given $a \in \mathbb{N}$, we also denote

$$\mathcal{S}\left(a \mid n\right) = \sum_{i=0}^{n-1} a^i = \begin{cases} n, & \text{if } a = 1; \\ \frac{a^n-1}{a-1}, & \text{otherwise.} \end{cases}$$

This notation occurs in the following statement where g and h are elements of a group:

$$\text{If } g^h = g^a \text{ then } (hg)^n = h^n g^{\mathcal{S}(a|n)}. \tag{1.1}$$

The following lemma collects some useful properties of the operator $\mathcal{S}\left(- \mid -\right)$ which will be used throughout the thesis. Some of these properties will be referenced very frequently, so we remark the importance of this auxiliary result.

Lemma 1.1. *Let $p, R, m \in \mathbb{N}$ with p prime and suppose that $R \equiv 1 \mod p$. We also denote $a = v_p(R-1) > 0$.*

(1) Suppose that either $p \neq 2$ or $p = 2$ and $R \equiv 1 \mod 4$. Then

(a) $v_p(R^m - 1) = a + v_p(m)$ and $v_p(\mathcal{S}\left(R \mid m\right)) = v_p(m)$.

(b) $o_{p^m}(R) = p^{\max(0,m-a)}$.

(c) If $a \leq m$ *then* $\langle R \rangle_{p^m} = \{[1 + yp^a]_{p^m} : 0 \leq y < p^{m-a}\}$.

(d) Suppose that $a \leq m$. *If* $n \in \mathbb{N}$ *and* $n \equiv kp^{m-a} \mod p^m$ *for some* $k \in \mathbb{N}$ *with* $p \nmid k$ *then*

$$\mathcal{S}\left(R \mid n\right) \equiv \begin{cases} n + k2^{m-1} \mod 2^m, & \text{if } p = 2 \text{ and } m > a; \\ n \mod p^m, & \text{otherwise.} \end{cases}$$

(2) Suppose that $R \equiv -1 \mod 4$. *Then*

(a) $$v_2(R^m - 1) = \begin{cases} v_2(R+1) + v_2(m), & \text{if } 2 \mid m; \\ 1, & \text{otherwise}; \end{cases}$$

and $$v_2(\mathcal{S}\left(R \mid m\right)) = \begin{cases} v_2(R+1) + v_2(m) - 1, & \text{if } 2 \mid m; \\ 0, & \text{otherwise}; \end{cases}.$$

(b) $$o_{2^m}(R) = \begin{cases} 1, & \text{if } m \leq 1; \\ 2^{\max(1, m - v_2(R+1))}, & \text{otherwise} \end{cases}.$$

(c) $$v_2(R^m + 1) = \begin{cases} v_2(R+1), & \text{if } 2 \nmid m; \\ 1, & \text{otherwise.} \end{cases}.$$

Proof. (1a) To prove the first equality let us start by proving a simpler case: $v_p(R^p - 1) = a + v_p(1)$. We can write $R = 1 + bp^a$ for an integer b such that $p \nmid b$. Then:

$$R^p = 1 + bp^{a+1} + \sum_{i=2}^{p} \binom{p}{i} b^i p^{ai}. \tag{1.2}$$

Now, if $a \geq 2$, then $ai \geq i + 2$ for every i in the range of the sum. On the one hand, p^{a+2} divides all of the terms of the sum but it does not divide ba^{p+1}. On the other hand, p^{a+1} divides everyone, so clearing the 1 we obtain from the previous equation the result in this case: $v_p(R^p - 1) = a + 1$. Let us finish the case where $a = 1$. In this case, p is odd, as the hypothesis says that when $p = 2$, $a \geq 2$. Then:

$$R^p = 1 + bp^2 + \binom{p}{2} b^2 p^2 + \sum_{i=3}^{p} \binom{p}{i} b^i p^i.$$

In this case, p^3 divides the terms in the sum, and also divides $\binom{p}{2}b^2p^2$, because as p is odd, p divides $\binom{p}{2}$. But it does not divide b^{p^2}. On the contrary, p^2 divides all of them, so $v_p(R^p-1) = 2 = a+1$ in this case as well. We have proved the formula $1+v_p(R-1) = v_p(R^p-1)$, but now we can use it to prove the following formula for powers of p: $v_p(m)+v_p(R-1) = v_p(R^{p^m}-1)$. Operating by induction, we have proved the result for $m = 1$, so let us assume the result true for $m-1$ and let us prove it for m:

$$v_p(R^{p^m}-1) = v_p((R^{p^{m-1}})^p-1) = 1+v_p(R^{p^{m-1}}-1) = 1+v_p(m-1)+v_p(R-1) = v_p(m)+v_p(R-1).$$

In the second equality we used the formula already proved and in the third equality we used the induction hypothesis. Now we only have left to prove it for an integer m that is not necessarily a power of m, but this is easy:

$$v_p(R^m-1) = v_p((R^{m_{p'}})^{m_p}-1) = v_p(m_p) + v_p(R^{m_{p'}}-1) = v_p(m) + v_p(R-1).$$

This is because $v_p(R^{m_{p'}}-1) = v_p(R-1)$. This can be seen using the same argument as in equation (1.2), taking m'_p instead of p. Now, the second equality follows using the first one and the equality $R^m - 1 = (R-1)\mathcal{S}(R \mid m)$.

(1b) is a direct consequence of (1a).

(1c) By (1a) we have $\langle R\rangle_{p^m} \subseteq \{[1+yp^a]_{p^m} : 0 \le y < p^{m-a}\}$ and by (1b) the first set has p^{m-a} elements. As the second one has the same cardinality, equality holds.

(1d) We first assume that $n = p^{m-a}$. By (1c) we have

$$\begin{aligned}\mathcal{S}(R \mid n) &\equiv \sum_{y=0}^{p^{m-a}-1}(1+yp^a) = p^{m-a} + p^a\sum_{y=0}^{p^{m-a}-1} y\\ &= p^{m-a} + \frac{p^m(p^{m-a}-1)}{2} \equiv \begin{cases} 2^{m-a}+2^{m-1} \mod 2^m, & \text{if } p=2 \text{ and } m>a;\\ p^{m-a} \mod p^m, & \text{otherwise.}\end{cases}\end{aligned}.$$

Now suppose that $n = kp^{m-a}$. Then $R^{p^{m-a}} \equiv 1 \mod p^m$, by (1b) and hence

$$\begin{aligned}\mathcal{S}(R \mid n) &= \sum_{j=0}^{k-1}\sum_{i=0}^{p^{m-a}-1} R^{i+jp^{m-a}} \equiv \sum_{j=0}^{k-1}\mathcal{S}\left(R \mid p^{m-a}\right)\\ &\equiv \begin{cases} k(2^{m-a}+2^{m-1}) \mod 2^m; & \text{if } p=2 \text{ and } m>a;\\ kp^{m-a} = n \mod p^m & \text{otherwise.}\end{cases}\end{aligned}$$

Suppose now that $n \equiv kp^{m-a} \mod p^m$ with $n > 0$. Then $n = (k_0 + p^a l)2^{m-a}$ with $0 < k_0 \equiv k \mod p^a$ and $l \geq 0$. Then

$$\mathcal{S}\left(R \mid n\right) \equiv \begin{cases} (k_0 + l2^a)(2^{m-a}) + 2^{m-1}) \equiv k(2^{m-a} + 2^{m-1}) \equiv n + k2^{m-1} \mod 2^m, & \text{if } p = 2; \\ (k_0 + lp^a)p^{m-a} \equiv kp^{m-a} \equiv n \mod p^m, & \text{otherwise.} \end{cases}$$

So we have the result.

(2a) Suppose that $R \equiv -1 \mod 4$. If $2 \nmid m$ then $R^m \equiv -1 \mod 4$ and hence $v_2(R^m - 1) = 1$. As $R^2 \equiv 1 \mod 4$, if $2 \mid m$ then, by (1a) we have $v_2(R^m - 1) = v_2((R^2)^{\frac{m}{2}} - 1) = v_2(R^2 - 1) + v_2\left(\frac{m}{2}\right) = v_2(R+1) + v_2(m)$. This proves the first part of (2a). Then the second part follows from $R^m - 1 = (R-1)\mathcal{S}\left(R \mid m\right)$.

(2b) follows easily from (2a).

(2c) Since R is odd, both $R^m - 1$ and $R^m + 1$ and are even and exactly one of $v_2(R^m - 1)$ and $v_2(R^m + 1)$ equals 1. Thus, from (2a) we deduce that if $2 \mid m$ then $v_2(R^m + 1) = 1$. Suppose otherwise that m is odd and greater than 2. Then $v_2(R^{m-1} - 1) = v_2(R+1) + v_2(m-1) > v_2(R+1)$, so that $v_2(R^m + 1) = v_2(R(R^{m-1} - 1 + 1) + 1) = v_2(R + 1 + R(R^{m-1} - 1)) = v_2(R+1)$.

□

1.2 Group theory

In this section we will continue establishing the notation of the document. By default all the groups in this paper are finite. We use standard notation for a group G, $g, h, g_1, \dots, g_n \in G$

and subsets A, B of G:

$\langle g_1, \dots, g_n \rangle =$ Subgroup of G generated by $g_1, \dots, g_n$.

$g^h = h^{-1}gh$, i. e. *conjugator* of g by h.

$[g, h] = g^{-1}g^h$, i. e. *conmutator* of g and h.

$g^G = \{g^h,$ for every $h \in H\}$, i. e. *conjugacy class* of g in G.

$\langle A \rangle =$ Subgroup of G generated by the elements in A.

$A^g = \{a^g$ for every $a \in A\}$.

$[A, B] = \{[a, b],$ for every $a \in A, b \in B\}$, *commutator* of A and B.

$G' =$ *Commutator subgroup* of G, this is: $[G, G]$.

$\mathcal{Z}(G) =$ *Center* of G, this is: $\{g \in G \mid gh = hg$ for every $h \in G\}$.

$\exp(G) =$ *Exponent* of G, this is, the smallest integer n such that $g^n = 1$ for every $g \in G$.

$\mathrm{Aut}(G) =$ *Automorphism group* of G.

$|g| =$ Order of g.

$H \leq G = H$ is a subgroup of G.

$N \trianglelefteq G = N$ is a normal subgroup of G.

$G \times H =$ Direct product of the groups G and H

$G \rtimes_m H =$ Semidirect product of the groups G and H with kernel of order m

$|A| =$ The cardinal of a set.

$\pi(A) = \pi(|A|)$.

Now, given $H \leq G$, we also fix the following notation regarding subgroups of a group:

$[G : H] =$ The index of H in G.

$N_G(H) =$ The largest subgroup of G in which H is normal.

$\mathrm{C}_G(H) =$ The largest subgroup of G in which H is central.

$\mathrm{Core}_G(H) =$ The largest subgroup of H that is normal in G.

Fix a prime p and g an element of a finite group G. Then, g can be uniquely written as $g = g_p g_{p'}$, where g_p, $g_{p'} \in \langle g \rangle$, $|g_p|$ is a power of p and $|g_{p'}|$ is a number coprime with p.

We call g_p the *p-part* of g and $g_{p'}$ the *p'-part* of g. When instead of a prime p we have a set of primes π, the definition is analogous and in this case we call g_π the *π-part* of g and $g_{\pi'}$ the *π'-part* of g. An important concept that requires its own definition is that of Hall subgroups.

Definition 1.2 (Hall Subgroup)**.** *Let G be a group and π a set of primes. A subgroup of G is a* Hall subgroup *if its order is coprime to its index. Additionally, a subgroup of G is a* Hall π-subgroup *if it is a Hall subgroup and its order is divisible only by the primes in π.*

In case G is a finite group having a unique Sylow p-subgroup, this will be denoted by G_p. In particular, this applies to each nilpotent group, because if G is a finite nilpotent group then the Sylow p-subgroups of G are unique [Rob82, 5.2.4]. If G has a unique Hall p'-subgroup then it will be denoted by $G_{p'}$. An important theorem about Hall subgroups is the following:

Theorem 1.3 (P. Hall, [Rob82, 9.1.7])**.** *Let π be a non-empty set of primes and G a finite solvable group. Then every π-subgroup of G is contained in a Hall π-subgroup of G. Moreover, all Hall π-subgroups of G are conjugate in G.*

The previous theorem will be used a lot in Chapter 2, mostly without mention.

The majority of the groups studied in this thesis are metacyclic. Let us proceed with the definition of metacyclic groups.

Definition 1.4 (Metacyclic)**.** *A group G is* metacyclic *if there exists $N \trianglelefteq G$ such that N and G/N are both cyclic.*

The second chapter will be dedicated to the classification of these groups. They will also be the main actors of the third and fourth chapters, as these will be dedicated to solving a research problem for finite metacyclic groups.

The following is a very important notation that will occur frequently in the following chapters:

$$\pi_G = \{p \in \pi(G) : G \text{ has a normal Hall } p'\text{-subgroup}\} \quad \text{and} \quad \pi'_G = \pi(G) \setminus \pi_G. \tag{1.3}$$

Observe that if $p \in \pi_G$, then G has a unique Hall p'-subgroup $G_{p'}$, and hence $G_{\pi'_G} = \cap_{p \in \pi_G} G_{p'}$ is the unique Hall π'-subgroup of G.

Let m be a positive integer. Then we have isomorphisms $\operatorname{Aut}(\mathbb{C}_m) \leftarrow \mathcal{U}_m \rightarrow \operatorname{Aut}(\mathbb{Q}_m)$ which associate $[t]_m \in \mathcal{U}_m$ with the automorphism of $\mathbb{C}_m$ given by $a \mapsto a^t$ and the automorphism of $\mathbb{Q}_m$ given by $\zeta_m \mapsto \zeta_m^t$. Sometimes we abuse the notation and identify elements of $\operatorname{Aut}(\mathbb{C}_m)$, $\mathcal{U}_m$ and $\operatorname{Aut}(\mathbb{Q}_m)$ via these isomorphisms. For example, if X is a subset of $\operatorname{Aut}(\mathbb{C}_m)$ or $\mathcal{U}_m$, then $(\mathbb{Q}_m)^X$ denotes the subfield of $\mathbb{Q}_m$ formed by the elements fixed by the images of the elements X in $\operatorname{Aut}(\mathbb{Q}_m)$.

Fix m a positive integer and let T be a subgroup of $\mathcal{U}_m$. Then we define $[T] = (r, \epsilon, k)$ with

$$\begin{array}{rcl} r & = & \text{greatest divisor of } m \text{ such that } \operatorname{Res}_{r_{2'}}(T) = 1 \text{ and } \operatorname{Res}_{r_2}(T) \subseteq \langle -1 \rangle_{r_2}\,; \\ \epsilon & = & \begin{cases} -1, & \text{if } \operatorname{Res}_{r_2}(T) \neq 1; \\ 1, & \text{otherwise.} \end{cases} \\ k & = & |\operatorname{Res}_{m_\nu}(T)|, \text{ with } \nu = \pi(m) \setminus \pi(r). \end{array}$$

If moreover, $n, s \in \mathbb{N}$ then we denote

$$[T, n, s] = m_\nu \prod_{p \in \pi(r)} m'_p$$

with m'_p defined for each $p \in \pi(r)$ as follows:

$$\begin{array}{l} \text{if } \epsilon^{p-1} = 1 \text{ then } m'_p = \min\left(m_p, k_p r_p, \max\left(r_p, s_p, r_p \dfrac{s_p k_p}{n_p}\right)\right); \\ \text{if } \epsilon = -1 \text{ then } m'_2 = \begin{cases} r_2, & \text{if either } k_2 \leq 2 \text{ or } m_2 \leq 2r_2; \\ \frac{m_2}{2}, & \text{if } 4 \leq k_2 < n_2, 4r_2 \leq m, \text{ and if } s_2 \leq n_2 r_2 \text{ then } s_2 = m_2 < n_2 r_2; \\ m_2, & \text{otherwise.} \end{cases} \end{array} \tag{1.4}$$

Let A be a cyclic group of order m. Then the map $\sigma_A : \mathcal{U}_m \rightarrow \operatorname{Aut}(A)$ associating $[r]_m$ with the map $a \mapsto a^r$, is a group isomorphism. If moreover A is a normal subgroup of a group G then we define

$$T_G(A) = \sigma_A^{-1}(\operatorname{Inn}_G(A)),$$

where $\mathrm{Inn}_G(A)$ is formed by the restriction to A of the inner automorphisms of G. We introduce notation for the entries of $T_G(A)$ by setting

$$(r^G(A), \epsilon^G(A), k^G(A)) = [T_G(A)].$$

Definition 1.5 (Metacyclic kernel, factorization, minimal)**.** *Let G be a group. A* metacyclic kernel *of G is a normal subgroup A of G such that A and G/A are cyclic. A* metacyclic factorization *of a group G is an expression $G = AB$ where A is a normal cyclic subgroup of G and B is a cyclic subgroup of G.*

A minimal kernel *of G is a kernel of G of minimal order.*

A metacyclic factorization $G = AB$ is said to be minimal *in G if $(|A|, r^G(A), [G : B])$ is minimal in the lexicographical order. In that case we denote $m^G = |A|$, $n^G = [G : A]$, $s^G = [G : B]$ and $r^G = r^G(A)$.*

Clearly a group is metacyclic if and only if it has a metacyclic kernel if and only if it has a metacyclic factorization. Sometimes we abbreviate metacyclic kernel of G or metacyclic factorization of G and we simply say kernel of G or factorization of G.

If $G = AB$ is a metacyclic factorization of G then we denote

$$\Delta(AB) = \mathrm{Res}_{[T,n,s]}(T), \quad \text{with} \quad T = T_G(A), \quad n = [G : A] \quad \text{and} \quad s = [G : B].$$

We will prove that $\Delta(AB)$ is constant for all the minimal metacyclic factorizations (Corollary 2.10). This allows us to define the desired invariant:

$$\mathrm{MCINV}(G) = (|A|, [G : A], [G : B], \Delta(AB)), \text{ with } G = AB \text{ minimal factorization of } G.$$

Our main result of Chapter 2 states that $\mathrm{MCINV}(G)$ determines G up to isomorphisms, A.

Another kind of groups that will appear in the document, albeit with less relevance, are metabelian groups.

Definition 1.6 (Metabelian)**.** *A group G is* metabelian *if there exists $N \trianglelefteq G$ such that*

N and G/N are both abelian.

Every metacyclic group is clearly metabelian, but the implication does not hold the other way around.

If G is a group, then a normal subgroup H of G is said to be *cocyclic* in G if G/H is cyclic. We close this section computing the cocyclic subgroups of a 2-generated abelian p-group. This will be used in Section 4.4.

Lemma 1.7. *Let $L = \langle g \rangle \times \langle h \rangle$ be a an abelian p-group with $|g| \geq |h|$ and let*

$$C_L = \left\{ (i,y,x) : i \in \{1,2\}, \quad 1 \leq x \leq y \quad \textit{and} \quad \begin{cases} y \mid |h|, & \textit{if } i=1; \\ y \mid |g|, p \mid x \textit{ and } p \mid y \mid |h|x, & \textit{if } i = 2 \end{cases} \right\}$$

Then

$$(i,y,x) \mapsto K_{i,y,x} = \begin{cases} \langle gh^x, h^y \rangle, & \textit{if } i = 1; \\ \langle g^x h, g^y \rangle, & \textit{if } i = 2; \end{cases}$$

defines a bijection from C_L to the set of cocyclic subgroups of L. Moreover, for every $(i,y,x) \in C_L$ we have

$$[L : K_{i,y,x}] = y, \quad \langle g \rangle \cap K_{i,y,x} = \begin{cases} \left\langle g^{\frac{y}{xp}} \right\rangle, & \textit{if } i = 1; \\ \langle g^y \rangle; & \textit{if } i = 2; \end{cases} \quad \textit{and} \quad \langle h \rangle \cap K_{i,y,x} = \begin{cases} \langle h^y \rangle, & \textit{if } i=1; \\ \left\langle h^{\frac{y}{xp}} \right\rangle; & \textit{if } i = 2. \end{cases}$$

Proof. Clearly, if $(i,y,x) \in C_L$, then $K_{i,y,x}$ is a cocyclic subgroup of L.

Let K be a cocyclic subgroup of L. Suppose that $K \not\subseteq \langle g^p, h \rangle$. Then K contains $\langle gh^z \rangle$ for some integer z. Moreover, $L = \langle gh^z \rangle \times \langle h \rangle$. Therefore $K = \langle gh^z, h^y \rangle = \langle gh^x, h^y \rangle = K_{1,y,x}$, with $y = [L : K] \mid |h|$ and x the unique integer in the interval $[1,y]$ such that $x \equiv z \mod y$. Moreover, $K_{1,y,x} = \langle gh^x \rangle \times \langle h^y \rangle$ and $K_{1,y,x} \cap \langle h \rangle = \langle h^y \rangle$. Let u be a positive integer. Then $g^u \in K_{1,y,x}$ if and only if there are integers a and b such that $g^u = g^a h^{ax+by}$. In that case, $u \equiv a \mod |g|$. As $y \mid |h|$ and $|h| \mid |g|$, it follows that $g^u \in K_{1,y,x}$ if and only if there is an integer b such that $|h| \mid xu + by$ if and only if $y \mid xu$ if and only if $\frac{y}{\gcd(x,y)} \mid u$ if and only if $\frac{y}{x_p} \mid u$. This shows that $\langle g \rangle \cap K_{1,y,x} = \left\langle g^{\frac{y}{x_p}} \right\rangle$.

Suppose otherwise that $K \subseteq \langle g^p, h \rangle$. Then $K \cap \langle g \rangle = \langle g^y \rangle$ for some y with $p \mid y$ and $y \mid |g|$, and K contains $\langle g^x h \rangle$ for some integer x with $p \leq x \leq y$ and $p \mid x$. Then

$L = \langle g^x h, g \rangle$ and $|g \langle g^x h, g^y \rangle| = y$ and hence $K = \left\langle g^x h, g^y, g^\delta \right\rangle$ for some $\delta \mid y$. However, as $K \cap \langle g \rangle = \langle g^y \rangle$ it follows that $K = \langle g^x h, g^y \rangle$. As $g^{x|h|} \in \langle g \rangle \cap K = \langle g^y \rangle$, $y \mid x|h|$. Thus $(2, y, x) \in C_L$ and $K = K_{2,y,x}$. Furthermore, $[L : K] = [\langle g \rangle : K \cap \langle g \rangle] = [\langle g \rangle, \langle g^y \rangle] = y$, since $L = \langle K, g \rangle$. Conversely, suppose that $(2, y, x) \in C_L$ Let u be a positive integer. Then $g^u \in K_{2,y,x}$ if and only if $g^u = g^{ax+by}h^a$ for some integers a and b. In that case $|h| \mid a$ and hence $y \mid ax$ because $y \mid x|h|$. Moreover $u \equiv ax + by \mod |g|$ and as $y \mid |g|$ we have that $y \mid u$. Therefore $\langle g \rangle \cap K_{2,y,x} = \langle g^y \rangle$. Finally, $h^u \in K_{2,y,x}$ if and only if there are integers a and b with $h^u = g^{ax+by}h^a$. Then $a = u + c|h|$ for some integer c and $ux + xc|h| + by \equiv 0 \mod |g|$. As $y \mid |g|$ and $y \mid x|h|$ we deduce that $y \mid ux$. Thus $\langle h \rangle \cap K_{2,y,x} \subseteq \left\langle h^{\frac{y}{xp}} \right\rangle$ and as $h^{\frac{y}{xp}} = (g^x h)^{\frac{y}{xp}} (g^y)^{-\frac{x}{xp}} \in K_{2,y,x}$, we conclude that $\langle h \rangle \cap K_{2,y,x} = \left\langle h^{\frac{y}{xp}} \right\rangle$.

Let $(i_1, y_1, x_1), (i_2, y_2, x_2) \in C_L$ with $K_{i_1,y_1,x_1} = K_{i_2,y_2,x_2}$. It remains to prove that $(i_1, y_1, x_1) = (i_2, y_2, x_2)$. First of all $i_1 = i_2$, as $K_{1,y_1,x_1} \not\subseteq \langle g^p, h \rangle$ and $K_{2,y_2,x_2} \subseteq \langle g^p, h \rangle$. Suppose that $i_1 = i_2 = 1$. Then $\langle h^{y_1} \rangle = K_{1,y_1,x_1} \cap \langle h \rangle = K_{1,y_2,x_2} \cap \langle h \rangle = \langle h^{y_2} \rangle$ and therefore $y_1 = y_2$. Moreover, $gh^{x_1} = (gh^{x_2})^a (h^{y_2})^b = g^a h^{ax_2+by}$ for some integers a and b. Then $a \equiv 1 \mod |g|$ and, as $|h| \mid |g|$ and $y \mid |h|$, we have that $x_1 \equiv x_2 \mod y_1$. Then $x_1 = x_2$, as $1 \leq x_1, x_2 \leq y_1 = y_2$. Suppose that $i_2 = 2$. Since $y_1, y_2 \mid |g|$ and $\langle g^{y_1} \rangle = K_{2,y_1,x_1} \cap \langle g \rangle = K_{2,y_2,x_2} \cap \langle g \rangle = \langle g^{y_2} \rangle$, we have $y_1 = y_2$. Moreover, $g^{x_1}h = (g^{x_2}h)^a (g^{y_2})^b = g^{ax_2+by_2}h^a$ for some integers a and b. Then $a = 1 + c|h|$ for some integer c and as $y_2 \mid x_2|h|$ and $y \mid |g|$, it follows that $x_1 \equiv ax_2 = x_2 + cx_2|h| \equiv x_2 \mod y_2$. Thus $x_1 = x_2$. □

1.3 Group Rings and the Isomorphism Problem

The concept of *group ring* appeared implicitly in an article by A. Cayley [Cay54] in 1854, which is considered the first work in abstract Group Theory. In its article, Cayley exposed a formal construction of the group ring $\mathbb{C}S_3$ which is essentially the same that is studied nowadays. In 1892, group rings appeared again in an article by T. Molien [Mol92] about complex algebras, in which he introduced the notions of simple and semisimple algebras. In a later article [Mol97], Molien obtained important results in the Theory of Complex Representations of Finite Groups, including the orthogonality relations for group characters. The link between Representation Theory of Groups and Theory of Algebras (which is obtained through group algebras) was vastly recognised after an important article by E. Noether [Noe29], some works with R. Brauer [BN27] and an article by Brauer [Bra29]. The study of group rings by themselves followed soon, after the inclusion of questions about group rings in a famous list of problems in Ring Theory of I. Kaplansky ([Kap57], [Kap70]). The first book dedicated exclusively to group rings was written by D. Passman and published in 1977 [Pas77].

After giving a small historic introduction to group rings, it is time to give a proper definition:

Definition 1.8 (Group Ring)**.** *Given G a group and R a ring, the group ring of G over R is the ring RG of all linear combinations of the form*

$$\sum_{g\in G} a_g g,$$

where $a_G \in R$ and for almost all $g \in G$, $a_g = 0$. The sum in this ring is defined component-wise

$$\sum_{g\in G} a_g g = \sum_{g\in G} b_g g = \sum_{g\in G} (a_g + b_g) g,$$

and the product is given by

$$\left(\sum_{g\in G} a_g g\right) \cdot \left(\sum_{g\in G} b_g g\right) = \sum_{g\in G} \left(\sum_{h_1 h_2 = g} a_{h_1} b_{h_2}\right) g.$$

The identity of this ring is the element $1_R 1_G$, where 1_R is the identity of R and 1_G the identity of G. When we work with RG, we will denote $1_R 1_G$ as 1, as usual. If R is a field, we will sometimes call RG the group algebra of G over R.

The following theorem provides the necessary and sufficient conditions on R and G for the group ring RG to be semisimple (see [PMS02, Theorem 3.4.7]).

Theorem 1.9 (Maschke)**.** *Given a ring R and a group G, the group ring RG is semisimple if and only if R is a semisimple ring, G is finite and $|G|$ is a unit in R.*

In particular, if G is a finite group and F is a field, then FG is semisimple if and only if the characteristic of F does not divide $|G|$. In particular, $\mathbb{Q}G$ is semisimple for every finite group G.

Theorem 1.10 (Artin-Wedderburn). *Let R be a semisimple ring. Then*

$$R \cong \bigoplus_{i=1}^{r} M_{n_i}(D_i), \text{ with each } D_i \text{ a division rings.}$$

In this formula, r is the number of simple R-modules and n_i and D_i are determined by R up to isomorphism.

As $\mathbb{Q}G$ is semisimple for every finite group G, that means that we can apply the previous theorem to obtain a decomposition of $\mathbb{Q}G$ into a sum of matrices of division rings. We will call this decomposition the *Wedderburn decomposition* of $\mathbb{Q}G$, and we will use it frequently along the thesis. In the next section we will see what is the structure of each simple component for our case.

The problem that we are trying to solve is the Isomorphism Problem for group algebras. This problem asks whether we can obtain an isomorphism of groups from an isomorphism from group algebras over the same groups. We can write this as follows.

$$RG \cong RH \quad \overset{?}{\Rightarrow} \quad G \cong H \tag{1.5}$$

We look for answers when $R = \mathbb{Q}$ and G metacyclic. The third and fourth chapters are all about solving this problem for metacyclic groups. Now we recall two results relevant for the Isomorphism Problem for rational group algebras. The first one is a well known result of Artin which tell us what is the number of Wedderburn components of a rational group algebra. See [CR62, Corollary 39.5] or [JdR16, Corollary 7.1.12]

Theorem 1.11 (Artin). *If G is a finite group then the number of Wedderburn components of $\mathbb{Q}G$ is the number of conjugacy classes of cyclic subgroups of G.*

The second one is a consequence of the Perlis-Walker Theorem. Let us first state this Theorem:

Theorem 1.12 (Perlis-Walker[PW50]). *Let G be a finite abelian group. Then the group ring $\mathbb{Q}G$ determines G up to isomorphism.*

In the same article [PW50], Perlis and Walker proved that given an abelian group G, the group algebra $\mathbb{C}G$ is isomorphic to $|G|$ copies of $\mathbb{C}$. The result is more general than that, but this statement is enough to give easy counterexamples to the Equation (1.5) for $R = \mathbb{C}$:

Example 1.13. *Consider the groups $\mathcal{C}_4$ and $\mathcal{C}_2 \times \mathcal{C}_2$. This groups are obviously not isomorphic, but using Perlis-Walker's Theorem we find:*

$$\mathbb{C}\mathcal{C}_4 \cong \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \cong \mathbb{C}\left(\mathcal{C}_2 \times \mathcal{C}_2\right)$$

The following result is a consequence of Theorem 1.12 that will be used to get information of the group from the rational group algebra.

Theorem 1.14. *If G and H are finite groups with $\mathbb{Q}G \cong \mathbb{Q}H$ then $G/G' \cong H/H'$.*

Proof. Let $A(G)$ denote the kernel of the natural homomorphism $\mathbb{Q}G \to \mathbb{Q}(G/G')$. Then $A(G)$ is a the smallest ideal I of $\mathbb{Q}G$ such that $(\mathbb{Q}G)/I$ is commutative. In particular, if $f : \mathbb{Q}G \to \mathbb{Q}H$ is an isomorphism then $f(A(G)) = A(H)$ and therefore f induces an isomorphism $\mathbb{Q}(G/G') \cong \mathbb{Q}(H/H')$. Then $G/G' \cong H/H'$ by the Perlis-Walker Theorem [PW50]. □

1.4 Wedderburn decomposition of rational group algebras

In this section we are going to explain the structure of $\mathbb{Q}G$ in the case where G is metacyclic. To do this we need to introduce some more notation and concepts of Theory of Algebras. Most of the contents of this section are taken from the books [Pie82] and [JdR16] and the article [OdRS04].

Definition 1.15 (Degree). *If F is a field and A is a finite dimensional central simple F-algebra, then $\operatorname{Deg}(A)$ denotes the degree of A, i.e. $\dim_F A = \operatorname{Deg}(A)^2$ (cf. [Pie82]).*

Let F/K be a finite Galois field extension and let $G = \operatorname{Gal}(F/K)$. Let $\mathcal{U}(F)$ denote the multiplicative group of F. If $f : G \times G \to \mathcal{U}(F)$ is a 2-cocycle, then $(F/K, f)$ denotes the crossed product

$$(F/K,f)=\sum_{\sigma\in G}t_\sigma F,\quad xt_\sigma=t_\sigma\sigma(x),\quad t_\sigma t_\tau=t_{uv}f(u,v),\quad (x\in F,\sigma,\tau\in G).$$

Suppose that G is cyclic of order n and generated by σ and let $a\in\mathcal{U}(K)$. Then there is a cocycle $f:G\times G\to\mathcal{U}(K)$ given by

$$f(\sigma^i,\sigma^j)=\begin{cases}1, & \text{if } 0\le i,j,i+j<n;\\ a, & \text{if } 0\le i,j<n\le i+j;\end{cases}$$

and the crossed product algebra $(F/K,f)$ is said to be a *cyclic algebra*. This algebra is usually denoted $(F/K,\sigma,a)$, and it can be described as follows:

$$(F/K,\sigma,a)=\sum_{i=0}^{n-1}u^iF=F[u\mid xu=u\sigma(x),u^n=a]$$

If A is a semisimple ring, then A is a direct sum of central simple algebras, such expression of A is called the *Wedderburn decomposition* of A and its simple factors are called the *Wedderburn components* of A. The Wedderburn components of A are the direct summands of the form Ae with e a primitive central idempotent of A.

Let G be a finite group. By Maschke's Theorem (1.9), $\mathbb{Q}G$ is semisimple and the center of each Wedderburn component A of $\mathbb{Q}G$ is isomorphic to the field of character values $\mathbb{Q}(\chi)=\mathbb{Q}\left(\chi(g):g\in G\right)$ of any irreducible character χ of G satisfying $\chi(A)\neq 0$. It is well known that $\mathbb{Q}(\chi)$ is a finite abelian extension of $\mathbb{Q}$ inside $\mathbb{C}$ and henceforth it is the unique subfield of $\mathbb{C}$ isomorphic to $\mathbb{Q}(\chi)$. Sometimes we will abuse the notation and consider $Z(A)$ as equal to $\mathbb{Q}(\chi)$.

An important tool for us is a technique introduced in [OdRS04] to describe the Wedderburn decomposition of $\mathbb{Q}G$ for G a metabelian group. See also [JdR16, Section 3.5]. Let us go over the main ingredients.

If H is a subgroup of G, then denote $\widehat{H}=|H|^{-1}\sum_{h\in H}h$, as an element in $\mathbb{Q}G$. It is clear that $\widehat{H}$ is an idempotent of $\mathbb{Q}G$ and it is central in $\mathbb{Q}G$ if and only if H is normal in G.

If $N\trianglelefteq G$ then we denote

$$\varepsilon(G,N)=\begin{cases}\widehat{G}, & \text{if } G=N;\\ \prod_{D/N\in M(G/N)}(\widehat{N}-\widehat{D}), & \text{otherwise.}\end{cases}$$

where $M(G/N)$ denotes the set of minimal normal subgroups of G/N. Clearly $\varepsilon(G,N)$ is a central idempotent of $\mathbb{Q}G$.

If (L,K) is a pair of subgroups of G with $K \trianglelefteq L$, then we denote

$$e(G,L,K) = \sum_{gC_G(\varepsilon(L,K)) \in G/C_G(\varepsilon(L,K))} \varepsilon(L,K)^g.$$

Then $e(G,L,K)$ belongs to the center of $\mathbb{Q}G$. If moreover, $\varepsilon(L,K)^g\varepsilon(L,K) = 0$ for every $g \in G \setminus C_G(\varepsilon(L,K))$, then $e(G,L,K)$ is an idempotent of $\mathbb{Q}G$.

An important concept that will be used a lot in this thesis is the following:

Definition 1.16 (SSP)**.** *A* strong Shoda pair *of G is a pair (L,K) of subgroups of G satisfying the following conditions:*

(SS1) $K \subseteq L \trianglelefteq N_G(K)$*,*

(SS2) L/K *is cyclic and maximal abelian in* $N_G(K)/K$*,*

(SS3) $\varepsilon(L,K)^g\varepsilon(L,K)$ *for every* $g \in G \setminus C_G(\varepsilon(L,K))$*.*

We can now give the following construction, which illustrate the correspondence between strong Shoda pairs and Wedderburn components.

Remark 1.17. *Suppose that (H,K) is a strong Shoda pair of G and let $m = [H:K]$ and $N = N_G(K)$. Then $H/K \cong C_m$ and the action of N by conjugation on H induces a faithful action of N/H on $\mathbb{Q}(\zeta_m)$. More precisely, if $n \in N$ then $h^nK = \alpha_r(hK)$ for some integer r, with $\gcd(r,m) = 1$. The map $nH \to \sigma_r$ defines an injective homomorphism $\alpha : N/H \to \mathrm{Aut}(\mathbb{Q}(\zeta_m))$. Let $F_{G,H,K} = \mathbb{Q}(\zeta_m)^{\mathrm{Im}\,\alpha}$. Then we have a short exact sequence [JdR16, Theorem 3.5.5]:*

$$1 \to H/K \cong \langle\zeta_m\rangle \to N/K \to N/H \cong \mathrm{Gal}(\mathbb{Q}(\zeta_m)/F_{G,H,K}) \to 1$$

which induces an element $\overline{f} \in H^2(N/H, \mathbb{Q}(\zeta_m))$. More precisely from an election of a set of representatives $\{c_u : u \in N/H\}$ of H cosets in N, we define $f(u,v) = \zeta_m^k$ if $c_uc_v = c_{uv}h^k$. This defines an element of $H^2(N/H, \mathbb{Q}(\zeta_m))$ because another election yields to another 2-cocycle differing in a 2-coboundary. Associated to $\overline{f}$ one has the *crossed product algebra*

$$A(G,H,K) = (\mathbb{Q}(\zeta_m)/F_{G,H,K}, \overline{f}) = \oplus_{u\in N/H} t_u \mathbb{Q}(\zeta_m),$$
$$x t_u = t_u \sigma_u(x), \quad t_u t_v = t_{uv} f(u,v), \quad (x \in \mathbb{Q}(\zeta_m), u, v \in N/K).$$

Proposition 1.18. *[OdRS04, Proposition 3.4] [JdR16, Theorem 3.5.5] Let (L,K) be a strong Shoda pair of G and let $N = N_G(K)$, $m = [L : K]$, $n = [G : N]$ and $e = e(G,L,K)$. Then e is a primitive central idempotent of $\mathbb{Q}G$ and $\mathbb{Q}Ge \cong M_n(A(N,L,K))$. Moreover, $\mathrm{Deg}(\mathbb{Q}Ge) = [G : L]$, $Z(\mathbb{Q}Ge(G,L,K)) \cong F_{N,L,K}$ and $\{g \in G : ge = e\} = \mathrm{Core}_G(K)$.*

In the particular case where G is metabelian all the Wedderburn components of $\mathbb{Q}G$ are of the form $A(N,L,K)$ for some special kind of strong Shoda pairs of G. More precisely:

Theorem 1.19. *[OdRS04, Theorem 4.7] [JdR16, Theorem 3.5.12] Let G be a finite metabelian group and let A be a maximal abelian subgroup of G containing G'. Then every Wedderburn component of $\mathbb{Q}G$ is of the form $\mathbb{Q}Ge(G,L,K)$ for subgroups L and K satisfying the following conditions:*

(1) L is a maximal element in the set $\{B \leq G : A \leq B$ and $B' \leq K \leq B\}$.

(2) L/K is cyclic.

Moreover every pair (L,K) satisfying (1) and (2) is a strong Shoda pair of G and hence $\mathbb{Q}Ge(G,L,K) \cong M_n(A(N,L,K))$ with $N = N_G(K)$ and $n = [G : N]$.

Suppose that G is a finite metacyclic group and $G = AB$ is a metacyclic factorization of G. Then every Wedderburn component of $\mathbb{Q}G$ is of the form $\mathbb{Q}Ge(G,L,K)$ for L and K subgroups of G with $A \subseteq L$ and satisfying the conditions of Theorem 1.19. Then $L = \langle a, b^d \rangle$, $N = N_G(K) = \langle a, b^n \rangle$ where $[G : N] = n \mid d \mid [G : A]$. Moreover, L/K is cyclic, say generated by uK, and normal in N/K so that $(uK)^{b^n K} = u^x K$ and $(uK)^{\frac{d}{n}} = a^y$ for some integers x and y. By Proposition 1.18,

$$A(N,L,K) \cong (\mathbb{Q}_m/F, \sigma_x, \zeta_m^y) = \mathbb{Q}_m[\overline{u} \mid \zeta_m \overline{u} = \overline{u}\zeta_m^x, \overline{u}^k = \zeta_m^y], \tag{1.6}$$

where $m = [L : K]$ and σ_x is the automorphism of $\mathbb{Q}_m$ given $\sigma_x(\zeta_m) = \zeta_m^x$.

CHAPTER 2

Finite Metacyclic Groups

Over the course of this chapter we will explore metacyclic groups and their classification. The main results are collected in Theorem A, Theorem B and Theorem C. The contents of this chapter are compiled in [GBdR23a].

In Section 2.1 we introduce the main theorems to prove and their consequences. In Section 2.2 we prove several lemmas on metacyclic factorizations aiming to an intrinsic description of when a metacyclic factorization is minimal. It includes an algorithm to obtain a minimal metacyclic factorization from an arbitrary one. This section concludes with Theorem 2.9 which is the keystone to prove Theorem A, Theorem B and Theorem C in Section 2.3. In Section 2.4 we introduce an algorithm to compute the metacyclic invariants of a given metacyclic group and use this to decide if two metacyclic groups are isomorphic, and another algorithm to construct all the metacyclic groups of a given order. We present also implementations in GAP [GAP12] of these algorithms.

2.1 Introduction

It is well known that every finite metacyclic group has a presentation of the following form

$$\mathcal{G}_{m,n,s,t} = \left\langle a, b \mid a^m = 1, b^n = a^s, a^b = a^t \right\rangle$$

for $m, n, s, t \in \mathbb{N}$ satisfying $s(t-1) \equiv t^n - 1 \equiv 0 \mod m$. However, the parameters m, n, s and t are not invariants of the group. Traditionally, the authors that deal with the classification of finite metacyclic group select distinguished values of m, n, s and t so that each isomorphism class is described by a unique election of the parameters (see [Zas99, Hal59, Bey72, Kin73, Lie96, Lie94, NX88, Réd89, Lin71, Sim94]). This approach was culminated by C.E. Hempel who presented a classification of all the finite metacyclic groups in [Hem00]. However it is not clear how to use this classification to describe the distinguished parameters identifying a given metacyclic group and how those distinguished parameters are connected with group invariants.

In [GBdR23a], we presented an alternative classification of the finite metacyclic using a slightly different approach in terms of group invariants which allows an easy implementation. We associate to every finite metacyclic group G a 4-tuple $\mathrm{MCINV}(G) = (m^G, n^G, s^G, \Delta^G)$ where m^G, n^G and s^G play the role of m, n and s in the presentation above and Δ^G is a cyclic subgroup of units modulo a divisor of m^G, such that any generator of this subgroup can play the role of t. Our main result consists in proving that $\mathrm{MCINV}(G)$ is an invariant of the group G which determines G up to isomorphism, i.e. if G and H are two finite metacyclic groups then they are isomorphic if and only if $\mathrm{MCINV}(G) = \mathrm{MCINV}(H)$ (Theorem A). Moreover, we describe in Theorem B the possible values (m, n, s, Δ) of $\mathrm{MCINV}(G)$ and for such value we show how to find an integer t such that $\mathrm{MCINV}(\mathcal{G}_{m,n,s,t}) = (m, n, s, \Delta)$ (Theorem C). This allows a computer implementation of the following function: one which computes $\mathrm{MCINV}(G)$ for any given finite metacyclic group, and hence of another function which decide whether two metacyclic groups are isomorphic, and another one which computes all the metacyclic subgroups of a given order. This classification will be important in Chapter 4, where we will need it to prove Theorem F.

Theorem A. *Two finite metacyclic groups G and H are isomorphic if and only if $\mathrm{MCINV}(G) = \mathrm{MCINV}(H)$.*

Our next result describes the values realized as $\mathrm{MCINV}(G)$ with G a finite metacyclic group. In the remainder of the section we use the notation in Theorem B.

Theorem B. *Let $m, n, s \in \mathbb{N}$ and let Δ be a cyclic subgroup of $\mathcal{U}_{m'}$ with $m' \mid m$. Let $[\Delta] = (r, \epsilon, k)$ and $\nu = \pi(m) \setminus \pi(r)$. Then the following conditions are equivalent:*

(1) $(m, n, s, \Delta) = \mathrm{MCINV}(G)$ *for some finite metacyclic group* G*.*

(2) *(a)* s *divides* m*,* $|\Delta|$ *divides* n *and* $m_\nu = s_\nu = m'_\nu$*.*

(b) (1.4) *holds for every* $p \in \pi(r)$*.*

(c) *If* $\epsilon = -1$ *then* $\frac{m_2}{r_2} \le n_2$*,* $m_2 \le 2s_2$ *and* $s_2 \ne n_2 r_2$*. If moreover* $4 \mid n$*,* $8 \mid m$ *and* $k_2 < n_2$ *then* $r_2 \le s_2$*.*

(d) *For every* $p \in \pi(r)$ *with* $\epsilon^{p-1} = 1$*, we have* $\frac{m_p}{r_p} \le s_p \le n_p$ *and if* $r_p > s_p$ *then* $n_p < s_p k_p$*;*

Our last result shows how to construct a metacyclic group G with given $\mathrm{MCINV}(G)$: If $m, n, s \in \mathbb{N}$ with $s \mid m$ then we define the following subgroup of $\mathcal{U}_m$:

$$\mathcal{U}_m^{n,s} = \{[t]_m : m \mid s(t-1) \quad \text{and} \quad t^n \equiv 1 \mod m\}.$$

If T is a cyclic subgroup of $\mathcal{U}_m^{n,s}$ generated by $[t]_m$ then we denote

$$\mathcal{G}_{m,n,s,T} = \mathcal{G}_{m,n,s,t} = \{a, b : a^m = 1, b^n = a^s, a^b = a^t\}.$$

It is easy to see that the isomorphism type of this group is independent of the election of the generator $[t]_m$ of T (Lemma 2.2.(5)). Moreover, the assumption $T \subseteq \mathcal{U}_m^{n,s}$ warranties that $|a| = m$, $|\mathcal{G}_{m,n,s,T}| = mn$ and $|b| = \frac{mn}{s}$.

Remark 2.1. *Suppose that* m, n, s *and* $\Delta \le \mathcal{U}_{m'}$ *satisfy the conditions of statement (2) in Theorem B and* $[\Delta] = (r, \epsilon, k)$*. Then* $\mathrm{Res}_{m'_p}(\Delta) = \langle \epsilon^{p-1} + r_p \rangle_{m'_p}$ *for every* $p \in \pi(r)$ *and hence there is an integer* t' *such that* $\Delta = \langle t' \rangle_{m'}$ *and* $t' \equiv \epsilon^{p-1} + r_p \mod m'_p$ *for every* $p \in \pi(r)$*. Using the Chinese Remainder Theorem we can select an integer* t *such that* $t \equiv t' \mod m'$ *and* $t \equiv \epsilon^{p-1} + r_p \mod m_p$ *for every* $p \in \pi(r)$ *and let* $T = \langle t \rangle_m$*. Then* $T \subseteq \mathcal{U}_n^{n,s}$*,* $\mathrm{Res}_{m'}(T) = \Delta$ *and* $[T] = [\Delta]$*. Then the following theorem ensures that* $\mathrm{MCINV}(G_{m,n,s,T}) = (m, n, s, \Delta)$*.*

Theorem C. *Let $m, n, s \in \mathbb{N}$ and let Δ be a cyclic subgroup of $\mathcal{U}_{m'}$ with $m' \mid m$. Suppose that they satisfy the conditions of (2) in Theorem B and let T be a cyclic subgroup of $\mathcal{U}_m^{n,s}$ such that $[T] = [\Delta]$ and $\mathrm{Res}_{m'}(T) = \Delta$. Then $(m, n, s, \Delta) = \mathrm{MCINV}(\mathcal{G}_{m,n,s,T})$.*

For implementation it is convenient to replace the fourth entry of $\mathrm{MCINV}(G)$ by a distinguished integer t^G so that $G \cong \mathcal{G}_{m^G,n^G,s^G,t^G}$ and $G \cong H$ if and only if $(m^G, n^G, s^G, t^G) = (m^H, n^H, s^H, t^H)$. We select t^G satisfying the conditions of Remark 2.1. In particular, $[t^G]_{m_\pi}$ is uniquely determined by the condition $t \equiv \epsilon^{p-1} + r_p \mod m_p$ for every $p \in \pi(r)$. However there is not any natural election of $[t^G]_{m_{\pi'}}$ so when it comes to the implementation we will simply take the minimum possible value. More precisely, if $(m, n, s, \Delta) = \mathrm{MCINV}(G)$, $(r, \epsilon, k) = [\Delta]$ and m' is given by (1.4) then define

$$t^G = \min\{t \geq 0 : \mathrm{Res}_{m'}(\langle t\rangle_m) = \Delta \quad \text{and} \quad t \equiv \epsilon^{p-1} + r_p \mod m_p \text{ for every } p \in \pi(r)\}.$$

We call (m^G, n^G, s^G, t^G) the list of *metacyclic invariants* of G. Clearly if H is another metacyclic group then $G \cong H$ if and only if G and H have the same metacyclic invariants. Moreover, by Theorem C, if (m, n, s, t) is the list of metacyclic invariants of G then $G \cong \mathcal{G}_{m,n,s,t}$.

Let G be a metacyclic group. Observe that A is a kernel of G if and only if G has a metacyclic factorization of the form $G = AB$. In that case, if

$$m = |A|, \quad n = [G : A], \quad s = [G : B] \quad \text{and} \quad T = T_G(A) = \langle t\rangle_m,$$

then $s \mid m$, $|B| = n\frac{m}{s}$, $T \subseteq \mathcal{U}_m^{n,s}$ and A and B have generators a and b, respectively, such that $b^n = a^s$ and $a^b = a^t$. Thus $G \cong \mathcal{G}_{m,n,s,T}$.

The following lemma follows by straightforward arguments.

Lemma 2.2. *Let $m, n, s \in \mathbb{N}$, let T be a cyclic subgroup of $\mathcal{U}_m$, and denote $(r, \epsilon, k) = [T]$, $m' = [T, n, s]$ and $\Delta = \mathrm{Res}_{m'}(T)$.*

(1) If $T = \langle t\rangle_m$ then $|T| = o_m(t)$, $r_{2'} = \gcd(m_{2'}, t-1)$, $r_2 = \max(\gcd(m_2, t-1), \gcd(m_2, t+1)) = \gcd(m_2, t-\epsilon)$ and $k = o_{m_\nu}(t)$ with $\nu = \pi(m) \setminus \pi(r)$.

(2) $r \mid m' \mid m$ and $\pi(m) = \pi(m')$.

(3) $[T] = [\Delta]$.

(4) For every $p \in \pi(r)$ *we have* $\operatorname{Res}_{m_p}(T_p) = \langle \epsilon^{p-1} + r_p \rangle_{m_p}$ *and*

$$|\operatorname{Res}_{m_p}(T_p)| = \begin{cases} 2, & \text{if } p = 2, \epsilon = -1 \text{ and } r_2 = m_2; \\ \frac{m_p}{r_p}, & \text{otherwise.} \end{cases}$$

(5) If $s \mid m$ *and* $T \subseteq \mathcal{U}_m^{n,s}$ *then* $m_{\pi(r)} \mid rn$, $m_{\pi(r)} \mid rs$, $k \mid n_{\pi(m)\setminus\pi(r)}$ *and if* $\epsilon = -1$ *then* $m_2 \in \{s_2, 2s_2\}$. *If moreover* $T = \langle t \rangle_m = \langle u \rangle_m$ *then there is a* $k \in \mathbb{N}$ *with* $\gcd(k, |T|) = 1$ *and* $a \mapsto a^k$, $b \mapsto b^k$ *defines an isomorphism* $\mathcal{G}_{m,n,s,t} \to \mathcal{G}_{m,n,s,u}$.

The following property is related to that of being a minimal metacyclic factorization. We will see this in detail in Proposition 2.7.

Definition 2.3. *Given* $m, n, s \in \mathbb{N}$ *with* $s \mid m$ *and a cyclic subgroup of* $\mathcal{U}_m$, *we say that* T *is* (n, s)-canonical *if* $T \subseteq \mathcal{U}_m^{n,s}$ *and if* $(r, \epsilon, k) = [T]$ *then the following conditions are satisfied:*

(Can−) If $\epsilon = -1$ *then* $s_2 \neq r_2 n_2$. *If moreover,* $m_2 \geq 8$, $n_2 \geq 4$, $k_2 < n_2$ *then* $r_2 \leq s_2$.

(Can+) For every $p \in \pi$ *with* $\epsilon^{p-1} = 1$ *we have* $s_p \mid n$ *and* $r_p \mid s$ *or* $s_p k_p \nmid n$.

2.2 Metacyclic factorizations

In this section G is a finite metacyclic group. Moreover we fix the following notation:

$$\begin{aligned} \pi &= \pi_G \\ \pi' &= \pi'_G \\ k^G &= |\operatorname{Inn}_G(G'_{\pi'})|. \end{aligned}$$

In our first lemma we show that π, π' and k^G are determined by any kernel of G.

Lemma 2.4. *Let* $G = AB$ *be a metacyclic factorization and let* $m = |A|$, $s = [G : A]$, $r = r^G(A)$ *and* $k = k^G(A)$ *(see Chapter 1, Section 1.2). Then*

(1) For every set of primes μ, $A_\mu B_\mu$ is a Hall μ-subgroup of G.

(2) $p \in \pi'$ if and only if $G' \setminus Z(G)$ has an element of order p if and only if $A \setminus Z(G)$ has an element of order p.

(3) ${G'}_{\pi'} = A_{\pi'}$ and $A_{\pi'} \cap B_{\pi'} = 1$.

(4) $\pi' = \pi(m) \setminus \pi(r)$, $s_{\pi'} = m_{\pi'}$ and $k = k^G$.

(5) $G = A_{\pi'} \rtimes \left(B_{\pi'} \times \prod_{p\in\pi} A_p B_p\right)$. In particular $[B_{p'}, A_p] = 1$ for every $p \in \pi$.

Proof. (1) As A is normal in G, $A_\mu B_\mu$ is a μ-subgroup of G and $A_{\mu'} B_{\mu'}$ is a μ'-subgroup of G. Moreover $G = AB = A_\mu B_\mu A_{\mu'} B_{\mu'}$ and hence $[G : A_\mu B_\mu] = |A_{\mu'} B_{\mu'}|$. Thus $A_\mu B_\mu$ is a Hall μ-subgroup of G.

(2) As G/A is abelian, $G' \subseteq A$. Let $p \in \pi(|G|)$. If $p \nmid m$ then $AB_{p'}$ is a normal Hall p'-subgroup of G and hence $p \in \pi$. Suppose otherwise that $p \mid m$ and let C be the unique subgroup of order p in A. Since C is normal in G, it follows that $G' \setminus Z(G)$ has an element of order p if and only if $A \setminus Z(G)$ has an element of order p if and only if $C \not\subseteq Z(G)$. Since $\text{Aut}(C)$ is cyclic of order $p-1$, if $p \in \pi$ and N is a normal Hall p'-subgroup of G then $G = N \rtimes P$ with P a Sylow p-subgroup of G containing C and as $[P, C] = 1$ it follows that $[G, C] \subseteq [N, C] \subseteq N \cap C = 1$ and hence $C \subseteq Z(G)$. Conversely, if $C \subseteq Z(G)$ then $[A_p, A_{p'} B_{p'}] = 1$ because the kernel of the restriction homomorphism $\text{Aut}(A_p) \to \text{Aut}(C)$ is a p-group. As $A_{p'} B$ normalizes $A_{p'} B_{p'}$ it follows that the latter is a normal Hall p'-subgroup of G and hence $p \in \pi$.

(3) Let $p \in \pi'$, c an element of order p in A and a a generator of A. Since $|\text{Aut}(\langle c \rangle)| = p-1$ and $c \notin Z(G)$, we have that $a_p^b = a_p^o$ for some integer o such that $\gcd(o, p) = 1$. Moreover, $o-1$ is coprime with p because $1 \neq [c, b] = c^{o-1}$. Then $A_p = \left\langle a_p^{o-1} \right\rangle \subseteq G'$ and hence $A_p = {G'}_p$. Moreover, if $g \in A_p \cap B_p \setminus \{1\}$ then $[g, B] = 1$ and $c \in \langle g \rangle$, yielding a contradiction. Thus $A_p \cap B_p = 1$. Since this is true for each $p \in \pi'$, we have $A_{\pi'} = {G'}_{\pi'}$ and $A_{\pi'} \cap B_{\pi'} = 1$.

(4) is a direct consequence of (2) and (3).

(5) By (1) and (3), $A_{\pi'} B_{\pi'} = A_{\pi'} \rtimes B_{\pi'}$ is the unique Hall π'-subgroup of G and hence $G = (A_{\pi'} \rtimes B'_{\pi'}) \rtimes (A_\pi B_\pi)$. Moreover, if $p \in \pi$ and c is an element of order p in A_p then

$c \in Z(G)$ by (2). This implies that $[B_{p'}, A_p] = 1$ because the kernel of $\text{Res}_p : \text{Aut}(A_p) \to \text{Aut}(\langle c \rangle)$ is a p-group. Then $[B_{\pi'}, A_\pi B_\pi] = 1$ and $A_\pi B_\pi = \prod_{p \in \pi} A_p B_p$. □

Next lemma shows that ϵ^G is determined by any minimal kernel of G.

Lemma 2.5. *If A is a minimal kernel of G then $\epsilon^G = \epsilon^G(A)$.*

Proof. Let $m = m^G = |A|$, $\epsilon = \epsilon^G(A)$ and $r = r^G(A)$. If $m_2 \leq 2$ then $\epsilon = 1 = \epsilon^G$. Otherwise $4 \mid r_2$ and

$$G'_2 = \begin{cases} \langle a^{r_2} \rangle, & \text{if } \epsilon = 1; \\ \langle a^2 \rangle, & \text{if } \epsilon = -1. \end{cases}$$

Then

$$|G'_2| = \begin{cases} \frac{m_2}{r_2}, & \text{if } \epsilon = 1; \\ \frac{m_2}{2}, & \text{if } \epsilon = -1; \end{cases}$$

and hence $\epsilon = -1$ if and only if $m_2 = 2|G'_2| > 2$ if and only if $\epsilon^G = -1$. □

Let

$$R_G = \{r^G(A) : A \text{ is a minimal kernel of } G\}.$$

In the next lemma we see that $|R_G| \leq 2$ and in most cases $|R_G| = 1$. This is, we see that r^G is not always unique, so we cannot take it as an invariant, and we also study in exactly which circumstances this case takes place.

Lemma 2.6. *Let $m = m^G$, $n = n^G$ and $k = k^G$. Then the following statements are equivalent:*

(1) $|R_G| > 1$.

(2) $n_2 \geq 4$, $m_2 \geq 8$, $\epsilon^G = -1$, $k_2 < n_2$ and $R_G = \{\frac{r}{2}, r\}$ for some r with $r_2 = m_2$.

(3) $n_2 \geq 4$, $m_2 \geq 8$, $\epsilon^G = -1$, $k_2 < n_2$, $r_2 \in \{\frac{m_2}{2}, m_2\}$ for some $r \in R_G$ and $[G : B]_2 = \frac{m_2}{2}$ for some metacyclic factorization $G = AB$ with $m = |A|$.

(4) $n_2 \geq 4$, $m_2 \geq 8$, $\epsilon^G = -1$, $k_2 < n_2$, $r_2 \in \{\frac{m_2}{2}, m_2\}$ for some $r \in R_G$ and $[G : B]_2 = \frac{m_2}{2}$ for every metacyclic factorization $G = AB$ with $m = |A|$.

Furthermore, suppose that $G = AB$ is a metacyclic factorization satisfying the conditions of (3) *and let a be a generator of A and b be a generator of B and $s = [G : B]$. Let $C = \left\langle b^{\frac{nm_{2'}}{2s_{2'}}} a \right\rangle$. Then $G = CB$ is another metacyclic factorization with $|C| = m$ and $r^G(C) \neq r^G(A)$.*

Proof. Let $\epsilon = \epsilon^G$, $k = k^G$, $R = R_G$ and for every $p \in \pi$ let $R_p = \{r_p : r \in R\}$. Fix a minimal kernel A of G and let $r = r^G(A)$.

Let $p \in \pi$. If $\epsilon^{p-1} = 1$ then $|G'_p| = \frac{m_p}{r_p}$. Thus in this case $|R_p| = 1$. Therefore $r_{2'}$ is constant for every $r \in R$ and hence $|R| = |R_2|$. Moreover, if $\epsilon = 1$ then $G'_2 = \frac{m_2}{r_2}$ and hence $R_2 = \{\frac{m_2}{|G'_2|}\}$. In this case none of the conditions (1)-(4) hold. Otherwise, $4 \mid r^G(A)_2 \mid m_2$. Thus, if $m_2 < 8$ then $r^G(A)_2 = 4$ for every minimal kernel A of G and hence $|R| = |R_2| = 1$, so that again none of the conditions (1)-(4) hold. Thus in the remainder of the proof we assume that $\epsilon = -1$ and $8 \leq m_2$. Then $G'_2 = A^2$ and hence $\left\langle -1 + r^G(A)_2 \right\rangle_{\frac{m_2}{2}} = \text{Res}_{\frac{m_2}{2}}(\text{T}_G(A)) = \sigma^{-1}_{G'_2}(\text{Inn}_G(G'_2))$, which is independent of A. This shows that if R_2 contains an element smaller than $\frac{m_2}{2}$ then it only has one element and hence again none of the conditions (1)-(4) hold. So in the remainder of the proof we assume that $R_2 \subseteq \{\frac{m_2}{2}, m_2\}$.

Suppose that $k_2 = n_2$. Then, by Lemma 2.4.(4), $C_G(G'_{\pi'})_2 = A_2$, and hence

$$\left\langle -1 + r^G(A)_2 \right\rangle_{m_2} = \text{Res}_{m_2}(T_G(C_G(G'_{\pi'})_2))$$

is independent of A. Therefore, in this case $|R_2| = 1$, so that $|R| = 1$. So again in this case none of the conditions (1)-(4) hold and in the remainder of the proof we also assume that $k_2 < n_2$.

Suppose that $n_2 < 4$. Then none of the condition (2)-(4) holds and as $\epsilon = -1$, we have $n_2 = 2$. By means of contradiction suppose that (1) holds. By the previous paragraph $R_2 = \{\frac{m_2}{2}, m_2\}$ and hence G has two minimal kernels A and C with $r^G(A)_2 = m_2$ and $r^G(C)_2 = \frac{m_2}{2}$. If $G = AB$ and $G = CD$ are metacyclic factorization of G then A_2B_2 and C_2D_2 are Sylow 2-subgroups of G and hence they are isomorphic. However, by Lemma 2.2.(5), $[A_2B_2 : B_2]$ is either m_2 or $\frac{m_2}{2}$. In the first case A_2B_2 is dihedral and in the second case A_2B_2 is quaternionic. This yields a contradiction because from $r^G(C)_2 = \frac{m_2}{2}$ it follows that C_2D_2 is neither dihedral nor quaternionic.

Thus in the remainder we assume that $m_2 \geq 8$, $n_2 \geq 4$, $k_2 < n_2$, $\epsilon = -1$ and $R_2 \subseteq \{\frac{m_2}{2}, m_2\}$. Moreover, by the above arguments we have that $R \subseteq \{\frac{r}{2}, r\}$ for some r with $r_2 = m_2$. Thus (1) and (2) are equivalent.

(4) implies (3) is clear.

(3) implies (2). Let $G = AB$ be a metacyclic factorization of G satisfying the conditions of (3). Let $s = [G : B]$ and $r = r^G(A)$. Select generators a of A and b of B and let $z = b^{\frac{nm_{2'}}{2s_{2'}}}$, $c = za$ and $C = \langle c \rangle$. We will prove that if $G = CB$ is another metacyclic factorization with $|C| = m$ and $r^G(C) \neq r$, so that (2) holds. Indeed, since $k_2 < n_2$, we have $[z, a_{\pi'}] = 1$. Moreover, $[z_{p'}, a_p] = 1$ for every $p \in \pi$. If moreover, $p \neq 2$ then $[z_p, a_p] = 1$ because $[b^n, a] = 1$. Finally, $r_2 \in \{\frac{m_2}{2}, m_2\}$ and hence $o_{m_2}(-1+r_2) = 2$. As $4 \mid n$ and $a_2^{b_2} = a_2^{-1+r_2}$ it follows that $[z_2, a_2] = 1$. This shows that $z \in Z(G)$. As $s = [G : B]$ and $[G : A] = n$ we have $b^n = a^{sx}$ for some integer x coprime with m. Then $c^2 = a^{2+sx\frac{m_{2'}}{s_{2'}}} = a^{2+xs_2m_{2'}} = a^{2+x\frac{m}{2}} = a^{2+\frac{m}{2}}$. As $8 \mid m$ it follows that $|C| = m$. Suppose that $a^b = a^t$. Then $t + 1 \equiv r_2 \mod m_2$. Let $r' \in \mathbb{N}$ with $r'_{2'} = r_{2'}$ and $\{r_2, r'_2\} = \{\frac{m_2}{2}, m_2\}$ and let t' be an integer such that $t' \equiv t \mod m_{2'}$ and $t' \equiv -1 + r'_2 \mod m_2$. As $8 \mid m$ we have $t' \equiv t \equiv -1 \mod 4$ and hence $t' = 1 + 2y$ for some odd integer y. Then $c^{t'} = zz^{t'-1}a^{t'} = zz^{2y}a^{t'} = za^{t'+y\frac{m}{2}}$. Moreover, $t' + y\frac{m}{2} \equiv t' \equiv t \mod m_{2'}$ and $t' + y\frac{m}{2} \equiv -1 + r'_2 + \frac{m_2}{2} \equiv -1 + r_2 \equiv t \mod m_2$. Therefore $c^{t'} = za^t = c^b$. This shows that C is a cyclic normal subgroup of G and clearly $G = CB$ is a metacyclic factorization satisfying the desired condition.

Before proving (1) implies (4) we prove that if $G = AB = CD$ are metacyclic factorizations with $|A| = |B| = m$ then $[G : B]_2 = [G : D]_2$. The assumption $\epsilon = -1$ implies that ${G'}_2 = A^2 = C^2$. As A_2B_2 and C_2D_2 are Sylow 2-groups of G we may assume that they are equal and hence if $A_2 = \langle a \rangle$ and $B = \langle b \rangle$ we may write $c = b^ia^j$ and $d = b^oa^l$. Since $c^2 \in C^2 = A^2$ we have $\frac{n_2}{2} \mid i$ and as $4 \mid n$, necessarily $2 \mid i$ and hence $2 \nmid o$. Then, using that $r^G(A), r^G(C) \in \{\frac{m_2}{2}, m_2\}$ we have that $d^2 = b^{2o}$ or $d^2 = b^{2o}a^{l\frac{m_2}{2}}$. In both cases $d^4 = b^4$ and hence $D^4 = B^4$. As $4 \mid n$ it follows that $A_2 \cap B_2 = B_2^{n_2} = D_2^{n_2} = C_2 \cap D_2$. Therefore, $[G : B]_2 = [A_2B_2 : B_2] = [A_2, A_2 \cap B_2] = [C_2 : C_2 \cap D_2] = [G, D]_2$, as desired.

(1) implies (4). Suppose that $|R| > 1$. By the assumptions and the previous arguments we know that the only condition from (4) which is not clear is that if $G = AB$ is a metacyclic factorization with $m = |A|$ and $s = [G : B]$ then $s_2 = \frac{m_2}{2}$. So suppose that $s_2 = m_2$.

Since $|R| > 1$, there is a second metacyclic factorization $G = CD$ with $|C| = m$ and $\{r^G(A)_2, r^G(C)_2\} = \{\frac{m_2}{2}, m_2\}$. By the previous paragraph $[G : D]_2 = [G : B]_2 = 1$. By symmetry we may assume that $r^G(A)_2 = m_2$ and $r^G(C) = \frac{m_2}{2}$. As above we may assume that $A_2B_2 = C_2D_2$ and if $A_2 = \langle a\rangle$, $B_2 = \langle b\rangle$, $C_2 = \langle c\rangle$ and $D_2 = \langle d\rangle$ then $a^b = a^{-1}$, $c^d = c^{-1+\frac{m_2}{2}}$, $G'_2 = A_2^2 = C_2^2$, $A_2 \neq C_2$ and $A_2 \cap B_2 = C_2 \cap D_2 = 1$. Write $c = b^ia^j$ and $d = b^oa^l$ with $i, j, o, l \in \mathbb{N}$. Since $c^2 \in A$ we have that $\frac{n_2}{2} \mid i$ and as $4 \mid n_2$, we have that o is odd and $[b^i, a] = 1$. Thus $b^{2i} = c^2a^{-2j} \in A_2 \cap B_2 = 1$. Then $c^2 = a^{2j}$ and as $C^2 = A^2$, necessarily j is odd. However, from $b^{2i} = 1$, $[b^i, a] = 1$ and $8 \mid m$ we have $b_2^ia_2^{(-1+\frac{m_2}{2})j} = b_2^{(-1+\frac{m_2}{2})i}a_2^{(-1+\frac{m_2}{2})j} = c_2^{-1+\frac{m_2}{2}} = c_2^d = b_2^ia_2^{-j}$ and hence $2 \mid j$, a contradiction. □

In our next result we show a way to decide if a factorization of G is minimal and we prove that the following algorithm transforms a metacyclic factorization of G into a minimal one.

Algorithm 1. ***Input:*** *A metacyclic factorization $G = AB$ of a finite group G.*

Output: *$a, b \in G$ with $G = \langle a\rangle\langle b\rangle$ a minimal metacyclic factorization of G.*

```
(1) $m := |A|$, $n := [G : A]$, $s := [G : B]$,
(2) $a :=$ some generator of $A$, $b :=$ some generator of $B$, and $y \in \mathbb{N}$ with $b^n = a^y$.
(3) $r := r^G(A)$, $\epsilon := \epsilon^G(A)$ and $k = k^G(A)$.
(4) for $p \in \pi(r)$ with $\epsilon^{p-1} = 1$
      (a) if $s_p \nmid n$ then $b := ba_p$ and $s := s_{p'}n_p$.
      (b) if $r_p \nmid s$, $s_pk_p \mid n$ and $t \in \mathbb{N}$ satisfy $a_p^{b_p} = a_p^t$, compute $x \in \mathbb{N}$ satisfying
          $x\mathcal{S}\left(t^{\frac{n}{s_p}} \mid s_p\right) \equiv r - y \mod m_p$ and set $a := b_p^{\frac{n}{s_p}}a_{p'}a_p^x$, $m := s_p\frac{m}{r_p}$, $n := n\frac{r_p}{s_p}$,
          and
          $$(r, \epsilon) := \begin{cases} (4r_{2'}, -1), & \text{if } 8 \mid m, s_p = 2, \text{ and } r_2 = \frac{m_2}{2}; \\ (r_{p'}s_p, 1), & \text{otherwise.} \end{cases}$$
(5) If $\epsilon = -1$, $4 \mid n$, $8 \mid m$, $k_2 < n_2$ and $r_2 \nmid s$ then $a := b^{\frac{m_{2'}n}{2s_{2'}}}a$ and $r := r_{2'}s_2$
```

(6) *If $\epsilon = -1$ and $s_2 = r_2 n_2$ then $b := ba_2$ and $s := \frac{s}{2}$.*

(7) *Return (a, b).*

Proposition 2.7. *Let $G = AB$ be a metacyclic factorization and let $m = |A|$, $n = [G : A]$, $s = [G : B]$ and $T = T_G(A)$. Then $G = AB$ is minimal as metacyclic factorization of G if and only if T is (n, s)-canonical.*

Furthermore, if the input of Algorithm 1 is a metacyclic factorization of G and its output is (a, b) then $G = \langle a \rangle \langle b \rangle$ is a minimal metacyclic factorization of G.

Proof. Let $(r, \epsilon, k) = [T_G(A)]$. By Lemma 2.4, $\pi' = \pi(m) \setminus \pi(r)$. Fix $y, t \in \mathbb{N}$ with $b^n = a^y$ and $a^b = a^t$. Then $s = \gcd(t, m)$, $\gcd(t, m) = 1$, $r_{2'} = \gcd(m_{2'}, t-1)$ and $r_2 = \gcd(m_2, t-\epsilon)$. For every prime p let $G_p = A_p B_p$.

Claim 1. If condition (Can+) holds then A is a minimal kernel of G.

Suppose that condition (Can+) holds and let C be kernel of G. We want to prove that $|C| \geq m$ and for that it is enough to show that $|C_p| \geq m_p$ for every prime p. This is obvious if $m_p = 1$, and it is a consequence of Lemma 2.4.(3), if $p \in \pi'$. So we suppose that $p \in \pi$ and $m_p \neq 1$. Hence $p \mid r$.

Suppose first that $\epsilon^{p-1} = -1$. Then $p = 2$ and $A_2^2 = G_2' \subseteq C_2$. However $C_2 \not\subseteq A_2^2$ because G_2/A_2^2 is not cyclic. Therefore $|C_2| \geq 2|A_2^2| = m_2$.

Suppose otherwise that $\epsilon^{p-1} = 1$. Then $G_p' = A_p^{r_p}$ and $|G'_p| = \frac{m_p}{r_p}$. Assume that $r_p \mid s_p$. Then $G_p/G_p' = (A_p/G_p') \times (B_p G'_p/G'_p)$ and $r_p = |A_p/G'_p| \leq n_p = [B_p G'_p : G'_p]$. As $(G_p/G'_p)/(C_p/G'_p) \cong G_p/C_p$ is cyclic, necessarily $r_p \mid [C_p : G'_p]$ and hence $m_p \mid |C_p|$, as desired. Assume otherwise that $r_p \nmid s_p$. By condition (Can+) we have $s_p \mid n_p$ and $s_p k_p \nmid n_p$. In particular $p \mid k_p$. By Lemma 2.4.(3), $C_{\pi'} = A_{\pi'}$ and thence $C_p \subseteq C_{G_p}(A_{\pi'})_p = A_p B_p^{k_p}$. Using again that G_p/C_p is cyclic and $p \mid k_p$, we must have $C_p = \left\langle b_p^x a_p \right\rangle$ for $x \in \mathbb{N}$ with $k_p \mid x$ and $x \leq n$. Let $R \in \mathbb{N}$ such that $a_p^{b_p^x} = a_p^R$. Then R satisfies the hypothesis of Lemma 1.1.(2c) and hence $v_p\left(\mathcal{S}\left(R \mid \frac{n}{x_p}\right)\right) = v_p(n) - v_p(x) \leq v_p(n) - v_p(o) < v_p(s) = v_p(yx_{p'})$ and therefore $v_p\left(yx_{p'} + \mathcal{S}\left(R \mid \frac{n}{x_p}\right)\right) = v_p(n) - v_p(x)$. Then $|C_p| = \frac{n_p}{x_p}|(b_p^x a_p)^{\frac{n_p}{x_p}}| = \frac{n_p}{x_p}\left|a_p^{yx_{p'} + \mathcal{S}\left(R | \frac{n_p}{x_p}\right)}\right| = m_p$. This finishes the proof of Claim 1.

Claim 2. If $T_G(A)$ is (n,s)-canonical then for every metacyclic factorization $G = CD$ with $|C| = m$ one has $r^G(C) \ge r$ and $|D| \le |B|$.

If $r^G(C) < r$ then, by Lemma 2.6, $m_2 \ge 8$, $n_2 \ge 4$, $\epsilon = -1$, $k_2 < n_2$, $r^G(C)_2 = \frac{m_2}{2} = s_2$ and $r_2 = m_2$, in contradiction with the second part of condition (Can–). Thus $r^G(C) \ge r$.

To prove that $|D| \le |B|$ we show that $|D_p| \le |B_p|$ for each prime p. This is clear if $p \nmid m$ and a consequence of Lemma 2.4.(4) if $p \in \pi'$. Otherwise $p \mid r$. Since both G_p and C_pB_p are Sylow p-subgroups of G we may assume that $G_p = C_pD_p$.

Assume first that $\epsilon^{p-1} = 1$. Then by assumption $s_p \mid n_p$. Let $d = b_p^x a_p^y$ be a generator of D_p and let $R \in \mathbb{N}$ such that $a_p^{b_p^x} = a_p^R$. The assumption $\epsilon^{p-1} = 1$ implies that R satisfies the hypothesis of Lemma 1.1.(1a) and hence $m_p \mid \mathcal{S}\left(R \mid m_p \frac{n_p}{s_p}\right)$ and from (1.1) we deduce that $d^{\frac{m_p n_p}{s_p}} = a_p^{y\mathcal{S}\left((1+r_p)^x \mid m_p \frac{n_p}{s_p}\right)} = 1$ and hence $|D_p| \le \frac{m_p n_p}{s_p} = |b_p|$. Suppose otherwise that $\epsilon^{p-1} = -1$, i.e. $p = 2$ and $\epsilon = -1$. Then $C_2^2 = G'_2 = A_2$ and $C_2 \cap D_2 \subseteq Z(G_2) \cap C_2 = Z(G_2) \cap C_2^2 = Z(G_2)A = A^{\frac{m_2}{2}}$ and hence $|C_2 \cap D_2| \le 2$. Thus $|D_2| = [D_2 : C_2 \cap D_2]\ |C_2 \cap D_2| = [G_2 : C_2]\ |C_2 \cap D_2| \in \{n_2, 2n_2\}$. Similarly, $|B_2| \in \{n_2, 2n_2\}$. If $|B_2| = 2n_2$ then $|D_2|$ divides $|B_2|$ as desired. Suppose otherwise that $|B_2| = n_2$. Then $m_2 = s_2$ and hence m_2 divides $\frac{r_2 n_2}{2}$, by the hypothesis (Can–) and Lemma 2.2.(5). If $D_2 \subseteq \langle a, b_2^2 \rangle$ then $C_2 = \langle b_2 a_2^x \rangle$ for some integer x and hence $n_2 = 2$ because $C_2^2 = \langle a_2^2 \rangle$. Then $D_2 \subseteq \langle a_2 \rangle$ so that D_2 is normal in G_2 and hence $\langle a_2^2 \rangle = C_2^2 = [D_2, C_2] \subseteq C_2 \cap D_2 \subseteq \left\langle a_2^{\frac{m_2}{2}} \right\rangle \subseteq \langle a_2^2 \rangle$. Then $m_2 = 4$ and G_2 is dihedral of order 8. Then every metacyclic factorization of G_2 is of the form $\langle a_2 \rangle \langle c \rangle$ with $|c| = 2$. Thus $|D_2| = 2 = |b_2|$, as wanted. Assume otherwise that $D_2 \not\subseteq \langle a_2, b_2^2 \rangle$. Then $D_2 = \langle b_2 a_2^x \rangle$ for some integer x and let $R \in \mathbb{N}$ such that $a_2^{b_2} = a_2^R$. The hypothesis $\epsilon = -1$ implies that R satisfies the hypothesis of Lemma 1.1.(2a). Since m_2 divides $\frac{r_2 n_2}{2}$, we get $v_2(\mathcal{S}\,(R \mid n_2)) = v_2(r_2) + v_2(n_2) - 1 \ge v_2(m_2)$ and hence $(b_2 a_2^x)^{n_2} = a_2^{x\mathcal{S}(-1+r_2 \mid n_2)} = 1$. Then $|D_2| = n_2$, as desired. This finishes the proof of Claim 2.

The necessary part in the first statement of the proposition follows from claims 1 and 2.

Claim 3. If $p \mid r$, $\epsilon^{p-1} = 1$ and $s_p \nmid n_p$ then $[G : ba_p] = s_{p'} n_p < s$.

First of all $n = |ba_pA|$ and hence n divides $|ba_p|$. Using (1.1) we have $(ba_p)^n = a_{p'}^y a_p^{y+\mathcal{S}(t|n)}$ and $v_p([G : \langle ba_p \rangle]) = v_p(\mathcal{S}\,(t \mid n)) = v_p(n) < v_p(s) = v_p(y)$, by Lemma 1.1.(1a) and the assumption. Thus $|ba_p| = n \frac{m}{s_{p'} n_p}$ and hence $[G : ba_p] = s_{p'} n_p$. This finishes the proof of

Claim 3.

By Claim 3, if the first part of (Can+) fails then $G = AB$ is not minimal because $G = A\langle ba_p\rangle$ is a factorization with $[G : b] > [G : \langle ba_p\rangle]$. Moreover, the factorization $G = A\langle ba_p\rangle$ satisfies the first part of condition (Can+) and hence after step (4a) of Algorithm 1, the factorization $G = \langle a\rangle\langle b\rangle$ satisfies the first part of (Can+) for the prime p.

Claim 4. Suppose that $p \mid r$, $\epsilon^{p-1} = 1$, $s_p \mid n$, $r_p \nmid s$ and $s_pk_p \mid n$. Let $R \in \mathbb{N}$ with $a_p^{b_p^{\frac{n}{s_p}}} = a^R$. Then there is an integer x such that $r - y \equiv x\mathcal{S}\left(R \mid s_p\right) \mod m_p$. This justify the existence of x in step (4) of Algorithm 1. Let $c = b_p^{\frac{n}{s_p}} a_{p'} a_p^x$ and $C = \langle c\rangle$. Then $G = CB$ is a metacyclic factorization of G with $|C| = m\frac{s_p}{r_p} < |A|$. Moreover,

$$(r^G(C), \epsilon^G(C)) := \begin{cases} (4r_{2'}, -1), & \text{if } 8 \mid m, s_p = 2, \text{ and } r_2 = \frac{m_2}{2}; \\ (r_{p'}s_p, 1), & \text{otherwise.} \end{cases}$$

The assumption $s_pk_p \mid n_p$ implies that $k_p \mid \frac{n}{s_p}$ and hence $[b_p^{\frac{n}{s_p}}, a_{\pi'}] = 1$. As also $[b_p, a_{\pi\setminus\{p\}}] = 1$ we deduce that $[b_p^{\frac{n}{s_p}}, a_{p'}] = 1$. On the other hand, since $r_p \nmid s_p$, $v_p(y) = v_p(s) < v_p(r)$ and therefore $v_p(r - y) = v_p(s) = v_p(\mathcal{S}\left(t \mid s_p\right))$, by Lemma 1.1.(1a). Therefore there is an integer x coprime with p such that $r - y \equiv x\mathcal{S}\left(R \mid s_p\right) \mod m_p$. Using (1.1) we have $c^{s_p} = b_p^n a_{p'}^{s_p} a_p^{x\mathcal{S}(R|s_p)} = a_{p'}^{s_p} a_p^{y+x\mathcal{S}(R|s_p)} = a_{p'}^{s_p} a_p^r$. Then $G'_{p'} \subseteq \langle a_{p'}\rangle \subseteq C$ and $G'_p = \left\langle a_p^r\right\rangle \subseteq C$. Thus $G' \subseteq C$ and hence $G = CB$ is a metacyclic factorization of G with $|C| = s_p|a_{p'}||a_p^r| = m\frac{s_p}{r_p} < m = |A|$. As $C_{p'} = A_{p'}$, we have $r^G(C)_{p'} = r^G(A)_{p'} = r_{\pi'}$. If $\epsilon^G(C)^{p-1} = 1$ then $\frac{m_p}{r_p} = |G'_p| = \frac{|C_p|}{r^G(C)_p} = \frac{m_ps_p}{r_pr^G(C)_p}$ and hence in this case $r^G(C) = r_{p'}s_p$. Otherwise, i.e. if $p = 2$ and $\epsilon^G(C) = -1$ then $2|C_2| \le s_2 \le |C_2|$ and $4 \le r^G(C)_2 \le |C_2| = \frac{m_2s_2}{r_2} = 2|G'_2| = \frac{2m_2}{r_2}$ and hence $s_2 = 2$, $|C_2| = 4 = r^G(C)_2$ and $r_2 = \frac{m_2}{2}$. Conversely, if $s_2 = 2$ and $r_2 = \frac{m_2}{2}$ then $|C_2| = 4$ and hence $r^G(C)_2 = 4$. Moreover, as G_2 is not commutative then $\epsilon^G(C) = -1$. This finishes the proof of Claim 4.

Claim 4 shows that if the first part of (Can+) holds but the second one fails then $G = AB$ is not minimal. It furthermore the parameters associated to the factorization $G = CB$, i.e. $|C|, [G : C], [G : B], r^G(C), \epsilon^G(C), k^G(C)$, satisfy condition (Can+) for the prime p and hence, after step (4b) of Algorithm 1, the current factorization $G = \langle a\rangle\langle b\rangle$ satisfies this condition. Moreover, if $\epsilon^G(C) = 1$ then $r_p(C) = s_p \le n_p$ and condition (C+) holds for the prime p. Thus when the algorithm finishes the loop in step (4), the metacyclic factorization satisfies condition (Can+) and hence the current value of $\langle a \rangle$ is a minimal kernel of G by Claim 1.

Observe that the modification of a and b in steps (4a) and (4b) for some prime p does not affect the subsequent calculations inside the loop. Indeed, suppose that p and q are two different divisors of r with $\epsilon^{p-1} = \epsilon^{q-1} = 1$, and the prime p has been considered before the prime q in step (4). This has affected a and b which have been transformed by first transforming b into $d = ba_p$ and then transforming a into $c = d_p a_{p'} a_p^x = b_p a_{p'} a_p^{1+x}$. In principal we should recalculate the natural number y computed in step (2) to a new y'. However, as $p \in \pi$, $[b_{p'}, a_p] = [b_{q'}, a_p] = 1$ and hence $a_{p'} = c_{p'}$ and $b_{p'} = d_{p'}$. Therefore $d_q = c_q^y$ and hence $y' \equiv y \mod m_q$. Therefore when in step (4b) for the prime q we compute x satisfying if $r - y \equiv x\mathcal{S}\left(R \mid s_q\right) \equiv \mod m_q$ we also have $r - y' \equiv x\mathcal{S}\left(R \mid s_q\right) \mod m_q$.

By Lemma 2.6, if the second part of condition (Can–) is satisfied then $r^G(A) = r^G$. Otherwise, $r^G(A) > r^G$, and hence the factorization $G = AB$ is not minimal, However, after step (5) the factorization $G = \langle a \rangle \langle b \rangle$ satisfy both $|a| = m^G$ and $r^G(\langle a \rangle) = r^G$. In the remainder of the algorithm the kernel $\langle a \rangle$ is not modified and hence this is going to be valid in the remainder of the algorithm.

Finally suppose that the first part of (Can–) fails, so that $p = 2$, $\epsilon = -1$ and $s_2 = r_2 n_2$. Then $4 \mid r$ and $\langle t \rangle_{m_2} = \langle -1 + r_2 \rangle_{m_2}$. Moreover, by Lemma 2.2.(5), we have that $s_2 \in \{\frac{m_2}{2}, m_2\}$ and $m_2 \mid r_2 n_2$. Therefore $s_2 = m_2 = r_2 n_2$. Then $v_2(\mathcal{S}\left(t \mid n_2\right)) = v_2(r) + v_2(n) - 1 = v_2(m) - 1$, by Lemma 1.1.(2a). As in the proof of Claim 3, we use the metacyclic factorization of $G = A \langle ba_2 \rangle$. If $G = AB$ is minimal then we have $n|(ba_2)^n| = |ba_2| \leq |b| = n|a^s| = n\frac{m}{s}$. Therefore $|(ba_2)^n| \leq \frac{m}{s}$. Using (1.1) once more and $[b_{2'}, a_2] = 1$, we obtain $(ba_2)^n = a^y a_2^{\mathcal{S}(t|n_2)} = a_{2'}^y a_2^{\frac{m_2}{2}}$. Thus $|(ba_2)^n| = 2\frac{m}{s}$ and hence $|ba_2| = 2\frac{ms}{s} = 2|B|$, contradicting the minimality. Thus $G = AB$ is not minimal. Moreover, the new metacyclic factorization satisfies (Can–) because, $|ba_2|_2 = 2|b|_2$ and hence if $s' = [G : \langle ba_2 \rangle]$ then $s'_2 = \frac{m_2}{2} \neq m_2 = r_2 n_2$. □

In order to prove that the last entry of MCINV(G) is well defined and prove Theorem A we need one more lemma which is inspired in Lemmas 5.5 and 5.7 of [Hem00].

Lemma 2.8. *Let p be a prime and consider the group $P = \mathcal{G}_{m,n,s,\epsilon+r}$ with m and n powers of p, r and s divisors of m and $\epsilon \in \{1,-1\}$ satisfying the following conditions: $p \mid r$, $m \mid rn$, if $4 \mid m$ then $4 \mid r$, if $\epsilon = 1$ then $m \mid rs$ and if $\epsilon = -1$ then $2 \mid n$, $4 \mid m$ and $m \mid 2s$. Let o be a divisor of n and $N = \langle a, b^o \rangle$. Denote*

$$w = \begin{cases} \min(o, \frac{m}{r}, \max(1, \frac{s}{r}, \frac{so}{n})), & \text{if } \epsilon = 1; \\ 1, & \text{if } \epsilon = -1 \text{ and }, o \mid 2 \text{ or } m \mid 2r; \\ \frac{m}{2r}, & \text{if } \epsilon = -1, 4 \mid o < n, 4r \mid m, \text{ and if } s \neq nr \text{ then } 2s = m < nr; \\ \frac{m}{r}, & \text{otherwise.} \end{cases}$$

If y is an integer coprime with p then the following conditions are equivalent:

(1) There are $c \in N$ and $d \in b^y N$ such that $P = \langle c, d \rangle$, $|c| = m$, $d^n = c^s$ and $c^d = c^{\epsilon+r}$.

(2) $y \equiv 1 \mod w$.

Proof. Observe that N is the unique subgroup of G of index o containing a. We will make a wide use of (1.1) and Lemma 1.1, sometimes without specific mention. We consider separately the cases $\epsilon = 1$ and $\epsilon = -1$.

Case 1. Suppose $\epsilon = 1$.

(1) implies (2). Suppose that c and d satisfy the conditions of (1). If $w = 1$ then obviously (2) holds. So we may assume that $w \neq 1$ and in particular $p \mid o$ and $pr \mid m$. The first implies that $N \subseteq \langle a, b^p \rangle$ and the second that $P / \langle a^p, b^p \rangle$ is not cyclic. Therefore $c \notin \langle a^p, b^p \rangle$ and hence $\langle c \rangle = \langle b^{xv} a \rangle$ with $o \mid v \mid n$ and $p \nmid x$. Write $d = b^{y_1} a^z$ with $y_1, z \in \mathbb{Z}$. From the assumption $d \in b^y N$ we have that $y_1 \equiv y \mod o$ and hence $y \equiv y_1 \mod w$. Therefore, it suffices to prove that $y_1 \equiv 1 \mod w$. From $c^d = c^{1+r}$ we have

$$b^{xv} a^{z(1-(1+r)^{xv})+(1+r)^{y_1}} = (b^{xv}a)^{b^{y_1}a^z} = (b^{xv}a)^{1+r} = b^{xv} a b^{xvr} a^{\mathcal{S}((1+r)^{xv} \mid r)}.$$

Then $n \mid vr$ and $b^{xvr} = a^{xs\frac{vr}{n}}$. Thus

$$z(1-(1+r)^{xv}) + (1+r)^{y_1} - 1 \equiv xs\frac{vr}{n} + \mathcal{S}\left((1+r)^{xv} \mid r\right) \mod m.$$

This implies that that r divides $xs\frac{vr}{n}$, since r divides m. As r is coprime with x, it follows that n divides sv. Moreover, $(1+r)^{xv} \equiv 1 \mod rv$, by Lemma 1.1.(1a), and hence $\mathcal{S}\left((1+r)^{xv} \mid r\right) \equiv r \mod rv$. As r, v, m and s are powers of p we deduce that

$$(1+r)^{y_1} \equiv 1+r \mod \min(m, rv, \frac{svr}{n}).$$

Using Lemma 1.1.(1b) it follows that $y_1 \equiv 1 \mod \min(\frac{m}{r}, v, \frac{sv}{n})$.

Suppose that $y_1 \not\equiv 1 \mod w$. Then

$$\min\left(\frac{m}{r}, o, \frac{so}{n}\right) \leq \min\left(\frac{m}{r}, v, \frac{sv}{n}\right) < w = \min\left(\frac{m}{r}, o, \max\left(1, \frac{s}{r}, \frac{so}{n}\right)\right)$$

and hence $\frac{s}{r} > \left(1, \frac{so}{n}\right)$ and $\frac{m}{r} \geq w = \min\left(o, \frac{s}{r}\right) > \min\left(\frac{m}{r}, v, \frac{sv}{n}\right)$. Thus

$$\frac{s}{r} \geq w = \min\left(o, \frac{s}{r}\right) > \min\left(v, \frac{sv}{n}\right) \geq \min\left(o, \frac{so}{n}\right).$$

Since $n \mid vr$ it follows that $\min(v, \frac{sv}{n}) < \frac{s}{r} \leq \frac{sv}{n}$ and hence $o \leq v = \min(v, \frac{vs}{n}) < \min(o, \frac{s}{r})$, a contradiction.

(2) implies (1). We now suppose that $y \equiv 1 \mod w$ and we have to show that there is $c \in N$ and $d \in b^y N$ satisfying the conditions in (1). If $y \equiv 1 \mod o$ then $bN = b^y N$ and hence $c = a$ and $d = b$ satisfy the desired condition. If $(1+r)^y \equiv 1+r \mod m$ then $a^{b^y} = a^{1+r}$ and hence $c = a^y$ and b^y satisfy the desired conditions. So we suppose that $y \not\equiv 1 \mod o$ and $(1+r)^y \not\equiv 1+r \mod m$. The first implies that $w < o$ and the second that $y-1$ is not multiple of $o_m(1+r) = \frac{m}{r}$, by Lemma 1.1.(1b) and hence $w < \frac{m}{r}$. Thus $w = \max(1, \frac{s}{r}, \frac{os}{n}) < \min(o, \frac{m}{r})$.

By Lemma 1.1.(1b) we have $(1+r)^y = 1 + r(1+xu)$ with $p \nmid x$, u a power of p and $v_p(w) \leq v_p(u) = v_p(y-1) < v_p(\frac{m}{r}) \leq v_p(s)$. Moreover, if $u=1$ then $p \nmid 1+x$. Let $c_1 = b^{x\frac{nu}{s}}a$. We now prove that $|c_1| = m$. Observe that $\frac{nu}{s} \geq \frac{nw}{s} \geq o$. Therefore $c_1 \in N$. Moreover, as $v_p(u) < v_p(s)$ it follows that $|c_1 \langle a \rangle| = \frac{s}{u}$ and $c_1^{\frac{s}{u}} = a^{xs+\mathcal{S}\left((1+r)^{x\frac{nu}{s}} \mid \frac{s}{u}\right)}$. If $u \neq 1$ then $v_p(r) \geq v_p(\frac{s}{w}) \geq v_p(\frac{s}{u}) = v_p(\mathcal{S}\left((1+r)^{x\frac{nu}{s}} \mid \frac{s}{u}\right)) = v_p(xs + \mathcal{S}\left((1+r)^{x\frac{nu}{s}} \mid \frac{s}{u}\right))$ and therefore $G' = \langle a^r \rangle \subseteq \langle c_1 \rangle$ and $|c_1| = m$, as desired. Otherwise, i.e. if $u = 1$ then $w = 1$ and hence $s \leq r$ and $p \mid o \mid \frac{n}{s}$. Then $xs + \mathcal{S}\left((1+r)^{x\frac{nu}{s}} \mid s\right) \equiv s(x+1) \not\equiv 0 \mod pr$ because $s \leq r$ and $p \nmid x+1$. Therefore also in this case $v_p(r) \leq v_p(xs + \mathcal{S}\left((1+r)^{x\frac{nu}{s}} \mid s\right))$ and hence $G' \subseteq \langle c_1 \rangle$ and $|c_1| = m$, as desired.

Since $(1+r)^{x\frac{nu}{s}} \equiv 1 \mod r^{\frac{nu}{s}}$ we have $\mathcal{S}\left((1+r)^{x\frac{nu}{s}} \mid r\right) \equiv r \mod r^{\frac{nu}{s}}$. Therefore $(1+r)^y - 1 - xru - \mathcal{S}\left((1+r)^{x\frac{nu}{s}} \mid r\right) \equiv 0 \mod \frac{rnu}{s}$. Moreover, $v_p(1-(1+r)^{x\frac{nu}{s}}) = v_p(r^{\frac{nu}{s}})$, and hence there is an integer z satisfying

$$z(1-(1+r)^{x\frac{nu}{s}}) + (1+r)^y \equiv 1 + xru + \mathcal{S}\left((1+r)^{xu} \mid r\right) \mod m.$$

Let $d = b^y a^z \in b^y N$. Using that $u \geq w \geq \frac{s}{r}$ we have

$$c_1^d = (b^{x\frac{nu}{s}}a)^{b^y a^z} = b^{x\frac{nu}{s}} a^{z(1-(1+r)^{x\frac{nu}{s}})+(1+r)^y} = b^{x\frac{nu}{s}} a^{1+xru+\mathcal{S}\left((1+r)^{x\frac{nu}{s}} \mid r\right)} = c_1^{1+r},$$

On the other hand

$$d^n = (b^y a^z)^n = a^{sy+z\mathcal{S}((1+r)^y \mid n)}$$

and

$$c_1^s = (b^{x\frac{nu}{s}}a)^s = a^{xus+\mathcal{S}\left((1+r)^{x\frac{nu}{s}} \mid s\right)}.$$

if $s \geq n$ then $o > w = \max(\frac{so}{n}, \frac{s}{r}) \geq \frac{so}{n} \geq o$, a contradiction. Therefore, s is a proper divisor of n and hence $v_p(sy + z\mathcal{S}\left((1+r)^y \mid n\right)) = s$. Then d^n and c_1^s are elements of $\langle a \rangle$ of the same order. Therefore $b^n = c^{os}$ for some integer o coprime with p. Then $c = c_1^o$ and d satisfy the conditions of (1).

Case 2. Suppose that $\epsilon = -1$.

(1) implies (2). Suppose that c and $d = b^y a^z$ satisfy the conditions of (1). Then $4 \mid r$ and $G' = \langle a^2 \rangle = \langle c^2 \rangle$. As in Case 1 we may assume that $w \neq 1$. Then both o and $\frac{m}{r}$ are multiple of 4 and we must prove, on the one hand that $y \equiv 1 \mod \frac{m}{2r}$ and, on the other hand that $y \equiv 1 \mod \frac{m}{r}$, if one of the following conditions hold: $k = n$ or, $s = m \neq nr$, or $2s = m = nr$. From $4 \mid o$ and $G/\langle c \rangle$ being cyclic we deduce $\langle c \rangle = \langle b^{xv} a \rangle$ with $o \mid v \mid n$ and $2 \nmid x$. From $G' = \langle a^2 \rangle = \langle c^2 \rangle$ it follows that $\frac{n}{2} \mid v$ so that v is either n or $\frac{n}{2}$. If $v = n$ then $\langle c \rangle = \langle a \rangle$. Therefore $a^{-1+r} = a^d = a^{(-1+r)^y}$ and hence $(-1+r)^{y-1} \equiv 1 \mod 2^m$. Then $y \equiv 1 \mod \frac{m}{r}$ by Lemma 1.1.(2b). This proves the result if $k = n$ because in that case v is necessarily n.

Suppose otherwise that $v = \frac{n}{2}$. Then we distinguish the cases $m < nr$ and $m = nr$.

Assume that $m < nr$. Then, as $4 \mid o \mid v$ we have $o_m(-1+r) = \max\left(2, \frac{m}{r}\right) \leq \frac{n}{2} = v$ and hence b^v is central in G. Then, having in mind that $4 \mid r$ and $m \mid 2s$, we have

$$b^{xv} a^{(-1+r)^y} = (b^{xv}a)^{b^y a^z} = (b^{xv}a)^{-1+r} = b^{xv}a(b^{xv}a)^{r-2} = b^{xv}a^{r-1+xs(\frac{r}{2}-1)} = b^{xv}a^{-1+s+r}.$$

Therefore $(-1+r)^y \equiv -1+r+s \mod m$ and in particular $(-1+r)^y \equiv -1+r \mod s$, since $s \mid m$. Using Lemma 1.1 once more we deduce that $y \equiv 1 \mod \frac{m}{2r}$ and if $s=m$ then $y \equiv 1 \mod \frac{m}{r}$.

Suppose otherwise that $m = nr$. Then, from Lemma 1.1.(2a) we have $v_2((-1+r)^v-1) = v_2(r)+v_2(v) = v_2(r)+v_2(n)-1 = v_2(\frac{m}{2})$ so that $a^{b^v} = a^{1+\frac{m}{2}}$ and $(b^{xv}a)^2 = a^{2+s+\frac{m}{2}}$ and hence $(b^{xv}a)^4 = a^4$. As $4 \mid o$ it follows that $(b^{xv}a)^n = a^n$. On the other hand, as y is odd, it follows that $v_2((-1+r)^y+1) = v_2(r) \geq 2$, by Lemma 1.1.(2c). Therefore, $v_2(\mathcal{S}((-1+r)^y \mid n)) = v_2(rn)-1 = v_2(m)-1$, by Lemma 1.1.(2a). Then $\mathcal{S}((-1+r)^y \mid n) \equiv \frac{m}{2} \mod m$ an hence, having in mind that $8 \mid \frac{m}{2} \mid s$ we deduce that $a^s = c^s = d^n = a^{ys+z\mathcal{S}((-1+r)^y|n)} = a^{s+z\frac{m}{2}}$. Therefore z is even. On the other hand from $c^d = c^{-1+r}$ and having in mind that $(-1+r)^v - 1 \equiv \frac{m}{2} \mod m$ and z is even, we obtain

$$b^{xv}a^{(-1+r)^y} = (b^{xv}a)^{b^y a^z} = (b^{xv}a)^{-1+r} = b^{xv}a(b^{xv}a)^{r-2} = b^{xv}a(a^{xs+2+\frac{m}{2}})^{\frac{r}{2}-1} = b^{xv}a^{-1+s+r+\frac{m}{2}}.$$

Therefore $(-1+r)^y \equiv -1+r+s+\frac{m}{2} \mod m$. Again, from $m \mid 2s$ and Lemma 1.1.(2b) we deduce that $y \equiv 1 \mod \frac{m}{2r}$ and if $s = \frac{m}{2}$ then $y \equiv 1 \mod \frac{m}{r}$.

(2) implies (1). Suppose that $y \equiv 1 \mod w$. As y is odd, if $o \mid 2$ then $b \in b^y N$ and hence a and b satisfy condition (1). So we assume from now on that $4 \mid o$. In particular $4 \mid n$. Suppose that $m \mid 2r$, i.e. r is either m or $\frac{m}{2}$ and let $c = a^y$ and $d = b^y a^2$. In this case b^2 is central in P and hence $c^d = c^b = c^{-1+r}$ and applying statements (2a) and (2c) of Lemma 1.1 we obtain $d^n = a^{ys+\mathcal{S}((-1+r)^y|n)} = a^{ys} = c^s$. Hence c and d satisfy the conditions of (1).

Thus from now on we assume that 4 divides both o and $\frac{m}{r}$. Suppose that $y \equiv 1 \mod \frac{m}{r}$. Then $a^{b^y} = a^b = a^{-1+r}$ because $b^{\frac{m}{r}}$ is central in P. Moreover, as $m \mid 2s$ and y is odd we have $(b^y)^n = a^{sy} = a^s$. Therefore $c = a$ and $d = b^y$ satisfy condition (1) and this finishes the proof of the lemma if $w = \frac{m}{r}$ and it also proves that for $w = \frac{m}{2r}$ we may assume that $y \not\equiv 1 \mod \frac{m}{r}$. So suppose that $w = \frac{m}{2r}$ and $y \not\equiv 1 \mod \frac{m}{r}$. Then $y \equiv 1 + \frac{m}{2r} \mod \frac{m}{r}$, $o < n$ and either $m = s = nr$ or $2s = m < nr$. Let $c = b^{\frac{n}{2}}a$ and $d = b^y$. Then, in both cases, $c^2 = a^{2+\frac{m}{2}}$ and, as $\frac{m}{2}$ is multiple of 4 we have that $G' = \langle a^2 \rangle = \langle c^2 \rangle$, $|c| = m$ and $c^s = a^s$. Moreover,

$$c^{-1+r} = (b^{\frac{n}{2}}a)^{-1+r} = b^{\frac{n}{2}}a(b^{\frac{n}{2}}a)^{r-2} = b^{\frac{n}{2}}aa^{(2+\frac{m}{2})(\frac{r}{2}-1)} = b^{\frac{n}{2}}a^{-1+r+\frac{m}{2}} = b^{\frac{n}{2}}a^{(-1+r)(1+\frac{m}{2})} = (b^{\frac{n}{2}}a)^{b^{1+\frac{m}{2r}}} = c^d$$

and

$$d^n = a^{s(1+\frac{m}{2r})} = a^s = c^s.$$

Then c and d satisfy the conditions of (1). □

Theorem 2.9. *Let $m, n, s \in \mathbb{N}$ with $s \mid m$ and let T and $\bar{T}$ be (n,s)-canonical cyclic subgroups of $\mathcal{U}_m$. Set $(r, \epsilon, k) = [T]$, $[\bar{r}, \bar{\epsilon}, \bar{o}] = [\bar{T}]$, $\pi = \pi(r) \cup (\pi(n) \setminus \pi(m))$, $\bar{\pi} = \pi(\bar{r}) \cup (\pi(n) \setminus \pi(m))$, $m' = [T, n, s]$ and $\bar{m}' = [\bar{T}, n, s]$.*

Then the following statements are equivalent.

(1) $\mathcal{G}_{m,n,s,T}$ and $\mathcal{G}_{m,n,s,\bar{T}}$ are isomorphic.

(2) $\operatorname{Res}_{m'}(T) = \operatorname{Res}_{\bar{m}'}(\bar{T})$.

(3) $\pi = \bar{\pi}$, $\operatorname{Res}_{m_{\pi'}}(T_{\pi'}) = \operatorname{Res}_{m_{\pi'}}(\bar{T}_{\pi'})$ and $\operatorname{Res}_{m_{\pi'}m'_p}(T_p) = \operatorname{Res}_{m_{\pi'}m'_p}(\bar{T}_p)$ for every $p \in \pi$.

Proof. Let $G = \mathcal{G}_{m,n,s,T}$ and $\bar{G} = \mathcal{G}_{m,n,s,\bar{T}}$. To distinguish the generators a and b in the presentation of G and $\bar{G}$ we denote the latter by $\bar{a}$ and $\bar{b}$. We also denote $A = \langle a \rangle$, $B = \langle b \rangle$, $\bar{A} = \langle \bar{a} \rangle$ and $\bar{B} = \langle \bar{b} \rangle$. The hypothesis warrants that $G = AB$ and $\bar{G} = \bar{A}\bar{B}$ are minimal metacyclic factorizations by Proposition 2.7. In particular, $|A| = |\bar{A}| = m = m^G = m_{\bar{G}}$, $[G : A] = [\bar{G} : \bar{A}] = n = n^G = n_{\bar{G}}$, $[G : B] = [\bar{G} : \bar{B}] = s = s^G = s_{\bar{G}}$, $T = T_G(A)$ and $\bar{T} = T_{\bar{G}}(\bar{A})$.

(2) implies (3) Suppose that statement (2) holds. Then, using that $\pi(m) = \pi(m') = \pi(\bar{m}')$, we have $\operatorname{Res}_p(T) = \operatorname{Res}_p(\operatorname{Res}_{m'}(T)) = \operatorname{Res}_p(\operatorname{Res}_{m'}(\bar{T})) = \operatorname{Res}_p(\bar{T})$ for every prime p dividing m. Thus, $\pi' = \bar{\pi}'$ and, as $m_{\pi'} = m'_{\pi}$, we have $\operatorname{Res}_{m_{\pi'}}(T_{\pi'}) = \operatorname{Res}_{m'_{\pi'}}(T)_{\pi} = \operatorname{Res}_{m'_{\pi'}}(\bar{T})_{\pi} = \operatorname{Res}_{m_{\pi'}}(\bar{T}_{\pi'})$ and $\operatorname{Res}_{m_{\pi'}m'_p}(T_p) = \operatorname{Res}_{m'_{\pi' \cup \{p\}}}(T)_p = \operatorname{Res}_{m'_{\pi' \cup \{p\}}}(\bar{T})_p = \operatorname{Res}_{m_{\pi'}m'_p}(\bar{T}_p)$ for every $p \in \pi(m) \setminus \pi'$.

(1) implies (2). Suppose that $G \cong \bar{G}$. Then, as T and $\bar{T}$ are (n,s)-canonical they yield the same parameters, i.e. $\pi' = \bar{\pi}'$, $k = \bar{k}$, etc.

Let $f : \bar{G} \to G$ be an isomorphism and let $c = f(\bar{a})$, $d = f(\bar{b})$, $C = \langle c \rangle$ and $D = \langle d \rangle$. Then $C_{\pi'} = f(\bar{G}'_{\pi'}) = G'_{\pi'} = A_{\pi'}$, by Lemma 2.4.(3). Furthermore, $C_{\pi'}D_{\pi'} = A_{\pi'}B_{\pi'}$ because AB and $\bar{A}\bar{B}$ are the unique Hall π'-subgroup of G and $\bar{G}$, respectively. Then $\operatorname{Res}_{m_{\pi'}}(T) = T_G(A_{\pi'}) = T_G(C_{\pi'}) = \operatorname{Res}_{m_{\pi'}}(\bar{T})$. As $\operatorname{Res}_{m_\pi}(T_{\pi'}) = \operatorname{Res}_{m_\pi}(\bar{T}_{\pi'}) = 1$ it follows that $\operatorname{Res}_{m'}(T_{\pi'}) = \operatorname{Res}_{m'}(\bar{T}_{\pi'})$. Since T and $\bar{T}$ are cyclic, it remains to prove that $\operatorname{Res}_{m'}(T_p) =$

$\mathrm{Res}_{m'}(\bar{T}_p)$ for every $p \in \pi$. Moreover, as G and $\bar{G}$ have the same parameters ϵ and r we have $\mathrm{Res}_{m_p}(T_p) = \mathrm{Res}_{m_p}(\bar{T}_p) = \langle \epsilon^{p-1} + r_p \rangle_{m_p}$. Denote $R = \epsilon^{p-1} + r_p$ and select generators t of $\mathrm{Res}_{m_{\pi'} m'_p}(T_p)$ and $\bar{t}$ of $\mathrm{Res}_{m_{\pi'} m'_p}(T_p)$ such that $\mathrm{Res}_{m_p}(t) = \mathrm{Res}_{m_p}(\bar{t})[R]_{m_p}$. We already know that $\mathrm{Res}_{m'_{\pi'}}(T) = \mathrm{Res}_{m'_{\pi'}}(\bar{T})$ and in particular, there is an integer x coprime with p such that $\bar{t} = t^x \mod m_{\pi'}$. If $k_p \leq 2$ then $\mathrm{Res}_{m'_{\pi'}}(t) = \mathrm{Res}_{m'_{\pi'}}(\bar{t})$ and if $o_{m'_p}(R) \leq 2$ then $\mathrm{Res}_{m'_p}(t^x) = [R^x]_{m'_p} = [R]_{m_p} = \mathrm{Res}_{m'_p}(\bar{t})$. In both cases $\mathrm{Res}_{m_{\pi'} m'_p}(T) = \langle t \rangle = \langle t^x \rangle = \mathrm{Res}_{m_{\pi'} m'_p}(\bar{T})$, as desired. Therefore, in the remainder we may assume that both k_p and $o_{m'_p}(R)$ are greater than 2 and, in particular, $o_{m'_p}(R) = \frac{m'_p}{r_p} = \mathrm{Res}_{m'_p}(T)$ and this number coincides with the w in Lemma 2.8.

On the other hand $A_p B_p$ and $f(\bar{A}_p \bar{B}_p) = C_p D_p$ are Sylow p-subgroup of G and hence they are conjugate in G. Composing f with an inner automorphism of G we may assume that $C_p D_p = A_p B_p$. Then $\left\langle c, d^{k_p} \right\rangle = f(\left\langle \bar{a}, \bar{b}^{k_p} \right\rangle) = f(C_{\bar{G}_p}(\bar{G}'_{\pi'})) = C_{G_p}(G'_{\pi'}) = \left\langle a, b^{k_p} \right\rangle$. By Lemma 2.8 we have $d = b^y g$ for some $g \in C_{G_p}(G'_{\pi'})$ and $y \equiv 1 \mod w$. Thus $\mathrm{Res}_{m_{\pi'}}(\bar{t}) = \mathrm{Res}_{m_{\pi'}}(t^y)$ and $\mathrm{Res}_{m'_p}(\bar{t}) = \mathrm{Res}_{m'_p}(t) = \mathrm{Res}_{m'_p}(R) = \mathrm{Res}_{m'_p}(R^y) = \mathrm{Res}_{m'_p}(t^y)$, because $y \equiv 1 \mod o_{m'_p}(R)$. Thus $\mathrm{Res}_{m'_{\pi'} m'_p}(\bar{T}_p) = \mathrm{Res}_{m'_{\pi'} m'_p}(\bar{t}) = \mathrm{Res}_{m'_{\pi'} m'_p}(t^y) = \mathrm{Res}_{m'_{\pi'} m'_p}(T_p)$, as desired.

(3) implies (1) Suppose that the conditions of (3) holds. We may assume that $a = \bar{a}$ and take generators t of T and $\bar{t}$ of $\bar{T}$ so that $G = \langle a, b \rangle$, $\bar{G} = \left\langle a, \bar{b} \right\rangle$, with $|a| = m$, $[G : \langle a \rangle] = n$, $b^n = a^s$, $a^b = a^t$, $a^{\bar{b}} = a^{\bar{t}}$. Moreover, from the assumption we may assume $a^{b_{\pi'}} = a^{\bar{b}_{\pi'}}$ and for every $p \in \pi$ we have $\mathrm{Res}_{m_{\pi'} m'_p}(T_p) = \mathrm{Res}_{m_{\pi'} m'_p}(\bar{T}_p)$. In particular, for every $p \in \pi$, we have $\langle \epsilon^{p-1} + r_p \rangle_{m'_p} = \mathrm{Res}_{m'_p}(T_p) = \mathrm{Res}_{m'_p}(\bar{T}_p) = \langle \bar{\epsilon}^{p-1} + \bar{r}_p \rangle$. Since $r_p \mid m'_p \mid m_p$ it follows that $\epsilon = \bar{\epsilon}$ and $r_p = \bar{r}_p$. Thus $r = \bar{r}$.

We claim that for every $p \in \pi$ we can rewrite $G_p = \langle a_p, b_p \rangle$ as $G_p = \langle c_p, d_p \rangle$ with $c_p \in \left\langle a_p, b_p^{k_p} \right\rangle = C_{G_p}(a_{\pi'})$ and $d_p \in b^y C_{G_p}(a_{\pi'})$ such that $|c_p| = m_p$, $c_p^{d_p} = c_p^{R_p}$, $a_{\pi'}^{d_p} = a_{\pi'}^{\bar{b}_p}$ and $d_p^{n_p} = c_p^{s_p}$.

Indeed, let $p \in \pi$. The assumption $\left\langle \mathrm{Res}_{m_{\pi'} m'_p}(t_p) \right\rangle = \left\langle \mathrm{Res}_{m_{\pi'} m'_p}(\bar{t}_p) \right\rangle$ implies that there is an integer y coprime with $|\mathrm{Res}_{m_{\pi'} m'_p}(t_p)|$ such that $\mathrm{Res}_{m_{\pi'} m'_p}(\bar{t}_p) = \mathrm{Res}_{m_{\pi'} m'_p}(t_p)^y$. If $k_p \leq 2$ or $o_{m_p}(R) \leq 2$ then, as in the proof of (1) implies (2) we have that $\mathrm{Res}_{m_{\pi'} m_p}(t) = \mathrm{Res}_{m_{\pi'} m_p}(\bar{t})$ so that $c_p = a_p$ and $d_p = b_p$ satisfies the desired conditions. So assume that $k_p > 2$ and $o_{m_p}(R) > 2$. From the equality $a_p^{b_p} = a_p^{\bar{b}_p}$ we deduce that $R^y \equiv R \mod m'_p$ and this implies that $y \equiv 1 \mod w$ where $w = o_{m'_p}(R) = \frac{m'_p}{r_p}$ and again this w coincides with the one in

Lemma 2.8. Applying Lemma 2.8 we deduce that $\langle a_p, b_p\rangle$ contain elements $c_p \in \left\langle a_p, b_p^o\right\rangle = C_{G_p}(a_{\pi'})$ and $d_p \in b^y C_{G_p}(a_{\pi'})$ such that $\langle a_p, b_p\rangle = \langle c_p, d_p\rangle$, $|c_p| = m_p$, $a_{\pi'}^{d_p} = a_{\pi'}^{b_p^y} = a_{\pi'}^{\bar{b}_p}$, $c_p^{d_p} = c_p^{R_p}$ and $d_p^{n_p} = c_p^{s_p}$, as desired. This finishes the proof of the claim.

For every $p \in \pi$ let c_p and d_p as in the claim and set $c = a_{\pi'} \prod_{p\in\pi} c_p$ and $d = b_{\pi'} \prod_{p\in\pi} d_p$ we deduce that $G = \langle c, d\rangle$ with $|c| = m$, $d^n = c^s$ and $c^d = a^{\bar{t}}$. Therefore $G \cong \bar{G}$. □

The following corollary is a direct consequence (1) implies (2) of Theorem 2.9. It shows that Δ_G is well defined.

Corollary 2.10. *If $G = AB = CD$ are two minimal factorizations of G then $\Delta(AB) = \Delta(CD)$.*

2.3 Proofs of Theorems A, B and C

Proof of Theorem A. Let G and $\bar{G}$ be finite metacyclic groups and let $G = AB$ and $\bar{G} = \bar{A}\bar{B}$ be minimal metacyclic factorizations of G and $\bar{G}$ respectively. Denote $m = |A|$, $\bar{m} = |\bar{A}|$, $n = [G : A]$, $\bar{n} = [\bar{G} : \bar{A}]$, $s = [G : B]$, $\bar{s} = [\bar{G} : \bar{B}]$, $T = T_G(A)$ and $\bar{T} = T_{\bar{G}}(\bar{A})$. We also denote $m' = [T, n, s]$, $\bar{m}' = [\bar{T}, \bar{n}, \bar{s}]$, $\Delta = \text{Res}_{m'}(T)$ and $\bar{\Delta} = \text{Res}_{\bar{m}'}(\bar{T})$. Then $G \cong \mathcal{G}_{m,n,s,T}$, $\bar{G} \cong \mathcal{G}_{\bar{m},\bar{n},\bar{s},\bar{T}}$, $m = m^G$, $n = n^G$, $s = s^G$, $\bar{n} = n^{\bar{G}}$, $\bar{m} = m^{\bar{G}}$, $s = s^{\bar{G}}$, T is (n, s)-canonical and $\bar{T}$ is $(\bar{n}, \bar{s})$-canonical. Moreover, $\Delta = \Delta_G$ and $\bar{\Delta} = \Delta_{\bar{G}}$.

If $G \cong G'$ then $m = \bar{m}$, $n = \bar{n}$, $s = \bar{s}$ and, by Theorem 2.9 we have $\Delta = \bar{\Delta}$. Thus $\text{MCINV}(G) = \text{MCINV}(\bar{G})$.

Conversely, if $\text{MCINV}(G) = \text{MCINV}(\bar{G})$ then $m = |A| = m^G = m_{\bar{G}} = |\bar{A}| = \bar{m}$ and similarly $n = \bar{n}$ and $s = \bar{s}$. Moreover, $\text{Res}_{m'}[T] = \Delta_G = \Delta_{\bar{G}} = \text{Res}_{\bar{m}'}(\bar{T})$. Then $G \cong \bar{G}$ by Theorem 2.9. □

Proof of (1) implies (2) in Theorem B. Suppose that $(m, n, s, \Delta) = \text{MCINV}(G)$ for some metacyclic group G and let $G = AB$ be a minimal factorization of G. Then $m = m^G = |A|$, $n = n^G = [G : A]$, $s = s^G = [G : B]$ and if $T = T_G(A)$ then $\Delta = \Delta(AB) = \text{Res}_{m'}(T)$. In particular, $s \mid m$, T is a cyclic subgroup of $\mathcal{U}_m^{n,s}$, $[T] = [\Delta]$ and $m'_\nu = m_\nu$. Moreover, $\nu = \pi(m') \setminus \pi(r)$ and $s_\nu = m_\nu$, by Lemma 2.4. Moreover, $|\Delta|$ divides n, because it divides $|T|$, which in turn divides n. Then conditions (2a) and (2b) of Theorem B hold. By Lemma 2.2, Lemma 2.4 and Lemma 2.5 we have $\pi = \pi_G$, $\pi'_G = \nu$, $k = k^G$, $\epsilon = \epsilon^G$ and $r = r^G$. Let $p \in \pi(r)$. If $\epsilon^{p-1} = 1$ then $\frac{m_p}{r_p} = |\operatorname{Res}_{m_p}(T_p)| \le n_p$ and if $\epsilon = -1$ then $\max(2, \frac{m_2}{r_2}) = |\operatorname{Res}_{m_2}(T_2)| \le |T_2| \le n_2$ and $m_2 \le 2s_2$. As the metacyclic factorization $G = AB$ is minimal, T is (n, s)-canonical by Proposition 2.7. Then the remaining conditions in (2c) and (2d) follow. □

Proofs of Theorem C and (2) implies (1) in Theorem B. Suppose that m, n, s and Δ satisfy the conditions of (2) in Theorem B. By Remark 2.1 there is a cyclic subgroup T of $\mathcal{U}_m^{n,s}$ with $\operatorname{Res}_{m'}(T) = \Delta$ and $[T] = [\Delta]$. Let $t \in \mathbb{N}$ with $T = \langle t \rangle_m$. Let $G = \mathcal{G}_{m,n,s,t}$ and denote $A = \langle a \rangle$ and $B = \langle b \rangle$. We will prove that $G = AB$ is a minimal factorization of G that $m = |A|$, $n = [G : A]$, $s = [G : B]$ and $\Delta = \Delta(AB)$. This will complete the proofs of Theorem B and Theorem C.

Of course $G = AB$ is a metacyclic factorization of G and $T = T_G(A)$. Since $m_\nu = s_\nu$, n is multiple of $|\Delta|$ and $|\operatorname{Res}_{m_\nu}(T)| = |\operatorname{Res}_{m_\nu}(\Delta)|$, it follows that $|\operatorname{Res}_{m_\nu}(T)|$ divides n and $s(t-1)$. On the other hand if $p \mid r$ then $t \equiv \epsilon^{p-1} + r_p \mod m_p$. Therefore, if $\epsilon^{p-1} = 1$ then $o_{m_p}(t) = \frac{m_p}{r_p} \mid n$ and $s(t-1) \equiv s r_p \equiv 0 \mod m_p$. Otherwise, i.e. if $\epsilon = -1$ and $p = 2$, then $2 \mid |\Delta| \mid n$ and $\frac{m_2}{r_2} \le n_2$ and $m_2 \mid 2s$. Thus $o_{m_2}(t) = o_{m_2}(-1 + r_2) = \max(2, \frac{m_2}{r_2}) \le n_2$ and $m_2 \mid t(s-1)$. This shows that m divides both $t^n - 1$ and $s(t-1)$, i.e. $T \subseteq \mathcal{U}_m^{n,s}$. Then $|A| = m$ and $[G : A] = n$, and hence $[G : B] = s$. From condition (2b) we have that $\Delta = \operatorname{Res}_{m'}(T_G(A)) = \Delta(AB)$ and from conditions (2d) and (2c) it follows that T is (n, s)-canonical. Then the metacyclic factorization $G = AB$ is minimal by Proposition 2.7. □

Having in mind that a metacyclic group is nilpotent if and only if $k^G = 1$ one can easily obtain from Theorem B a description of the finite nilpotent metacyclic groups or equivalently the values of the lists of metacyclic invariants of the finite nilpotent metacyclic groups. Observe that (1) corresponds to cyclic groups, (2) to 2-generated abelian groups, (3) to non-abelian nilpotent metacyclic groups G with $\epsilon^G = 1$ and (4) to metacyclic nilpotent groups with $\epsilon^G = -1$.

Corollary 2.11. *Let $m, n, s \in \mathbb{N}$ and $t \in \mathbb{N} \cup \{0\}$. Then (m, n, s, t) is the list of metacyclic invariants of a finite metacyclic nilpotent group if and only if $s \mid m$, $t < m$*

and one of the following conditions hold:

(1) $m = 1$.

(2) $t = 1$ *and* $s = m \le n$.

(3) $\pi(t-1) = \pi(m)$, $\operatorname{lcm}\left(t-1, \frac{m}{t-1}\right) \mid s \mid n$ *and if* $4 \mid m$ *then* $4 \mid t-1$.

(4) *There is a divisor* r *of* $s_{2'}m_2$ *such that* $\pi(r) = \pi(m)$, $4 \mid r$, $t \equiv 1 + r_{2'} \mod m_{2'}$, $t \equiv -1 + r_2 \mod m_2$, $\frac{m_{2'}}{r_{2'}} \mid s_{2'} \mid n_{2'}$, $\max\left(2, \frac{m_2}{r_2}\right) \le n_2$, $m_2 \le 2s_2$ *and* $s_2 \ne n_2 r_2$. *If moreover* $4 \mid n$ *and* $8 \mid m$ *then* $r_2 \le s_2$.

In that case $\mathcal{G}_{m,n,s,t}$ *is nilpotent with metacyclic invariants* (m, n, s, t).

2.4 A GAP implementation

In this section we show how we can use the result in previous sections to construct some GAP functions for calculations with finite metacyclic groups.

The code of these functions and a brief manual are available in Ángel del Río's webpage and Github.

We start with two auxiliar functions. We call *metacyclic parameters* to any list (m, n, s, t) with $m, n, s \in \mathbb{N}$ and $[t]_m \in \mathcal{U}_m^{n,s}$, i.e. $s(t-1) \equiv t^n - 1 \mod m$. In that case, `MetacyclicGroupPC([m,n,s,t])` outputs the group $\mathcal{G}_{m,n,s,t}$ with a power-conjugation presentation. The boolean function `IsMetacyclic` returns `true` if the input is a finite metacyclic and `false` otherwise.

```
gap> G:=MetacyclicGroupPC([10,20,5,3]);
<pc group of size 200 with 5 generators>
gap> IsMetacyclic(G);
true
gap> Filtered([1..16],x->IsMetacyclic(SmallGroup(100,x)));
[ 1, 2, 3, 4, 5, 6, 8, 9, 14, 16 ]
```

To introduce the next function we start presenting an algorithm that uses Algorithm 1 to compute MCINV(G) for a given metacyclic group G. Observe that in Algorithm 1 the values of $m = |a|$, $n = [G : \langle a\rangle]$, $s = [G : \langle a\rangle]$ and $(r, \epsilon, k) = [T_G(\langle a\rangle)]$ are updated along the calculations. We use this in step (2) of the following algorithm.

Algorithm 2. ***Input:*** *A finite metacyclic group G.*
Output: MCINV(G).

(1) Compute a metacyclic factorization $G = AB$ of G.

(2) Perform Algorithm 1 with input (A, B) saving not only the output $(\langle a\rangle, \langle b\rangle)$ but also m, n, s, r, ϵ and o computed along.

(3) Compute m' using (1.4) and $t \in \mathbb{N}$ such that $a^b = a^t$.

(4) Return $(m, n, s, \mathrm{Res}_{m'}(\langle t\rangle_m))$.

A slight modification of Algorithm 2 allows the computation of the list of metacyclic invariants of a finite metacyclic group:

Algorithm 3. ***Input:*** *A finite metacyclic group G.*
Output: *The list of metacyclic invariants of G.*

(1) Compute a metacyclic factorization $G = AB$ of G.

(2) Perform Algorithm 1 with input (A, B) saving not only the output $(\langle a\rangle, \langle b\rangle)$ but also m, n, s, r and ϵ computed along.

(3) Compute m' using (1.4) and $t \in \mathbb{N}$ such that $a^b = a^t$ and set $\Delta := \mathrm{Res}_{m'}(\langle t\rangle_m)$.

(4) Use the Chinese Remainder Theorem to compute the unique $1 \le t \le m_{\pi(r)}$ such that $t \equiv \epsilon^{p-1} + r_p \mod m_p$ for every $p \in \pi(r)$.

(5) While $\gcd(t, m') \neq 1$ or $\langle t\rangle_{m'} \neq \Delta$, $t := t + m_{\pi(r)}$.

(6) Return (m, n, s, t).

Observe that $G = \langle a\rangle \langle b\rangle$ is a minimal metacyclic factorization at step (2) of Algorithm 3, and $m = m^G$, $n = n^G$ and $s = s^G$. At step (3), we have $T_G(\langle a\rangle) = \langle t\rangle_m$ and hence $G \cong \mathcal{G}_{m,n,s,t}$

and $\Delta = \Delta_G = \mathrm{Res}_{m'}(\langle t \rangle_m)$. However, this t is not t^G yet. The t at step Item 4 is the smallest one with $t \equiv \epsilon^{p-1} + r_p \mod m_p$ for every $p \in \pi(r)$ and the next steps search for the first integer t satisfying this condition as well as representing an element of $\mathcal{U}_m$ with $\mathrm{Res}_{m'}(\langle t \rangle_m) = \Delta$.

The GAP function `MetacyclicInvariants` implements Algorithm 3. For example in the following calculations one computes the metacyclic invariants of all the metacyclic groups of order 200.

```
gap> mc200:=Filtered([1..52],i->IsMetacyclic(SmallGroup(200,i)));;
gap> List(mc200,i->MetacyclicInvariants(SmallGroup(200,i)));
[[25,8,25,24],[1,200,1,0],[25,8,25,7],[100,2,50,99],[100,2,50,49],[100,2,100,99],
[50,4,50,49],[2,100,2,1],[4,50,4,3],[4,50,2,3],[50,4,50,7],[5,40,5,4],[5,40,5,1],
[5,40,5,2],[20,10,10,19],[20,10,10,9],[20,10,20,19],[10,20,10,9],[10,20,10,1],
[20,10,20,11],[20,10,10,11],[10,20,10,3]]
```

The GAP functions `MCINV` and `MCINVData` implement Algorithm 2 representing $\mathrm{MCINV}(G)$ in two different ways. While `MCINV(G)` outputs $\mathrm{MCINV}(G)$ if G is a metacyclic group, `MCINVData(G)` ouputs a 5-tuple `[m,n,s,m',t]` such that $\mathrm{MCINV}(G) = (m, n, s, \langle t \rangle_{m'})$. The input data `G` can be replaced by metacyclic parameters $[m, n, s, t]$ representing the group $\mathcal{G}_{m,n,s,t}$:

```
gap> G:=SmallGroup(384,533);
<pc group of size 384 with 8 generators>
gap> MetacyclicInvariants(G);
[ 8, 48, 4, 5 ]
gap> x:=MCINV(G);
[ 8, 48, 4, <group of size 1 with 1 generator> ]
gap> y:=MCINVData(G);
[ 8, 48, 4, 4, 1 ]
gap> x[4]=Group(ZmodnZObj(y[5],y[4]));
true
```

```
gap> H:=MetacyclicGroupPC([8,48,4,5]);
<pc group of size 384 with 8 generators>
gap> IdSmallGroup(H);
[ 384, 533 ]
gap> MetacyclicInvariants([20,4,8,11]);
[ 4, 20, 4, 3 ]
gap> MCINVData([20,4,8,11]);
[ 4, 20, 4, 4, 3 ]
```

Observe that two finite metacyclic groups G and H are isomorphic if and only if they have the same metacyclic invariants if and only if $\mathrm{MCINV}(G) = \mathrm{MCINV}(H)$. The function `AreIsomorphicMetacyclicGroups` uses this to decide if two metacyclic groups G and H are isomorphic. It outputs `true` if G and H are isomorphic finite metacyclic groups and `false` if they are finite metacyclic groups but they are not isomorphic. If one of the inputs is not a finite metacyclic group then the function fails. The input data `G` and `H` can be replaced by metacyclic parameters of them.

```
gap> H:=MetacyclicGroupPC([100,30,10,31]);
<pc group of size 3000 with 7 generators>
gap> K:=MetacyclicGroupPC([300,30,10,181]);
<pc group of size 9000 with 8 generators>
gap> AreIsomorphicMetacyclicGroups(H,K);
false
gap> AreIsomorphicMetacyclicGroups([300,10,10,31],K);
false
gap> G:=MetacyclicGroupPC([300,10,10,31]);
<pc group of size 3000 with 7 generators>
gap> MetacyclicInvariants(G);
[ 100, 30, 10, 31 ]
gap> MetacyclicInvariants(H);
[ 100, 30, 10, 31 ]
```

```
gap> MetacyclicInvariants(K);
[ 50, 180, 10, 31 ]
```

We now explain a method to compute all the metacyclic group of a given order N. We start producing all the tuples (m,n,s,r,ϵ,k) such that $\mathrm{MCINV}(G) = (m,n,s,\Delta)$ and $[\Delta] = (r,\epsilon,k)$ for some finite metacyclic group G and some cyclic subgroup Δ of $\mathcal{U}_{m'}$ with m' as in (1.4). For such group G we denote $\mathrm{IN}(G) = (m,n,s,r,\epsilon,k)$. The following lemma characterizes when a given tuple (m,n,r,s,r,ϵ,k) equals $\mathrm{IN}(G)$ for some finite metacyclic group:

Lemma 2.12. *Let $m,n,s,r,k \in \mathbb{N}$ and $\epsilon \in \{1,-1\}$ and let $\pi' = \pi(m) \setminus \pi(r)$ and $\pi = \pi(mn) \setminus \pi'$. Then $\mathrm{IN}(G) = (m,n,s,r,\epsilon,k)$ for some finite metacyclic group G if and only if the following conditions hold:*

(A) $s \mid m$, $r \mid m$, $k \mid n_\pi$, $m_\pi \mid rn$, $m_\pi \mid rs$, $s_{\pi'} = m_{\pi'}$ and if $4 \mid m$ then $4 \mid r$.

(B) If $p \in \pi(r)$ and $\epsilon^{p-1} = 1$ then $s_p \mid n$ and either $r_p \mid s$ or $s_p k_p \nmid n$.

(C) If $\epsilon = -1$ then $2 \mid n$, $4 \mid m$, $m_2 \mid 2s$, $s_2 \neq n_2 r_2$. If moreover $4 \mid n$, $8 \mid m$ and $k_2 < n_2$ then $r_2 \mid s$.

(D) $k \mid \mathrm{lcm}\{q-1 : q \in \pi'\}$ and for every $q \in \pi'$ with $\gcd(k,q-1) = 1$ there is $p \in \pi' \cap \pi(n)$ with $p \mid q-1$.

Proof. Suppose first that $(m,n,s,r,\epsilon,k) = \mathrm{IN}(G)$ for some finite metacyclic group G. Then $\mathrm{MCINV}(G) = (m,n,s,\Delta)$ for some cyclic subgroup Δ of $\mathcal{U}_{m'}$ with $[\Delta] = (r,\epsilon,k)$. Then the conditions in statement (2) of Theorem B hold and this implies that conditions (A)–(C) hold. To prove (D) we fix a metacyclic factorization $G = AB$ and observe that $k = k^G(A) = |\mathrm{Res}_{m_{\pi'}}(T_G(A))|$ and $\mathrm{Res}_{m_{\pi'}}(T_G(A))_\pi$ is a cyclic subgroup of $(\mathcal{U}_{m_{\pi'}})_\pi$. Then k divides $\exp((\mathcal{U}_{m_{\pi'}})_\pi)$ which is $\mathrm{lcm}\{(q-1)_\pi : q \in \pi'\}$. This proves the first part of (D). To prove the second one we take $q \in \pi'$ such that $\gcd(k,q-1) = 1$. By Lemma 2.4.(4), we have $\mathrm{Res}_q(T_G(A)) \neq 1$. However $\mathrm{Res}_q(T_G(A))_\pi \mid \gcd(k,q-1) = 1$ and hence, if p is a divisor of $\mathrm{Res}_q(T_G(A))$ then $p \mid |U_q| = q-1$, $p \mid [G:A] = n$ and $p \notin \pi$, so that $p \in \pi'$. This finishes the proof of (D).

Conversely, suppose that conditions (A)-(D) hold. By condition (D), $2 \notin \pi'$ and hence if $q \in \pi'$ then $\mathcal{U}_{m_q}$ is cyclic of order $\varphi(m_q)$. Therefore for every $q \in \pi'$, the group $\mathcal{U}_q$ contains a cyclic subgroup of order $q-1$. Therefore $\mathcal{U}_m$ contains a cyclic subgroup of order $o = \text{lcm}\{q-1 : q \in \pi'\}$. Furthermore, by (D), for every $p \in \pi$ we have that $k_p \mid o$ and hence $k_p \mid q-1$ for some $q \in \pi'$. Then $\mathcal{U}_{m_q}$ contains an element of order k_p and, as $\mathcal{U}_{m_{\pi'}} \cong \prod_{q \in \pi'} \mathcal{U}_{m_q}$, it follows that $\mathcal{U}_{m_{\pi'}}$ contains an element of order k. Let $\tau = \{q \in \pi' : \gcd(k, q-1) = 1\}$. By (D), for every $q \in \tau$ there is $p_q \in \pi' \cap \pi(n)$ such that $p_q \mid q-1$. Let $h = \prod_{q \in \tau} p_q$. For every $q \in \tau$, there is an element in $\mathcal{U}_{m_q}$ of order p_q. Then $\mathcal{U}_{m_\tau}$ has an element of order h. As $k \mid n_\pi$ and $h \mid n_{\pi'}$, $\mathcal{U}_{m_{\pi'}}$ has a cyclic subgroup S of order kh. Then $\text{Aut}(C_m)$ has a cyclic subgroup T such that $\text{Res}_{m_{\pi'}}(T) = S$ and $\text{Res}_{m_p}(T) = \text{Res}_{m_p}(T) = \langle \epsilon^{p-1} + r_p \rangle_{m_p}$ for every $p \in \pi$. By condition (B), if $p \in \pi(r)$ and $\epsilon^{p-1} = 1$ then $|\text{Res}_{m_p}(T)| = \frac{m_p}{r_p} \mid n_p$. By condition (C), if $\epsilon = -1$ then $2 \in \pi$, $2 \mid n$ and $\frac{m_2}{r_2} \mid n$ by (A). Thus $|\text{Res}_{m_p}(T)| = \max(2, \frac{m_2}{r_2}) \mid n$. Then $|\text{Res}_{m_p}(T)|$ divides n for every $p \in \pi$. This implies that $|T| = \text{lcm}(|S|, |\text{Res}_{m_p}(T)|, p \in \pi)$ and this number divides n. On the one hand we have $s_{p'} = m_{\pi'}$ and if $p \in \pi$ then either $m_p \mid rs$ or $p = 2$, $\epsilon = -1$ and $2m_2 \mid s$. Using this it is easy to see that $\text{Res}_{\frac{m}{s}}(T) = 1$. This proves that $T \subseteq \mathcal{U}_m^{n,s}$ and by the election of T it follows that $[T] = (r, \epsilon, k)$. Moreover, from conditions (B) and (C), it follows that T is (n,s)-canonical and hence $\mathcal{G}_{m,n,s,T} = \langle a \rangle \langle b \rangle$ is a minimal factorization. Thus $\text{IN}(\mathcal{G}_{m,n,s,T}) = (m, n, s, r, \epsilon, k)$, as desired. □

Our last algorithm is based in Lemma 2.12 and compute a list containing exactly one representative of each isomorphism class of the metacyclic groups of a given order.

Algorithm 4. ***Input:*** *A positive integer N.*

Output: *A list containing exactly one representative of each isomorphism class of the metacyclic groups of order N.*

```
(1) $M := [\,]$, an empty list, $\pi' := \pi(m) \setminus \pi(r)$, $\pi' := \pi(N) \setminus \pi'$.

(2) $P := \{(m, n, s, r, \epsilon, k) : n, m, s, r, k \in \mathbb{N}, \epsilon \in \{1, -1\}, N = mn$ and conditions (A)-(D) hold$\}$.

(3) For each $(m, n, s, r, \epsilon, k) \in P$:

    (a) $m' := m_{\pi'} \prod_{p \in \pi(r)} m'_p$ with $m'_p$ as in (1.4) and $s' := \frac{sm'}{m}$.
```

(b) For every cyclic subgroup Δ of $\mathcal{U}_{m'}^{n,s'}$ with $[\Delta] = (r, \epsilon, k)$:

- *Select a cyclic subgroup T of $\mathcal{U}_m$ such that $\mathrm{Res}_{m'}(T) = \Delta$.*
- *Add $\mathcal{G}_{m,n,s,T}$ to the list M.*

(4) Return the list M.

Observe that if $(m, n, s, r, \epsilon, k)$ satisfy conditions (A)-(D) then m divides sm'. Indeed, if $p \nmid r$ then $m_p = m'_p$. If $\epsilon = -1$ then $\frac{m_2}{2}$ divides s and $2 \mid m'$, hence in this case $\frac{m_2}{s_2} \mid m'$. Finally, if $p \in \pi(r)$ and $\epsilon^{p-1} = 1$. Then $p \in \pi$ and hence $m_p \le r_p s_p$ by condition (A). Therefore $\frac{m_p}{s_p} \le \min(m_p, r_p k_p)$. If $r_p \mid s_p$ then also $\frac{m_p}{s_p} \le s_p$. Otherwise $s_p k_p \nmid n$ and hence $r_p \frac{s_p k_p}{n_p} > r_p \ge \frac{m_p}{s_p}$. This proves that $\frac{m_p}{s_p} \mid m'$ for every prime p, so that $m \mid sm'$, as desired. This justify that $s' \in \mathbb{N}$ is step (3a).

On the other hand if T is as in (3b) then $T \subseteq \mathcal{U}_m^{n,s}$. Indeed, $\frac{m}{s} = \frac{m'}{s'}$ and hence $\mathrm{Res}_{\frac{m}{s}}(T) = \mathrm{Res}_{\frac{m'}{s'}}(\Delta) = 1$. Moreover $\mathrm{Res}_{m_{\pi'}}(T) = \mathrm{Res}_{m'_{\pi'}}(\Delta)$ and hence $|\mathrm{Res}_{m_{\pi'}}(T)|$ divides n. On the other hand $[T] = (r, \epsilon, k) = [T]$ and hence if $\epsilon^{p-1} = 1$ then $|\mathrm{Res}_{m_p}(T)| = \frac{m_p}{r_p} \mid n$, by (A). Otherwise $|\mathrm{Res}_{m_2} T_2| = \max(2, \frac{m_2}{r_2})$ which divides n by (A) and (C).

The function `MetacyclicGroupsByOrder(N)` implements a combination of Algorithm 3 and Algorithm 4 and returns the complete list of metacyclic invariants of metacyclic groups of order N.

```
gap> MetacyclicGroupsByOrder(200);
[[1,200,1,0],[2,100,2,1],[4,50,2,3],[4,50,4,3],[5,40,5,1],[5,40,5,2],[5,40,5,4],
[10,20,10,1],[10,20,10,3],[10,20,10,9],[20,10,10,9],[20,10,10,11],[20,10,10,19],
[20,10,20,11],[20,10,20,19],[25,8,25,7],[25,8,25,24],[50,4,50,7],[50,4,50,49],
[100,2,50,49],[100,2,50,99],[100,2,100,99]]
gap> MetacyclicGroupsByOrder(8*3*5*7);
[[1,840,1,0],[2,420,2,1],[3,280,3,2],[4,210,2,3],[4,210,4,3],[5,168,5,2],[5,168,5,4],
[6,140,6,5],[7,120,7,2],[7,120,7,6],[7,120,7,3],[10,84,10,3],[10,84,10,9],[12,70,6,5]
[12,70,6,11],[12,70,12,11],[14,60,14,3],[14,60,14,9],[14,60,14,13],[15,56,15,2],
[15,56,15,14],[20,42,10,9],[20,42,10,19],[20,42,20,19],[21,40,21,20],[28,30,14,3],
[28,30,14,5],[28,30,14,11],[28,30,14,13],[28,30,14,27],[28,30,28,3],[28,30,28,11],
[28,30,28,27],[30,28,30,17],[30,28,30,29],[35,24,35,2],[35,24,35,3],[35,24,35,4],
[35,24,35,13],[35,24,35,19],[35,24,35,34],[42,20,42,41],[60,14,30,29],[60,14,30,59],
[60,14,60,59],[70,12,70,3],[70,12,70,9],[70,12,70,13],[70,12,70,19],[70,12,70,23],
[70,12,70,69],[84,10,42,41],[84,10,42,83],[84,10,84,83],[105,8,105,62],[105,8,105,104
[140,6,70,9],[140,6,70,19],[140,6,70,39],[140,6,70,69],[140,6,70,89],[140,6,70,139],
[140,6,140,19],[140,6,140,39],[140,6,140,139],[210,4,210,83],[210,4,210,209],
[420,2,210,209],[420,2,210,419],[420,2,420,419]]
```

CHAPTER 3

The Nilpotent Case

In this chapter we are going to prove that the Isomorphism Problem (1.5) has a positive answer when the groups are nilpotent and $R = \mathbb{Q}$. In fact we prove the stronger result:

> **Theorem D.** *Let G and H be a metacyclic finite groups such that $\mathbb{Q}G \cong \mathbb{Q}H$. Then $\pi_G = \pi_H$ and the Hall π_G-subgroups of G and H are isomorphic.*

As a direct consequence of Theorem D we obtain the following:

> **Corollary E.** *If G and H are finite metacylic groups with $\mathbb{Q}G \cong \mathbb{Q}H$ and G is nilpotent then $G \cong H$.*

In Section 3.1 we introduce some chapter-specific notation and review some known results. Suppose that G and H are finite metacyclic groups such that $\mathbb{Q}G$ and $\mathbb{Q}H$ are isomorphic. In Section 3.2 we prove that if G and H are p-groups then they are isomorphic. In Section 3.3 we prove Theorem D. The results of this chapter are contained in [GBdR23b].

3.1 Introduction

Observe that in Theorem D and Corollary E it is not sufficient to assume that only one of the two groups G or H is metacyclic:

Example 3.1. *The following groups:*

$$\left\langle a,b|a^{p^2}=b^p=1,a^b=a^{1+p}\right\rangle, \quad \langle a,b|a^p=b^p=[b,a]^p=[a,[b,a]]=[b,[b,a]]=1\rangle$$

have isomorphic rational group algebras while the first is metacyclic and the second is not.

We will need the following formula:

$$\begin{aligned}\sum_{d=0}^{n} d2^d &= \sum_{d=0}^{n}\sum_{i=0}^{d-1} 2^d = \sum_{i=0}^{n-1} 2^{i+1}\sum_{d=i+1}^{n} 2^{d-i-1} = \sum_{i=0}^{n-1} 2^{i+1}\sum_{j=0}^{n-i-1} 2^j = \sum_{i=0}^{n-1} 2^{i+1}(2^{n-i}-1) \\ &= n2^{n+1} - 2\sum_{i=0}^{n-1} 2^i = n2^{n+1} - 2(2^n-1) = (n-1)2^{n+1}+2\end{aligned} \tag{3.1}$$

Recall that if $R,n\in\mathbb{N}$ with $\gcd(R,n)=1$ and $i\in\mathbb{Z}$ then the R-cyclotomic class modulo n containing i is the subset of $\mathbb{Z}$ formed by the integers j such that $j\equiv iR^k \mod n$ for some $k\geq 0$. The R-cyclotomic classes module n form a partition of $\mathbb{Z}$ and each R-cyclotomic class modulo n is a union of cosets modulo n. More precisely, if i and j belong to the same R-cyclotomic class then $\gcd(n,i)=\gcd(n,j)$ and if $d=\frac{n}{\gcd(n,i)}$ then the R-cyclotomic class module n containing i is the disjoint union of $i+n\mathbb{Z}, iR+n\mathbb{Z},\dots,iR^{o_d(R)-1}+n\mathbb{Z}$. Therefore the number of R-cyclotomic classes module n is

$$C_{R,n}=\sum_{d|n}\frac{\varphi(d)}{o_d(R)}. \tag{3.2}$$

We will need a precise expression of this number for the case where n is a power of p and $R\equiv 1 \mod p$.

Lemma 3.2. *Let p be a prime and $R, m \in \mathbb{N}$ with $R \equiv 1 \mod p$. Then the number of R-cyclotomic classes modulo p^m is*

$$C_{R,p^m} = \begin{cases} p^m, & \textit{if } m \le v_p(R-1); \\ 1 + 2^{m-1}, & \textit{if } p = 2 \textit{ and } 2 \le m < v_2(R+1); \\ 1 + 2^{v_2(R+1)-1}(1 + m - v_2(R+1)), & \textit{if } p = 2 \textit{ and } 2 \le v_2(R+1) \le m; \\ p^{v_p(R-1)-1}(p + (p-1)(m - v_p(R-1))), & \textit{otherwise.} \end{cases}$$

Proof. If $m \le v_p(R-1)$ then $o_d(R) = 1$ for every divisor d of m and hence every R-cyclotomic class module p^m is formed by one coset modulo p^m. Therefore, in that case $C_{R,p^m} = p^m$. Suppose otherwise that $m > v_p(R-1)$.

Suppose that either p is odd or $p = 2$ and $R \equiv 1 \mod 4$. Using Lemma 1.1.(1b) and (3.2) we have

$$\begin{aligned} C_{R,p^m} &= \sum_{k=0}^{m} \frac{\varphi(p^k)}{p^{\max(0,k-v_p(R-1))}} = 1 + (p-1)\left(\sum_{k=1}^{v_p(R-1)} p^{k-1} + \sum_{k=v_p(R-1)+1}^{m} p^{v_p(R-1)-1}\right) \\ &= p^{v_p(R-1)} + (p-1)(m - v_p(R-1))p^{v_p(R-1)-1} = p^{v_p(R-1)-1}(p + (p-1)(m - v_p(R-1))) \end{aligned}$$

Otherwise, $p = 2$ and $R \equiv -1 \mod 4$. Then $2 \le v_2(R+1)$ and $1 = v_2(R-1) < m$. Using now Lemma 1.1.(2b) and (3.2) we have $C_{R,2^m} = 2 + \sum_{k=2}^{m} \frac{\varphi(2^k)}{2^{\max(1,k-v_2(R+1))}}$ Thus, if $m < v_2(R+1)$ the $C_{R,2^m} = 2 + \sum_{k=2}^{m} 2^{k-2} = 1 + 2^{m-1}$. Otherwise, i.e. if $m \ge v_2(R+1)$ then

$$\begin{aligned} C_{R,2^m} &= 2 + \sum_{k=2}^{v_2(R+1)} 2^{k-2} + \sum_{k=v_2(R+1)+1}^{m} 2^{v_2(R+1)-1} = 1 + 2^{v_2(R+1)-1} + (m - v_2(R+1))2^{v_2(R+1)-1} \\ &= 1 + 2^{v_2(R+1)-1}(1 + m - v_2(R+1)). \end{aligned}$$

□

Another tool that we want to introduce in this section is the classification of finite metacyclic p-groups. The finite metacyclic groups were classified by Hempel [Hem00]. Previously the finite metacyclic p-groups were classified by several means [Zas99, Lin71, Hal59, Bey72, Kin73, Lie96, Lie94, NX88, Réd89, Sim94]. For our purpose we need the description of the finite metacyclic groups in terms of group invariants given in [GBdR23a] for the special case of p-groups. More precisely when Theorem B is specialized to finite metacyclic p-groups one obtains the following:

Theorem 3.3. *Let p be a prime integer. Then every finite metacyclic p-group is isomorphic to a group given by the following presentation*

$$\mathcal{P}_{p,\mu,\nu,\sigma,\rho,\epsilon} = \left\langle a, b \mid a^{p^\mu} = 1, b^{p^\nu} = a^{p^\sigma}, a^b = a^{\epsilon + p^\rho} \right\rangle .$$

for unique non-negative integers μ, ν, σ and ρ and a unique $\epsilon \in \{1, -1\}$ satisfying the following conditions:

(A) $\rho \leq \mu$, if $\mu \geq 1$ then $\rho \geq 1$ and if $p = 2$ and $\mu \geq 2$ then $\rho \geq 2$.

(B) If $\epsilon = 1$ then $\rho \leq \sigma \leq \mu \leq \rho + \sigma$ and $\sigma \leq \nu$.

(C) If $\epsilon = -1$ then

(a) $p = 2 \leq \rho \leq \mu$, $\nu \geq 1$, $\mu - 1 \leq \sigma \leq \mu \leq \rho + \nu \neq \sigma$ and

(b) if $2 \geq \nu$ and $3 \geq \mu$ then $\rho \leq \sigma$,

Proof. Let G be a finite metacyclic p-group for a prime p. By Theorem B: $G = AB$, where $G = AB$ is a minimal metacyclic factorization, and $\mathrm{MCINV}(G) = (m, n, s, \Delta)$, where $m = |A|$, $n = [G : A]$, $s = [G : B]$ and $\Delta = \Delta(AB)$. As G is a p-group, this means that m, n and s are powers of p, so we write $m = p^\mu$, $n = p^\nu$ and $s = p^\sigma$. In addition, $[T_G(A)] = (r, \epsilon, k)$ (we write $T = T_G(A)$ from this point on). In particular r is the greatest divisor of m such that $\mathrm{Res}_{r_2'}(T) = 1$ and $\mathrm{Res}_{r_2}(T) \subseteq \langle -1 \rangle_{r_2}$, so we can write $r = p^\rho$ and we have proven (A). We also know that $k = |\mathrm{Res}_{m_\nu}(T)|$, with $\nu = \pi(m) \setminus \pi(n)$, but using (A) we see that $\nu = 1$ and $k = 1$. Using this on (1.4) leads to $m_p' = r_p$. In any case, we see that the group can be given the presentation $G = \left\langle a, b \mid a^{p^\mu} = 1, b^{p^\nu} = a^{p^\sigma}, a^b = a^{\epsilon + p^\rho} \right\rangle$. From Theorem B.(2a) and Theorem B.(2d), we obtain $s \leq m$, $m_p/r_p \leq s_p \leq n_p$ and if $r_p > s_p$ then $n_p < k_p s_p$. The statement (B) comes directly from this, using $o = 1$. If $\epsilon = -1$ then, by the definition of ϵ, $p = 2$. Using Theorem B.(2a) we get $\sigma \leq \mu$. Finally, the rest of the statement of (C) comes directly from Theorem B.(2c). □

3.2 ISO for finite metacyclic p-groups

In this section p is a prime and we prove that the Isomorphism Problem for rational group algebras has positive solution for finite metacyclic p-groups.

All throughout G is a finite metacyclic p-group. By Theorem 3.3, $G \cong \mathcal{P}_{p,\mu,\nu,\sigma,\rho,\epsilon}$ for unique non-negative integers μ, ν, σ and ρ and unique $\epsilon \in \{1, -1\}$ satisfying conditions (A)-(C) of Theorem 3.3. For the rest of the section, when we refer to (A)-(C) we mean that of Theorem 3.3.

The strategy for the proof of the main result of this sections relies in 4 invariants from the group that can be found in the group ring. One of them is the size of the group, which can be seen as the dimension of the group ring. Another one is the isomorphism class of the commutator of the group: $\mathbb{Q}(G/G')$ is isomorphic to the direct sum of the commutative Wedderburn components of $\mathbb{Q}G$; and by Theorem 1.12 two non-isomorphic abelian finite groups have non-isomorphic rational group algebras. The third invariant is the number of conjugacy classes, which it is well-known that it is the dimension of the center over $\mathbb{Q}$. Lastly, by Theorem 1.11, the number of $\mathbb{Q}$-characters of $\mathbb{Q}G$ equals the number of conjugacy classes of cyclic subgroups of G. Originally we tried to determine each metacyclic p-group which these 4 invariants, but examples like Example 3.7 prove it wrong.

The proof of the main result of this section relies in five technical lemmas, three of them consist in computing the mentioned invariants and the last two deal with the isolated remaining cases. As we said, one of the main tools in the proof consists on using Theorem 1.11. If two groups have isomorphic rational group algebras we know that the number of conjugacy classes of cyclic subgroups are the same. In this train of thought, in the first lemma we find some conditions to establish when two subgroups of G are conjugate.

Lemma 3.4. *Suppose that $\epsilon = 1$ and $\mu > 0$. Let $0 \leq d < \nu$ and for every $1 \leq i \leq p^\mu$ set*

$$l_i = \begin{cases} 2^\sigma + i(2^{\nu-d} + 2^{\mu-1}), & \text{if } p = 2 \nmid i \text{ and } \mu = \nu + \rho; \\ p^\sigma + ip^{\nu-d}, & \text{otherwise}, \end{cases}$$

$$k_i = \min(\mu, v_p(l_i)) \quad \text{and} \quad h_i = \min(k_i, \rho + d, \rho + v_p(i)).$$

Then $\left\langle b^{p^d}a^i\right\rangle$ *and* $\left\langle b^{p^d}a^j\right\rangle$ *are conjugate in* G *if and only if* $i \equiv j \mod p^{h_i}$. *In that case,* $k_i = k_j$ *and* $h_i = h_j$.

Proof. As $\mu > 0$, by condition (A), we also have $\rho > 0$. Let $R = 1 + p^\rho$. By Lemma 1.1.(1a) we have $v_p(R^{p^d} - 1) = d + \rho$ and by condition (B) we have $\mu - (d + \rho) \leq \nu - d$. Hence, applying Lemma 1.1.(1d) with $a = d + \rho$ and $m = \nu + \rho > a$ we obtain the following for every $k \in \mathbb{N}$:

$$\mathcal{S}\left(R^{p^d} \mid kp^{\nu-d}\right) = \begin{cases} k2^{\nu+d} + k2^{\nu+\rho-1} \mod 2^{\nu+\rho}, & \text{if } p = 2; \\ kp^{\nu+\rho}, & \text{if} p \neq 2 \end{cases}$$

Then

$$\mathcal{S}\left(R^{p^d} \mid kp^{\nu-d}\right) \equiv \begin{cases} k2^{\nu-d} + k2^{\mu-1} \mod 2^{\mu}, & \text{if } p = 2, \text{ and } \mu = \nu + \rho; \\ kp^{\nu-d} \mod p^{\mu}, & \text{otherwise.} \end{cases} \tag{3.3}$$

Moreover $a^{b^{p^d}} = a^{R^{p^d}}$ and hence, by Equation (1.1) we have

$$(b^{p^d}a^i)^{p^{\nu-d}} = b^{p^\nu}a^{i\mathcal{S}\left(R^{p^d}|p^{\nu-d}\right)} = a^{p^\sigma+i\mathcal{S}\left(R^{p^d}|p^{\nu-d}\right)} = a^{l_i}. \tag{3.4}$$

Suppose that $\left\langle b^{p^d}a^i\right\rangle$ and $\left\langle b^{p^d}a^j\right\rangle$ are conjugate in G. Then there are integers x, y, u with $p \nmid u$ such that $b^{p^d}a^j = ((b^{p^d}a^i)^u)^{b^y a^x}$. In particular $b^{p^d}\langle a\rangle = b^{up^d}\langle a\rangle$ and therefore $u \equiv 1 \mod p^{\nu-d}$. Write $u = 1 + vp^{\nu-d}$. Then

$$(b^{p^d}a^i)^u = b^{p^d}a^i(b^{p^d}a^i)^{vp^{\nu-d}} = b^{p^d}a^{i+vl_i}$$

Hence

$$b^{p^d}a^j = (b^{p^d}a^{i+vl_i})^{b^y a^x} = b^{p^d}a^{(i+vl_i)R^y+x(1-R^{p^d})}.$$

On the other hand, $R^y = 1 + Yp^\rho$ for some integer Y. Then

$$j \equiv i + iYp^\rho + vl_iR^y + x(1 - R^{p^d}) \equiv i \mod p^{h_i}$$

because $h_i = \min(k_i, \rho + d, r + v_p(i)) = \min(\mu, v_p(l_i), v_p(1 - R^{p^d}), \rho + v_p(i))$.

Conversely suppose that $j \equiv i \mod p^{h_i}$ and consider the four possibilities for h_i separately. Of course if $h_i = \mu$ then $b^{p^d}a^i = b^{p^d}a^j$. Suppose that $h_i = \rho + d$. Then $h_i = v_p(1 - R^{p^d})$, by Lemma 1.1.(1a). Therefore there is an integer x such that $j \equiv i + x(1 - R^{p^d}) \mod p^\mu$ and hence $(b^{p^d}a^i)^{a^x} = b^{p^d}a^{i+x(1-R^{p^d})} = b^{p^d}a^j$. Assume that $h_i = k_i = v_p(l_i)$. Then $j \equiv i + vl_i \mod p^\mu$ for some $v \in \mathbb{N}$. Hence using (3.4) we have $(b^{p^d}a^i)^{1+vp^{\nu-d}} = b^{p^d}a^{i+vl_i} = b^{p^d}a^j$. Finally, suppose that $h_i = \rho + v_p(i)$. Then there is an integer z such that $j \equiv i + zip^\rho \mod p^\mu$. Moreover, by Lemma 1.1.(1c), there is a non-negative integer y such that $R^y \equiv 1 + zp^\rho$. Then $(b^{p^d}a^i)^{b^y} = b^{p^d}a^{iR^y} = b^{p^d}a^{i(1+zp^\rho)} = b^{p^d}a^j$.

For the last part, suppose that $\left\langle b^{p^d}a^i \right\rangle$ and $\left\langle b^{p^d}a^j \right\rangle$ are conjugate in G. Then, from (3.4) we have $p^{\nu-d+\mu-k_i} = |b^{p^d}a^i| = |b^{p^d}a^j| = p^{\nu-d+\mu-k_j}$, so that $k_i = k_j$. Suppose that $h_i \neq h_j$. Then necessarily $v_p(i) \neq v_p(j)$ and, as $j \equiv i \mod p^{h_i}$, we have $h_i \leq v_p(i) < \rho + v_p(i)$. Interchanging the roles of i and j we also obtain $h_j \leq v_p(j) < \rho + v_p(j)$. So that $h_i = \min(k_i, \rho + d) = \min(k_j, \rho + d) = h_j$, a contradiction. □

In the following lemma we compute the number of conjugacy classes of cyclic subgroups of a finite metacyclic p-group when $\epsilon = 1$.

Lemma 3.5. *If $\epsilon = 1$ then the number of conjugacy classes of cyclic subgroups of G is $N = A_\sigma + A$ where*

$$\begin{aligned} A_\sigma &= p^{\rho-1}\sigma\left(1 + (p-1)\frac{1+2\nu-\sigma}{2}\right) - \frac{p^{\rho+\sigma-\mu}}{p-1} \quad \textit{and} \\ A &= \frac{3p^{\rho-1}-2}{p-1} + p^{\rho-1}\frac{6-\rho+2\nu\rho-\rho^2+p(\rho^2+2\nu-3\rho-2\nu\rho+2)}{2} \end{aligned}$$

Proof. For every $0 \leq d \leq \nu$ we let $\mathcal{C}_d$ denote the set of cyclic subgroups C of G satisfying $[C\langle a\rangle : \langle a\rangle] = p^{\nu-d}$. Clearly $\mathcal{C}_d$ is closed by conjugation in G. We let N_d denote the number of conjugacy classes of cyclic subgroups of G belonging to $\mathcal{C}_d$. Then the number of conjugacy classes of subgroups of G is $\sum_{d=0}^{\nu} N_d$. For every $1 \leq i \leq p^\mu$ we will use the notation l_i, k_i and h_i introduced in Lemma 3.4.

As $G/\langle a\rangle$ is cyclic of order p^ν, every element of $\mathcal{C}_d$ is formed by the groups of the form $\left\langle b^{p^d}a^i \right\rangle$ with $1 \leq i \leq p^\mu$. In particular $N_\nu = \mu + 1$, the number of subgroups of $\langle a\rangle$.

From now on we assume that $0 \leq d < \nu$.

Claim 1. If $v_p(i) \geq \min(\sigma, \rho + d)$ then $\left\langle b^{p^d}a^i \right\rangle$ is conjugate to $\left\langle b^{p^d} \right\rangle$ in G.

Indeed, suppose that $v_p(i) \geq \min(\sigma, \rho + d)$. By Lemma 3.4 we have to prove that

$i \equiv 0 \mod p^{h_i}$, i.e. $h_i \leq v_p(i)$. First of all observe that $v_p(i) \geq \min(\sigma, \rho + d) \geq 1$, because $1 \leq \rho \leq \sigma$. Hence $l_i = p^\sigma + ip^{\nu-d}$. If $v_p(ip^{\nu-d}) > \sigma$ then $v_p(l_i) = s$ and hence $h_i = \min(\sigma, \rho + d, \rho + v_p(i)) = \min(\sigma, \rho + d) \leq v_p(i)$, as desired. Suppose otherwise that $v_p(ip^{\nu-d}) \leq \sigma$. Then $v_p(i) < v_p(ip^{\nu-d}) \leq \sigma$ and hence, by hypothesis $\rho + d \leq v_p(i)$. Then, by condition (B) of Theorem 3.3 we have $v_p(ip^{\nu-d}) \geq \rho + \nu \geq \mu \geq \sigma \geq v_p(ip^{\nu-d})$. Therefore $v_p(ip^{\nu-d}) = \rho + \nu = \mu = \sigma$ and $v_p(i) = \rho + d < \sigma$. Then $h_i = \min(\sigma, \rho + d) = \rho + d \leq v_p(i)$, again as desired.

Claim 2. If $1 \leq i, j \leq p^\mu$, $v_p(i) < \min(\sigma, \rho + d)$ and $\left\langle b^{p^d} a^i \right\rangle$ and $\left\langle b^{p^d} a^j \right\rangle$ are conjugate in G then $v_p(i) = v_p(j)$.

Indeed, by Lemma 3.4 we have $h_i = h_j$, which we denote h, and $i \equiv j \mod p^h$. By means of contradiction suppose that $v_p(i) \neq v_p(j)$. Then $h \leq \min(v_p(i), v_p(j)) \leq v_p(i) < \min(\sigma, \rho + d)$ and therefore $\min(\mu, v_p(l_j), \rho + d) = \min(\mu, v_p(l_i), \rho + d) = h < \min(\sigma, \rho + d)$. Thus $v_p(l_i) = v_p(l_j) = h \leq \min(v_p(i), v_p(j))$. However $v_p(ip^{\nu-d}) > v_p(i)$ and if $p = 2 \neq i$ then $v_2(i(2^{\nu-d} + 2^{\mu-1})) > v_2(i)$. Therefore $v_p(l_i - p^\sigma) > v_p(i) \geq h = v_p(l_i)$. Then $h = v_p(l_j) = v_p(l_i) = \sigma \geq \min(\sigma, \rho + d)$, a contradiction.

We use Claims 1 and 2 and Lemma 3.4 as follows: For every $0 \leq h < \min(\sigma, \rho + d)$ let

$$X_h = \{i \in \mathbb{Z} : 1 \leq i \leq p^\mu \text{ and } v_p(i) = h\}$$

and consider the equivalence relation in X_h given by

$$i \sim_d j \text{ if and only if } k_i = k_j (= k) \text{ and } i \equiv j \mod p^{\min(k, \rho+d, \rho+h)}.$$

Let $N_{d,h}$ be the number of $\sim_d$-equivalence classes in X_h. By Lemma 3.4 and Claim 2, if $i \in X_h$, $1 \leq j \leq p^\mu$, $v_p(i) < \min(\sigma, \rho + d)$ and $\left\langle b^{p^d} a_i \right\rangle$ and $\left\langle b^{p^d} j \right\rangle$ are conjugate in G then $j \in X_h$ and i and j belong to the same $\sim_d$-class. Therefore, using also Claim 1 we have

$$N_d = 1 + \sum_{h=0}^{\min(\sigma,\rho+d)-1} N_{d,h}. \tag{3.5}$$

Our next goal is obtaining a formula for $N_{d,h}$ and for that we consider three cases:

Case 1: Suppose that $d \leq \nu - \rho$.

Let $h \in X_h$. We claim that $k_i = \min(\sigma, \rho + d, \rho + h)$. This is clear if $v_p(l_i) = \sigma$. Suppose that $v_p(l_i) > \sigma$. Then $v_p(l_i - p^\sigma) = \sigma$. If $h = 0$ then, as $\rho \leq \sigma$ we have $k_i = \rho = \min(\sigma, \rho +$

$d, \rho+h)$ as desired. Otherwise $l_i - p^\sigma = ip^{\nu-d}$, so that $h+\nu-d=\sigma$ and, by assumption we have $\rho+h = \rho+d-\nu+\sigma \leq \sigma$. Then again $k_i = \min(\sigma, \rho+d, \rho+h)$. Finally, suppose that $v_p(l_i) < \sigma$. Then $v_p(l_i - p^\sigma) = v_p(l_i)$. If $l_i - p^\sigma = ip^{\nu-d}$ then $h+\rho \leq h+\nu-d = v_p(l_i) < \sigma \leq \mu$ and hence $k_i = \min(\rho+d, \rho+h) = \min(\sigma, \rho+d, \rho+h)$. Otherwise $p=2$, $h=0$, $\mu = \nu+\rho$ and $l_i - 2^\sigma = i(2^{\nu-d} + 2^{\mu-1})$. Then $\mu \geq \sigma > v_2(l_i) = v_2(2^{\nu-d}+2^{\mu-1}) \geq \nu - d \geq \rho = \rho+h$, because $\nu - d = \mu-\rho-d \leq \mu-\rho \leq \mu-1$. Then $k_i = \rho = \min(\sigma, \rho+d, \rho+h)$. So all the cases $k_i = \min(\sigma, \rho+d, \rho+h)$, as desired.

Combining Lemma 3.4 with the claim in the previous paragraph we deduce that for $d \leq \nu-\rho$ and $h < \min(\sigma, \rho+d)$, the $\sim_d$-equivalence classes of X_h have $p^{\mu - \min(\sigma,\rho+d,\rho+h)}$ elements. Thus for each $d \leq \nu-\rho$ and $0 \leq h < \min(\sigma, \rho+d)$ we have

$$N_{d,h} = \frac{\varphi(p^{\mu-h})}{p^{\mu-\min(\sigma,\rho+d,\rho+h)}} = (p-1)p^{\min(\sigma,\rho+d,\rho+h)-h-1}$$

As, by Claim 1, for a fixed $d \mid \mu$, all the cyclic groups $\left\langle b^{p^d} a^i \right\rangle$ with $v_p(i) \geq \min(\sigma, \rho+d)$ are conjugate we have

$$\begin{aligned}
&\sum_{d=0}^{\nu-\rho} N_d = \sum_{d=0}^{\nu-\rho}\left(1 + \sum_{h=0}^{\min(\sigma,\rho+d)-1} N_{d,h}\right) = \sum_{d=0}^{\sigma-\rho}\left(1+\sum_{h=0}^{d-1}(p-1)p^{\rho-1} + \sum_{h=d}^{d+\rho-1}(p-1)p^{\rho+d-h-1}\right) \\
&+ \sum_{d=\sigma-\rho+1}^{\nu-\rho}\left(1+\sum_{h=0}^{\sigma-\rho-1}(p-1)p^{\rho-1} + \sum_{h=\sigma-\rho}^{\sigma-1}(p-1)p^{\sigma-h-1}\right) = (\nu-\rho+1) + \\
&\sum_{d=0}^{\sigma-\rho}\left(d(p-1)p^{\rho-1} + (p-1)\sum_{x=0}^{\rho-1}p^x\right) + \sum_{d=\sigma-\rho+1}^{\nu-\rho}\left((\sigma-\rho)(p-1)p^{\rho-1} + (p-1)\sum_{x=0}^{\rho-1}p^x\right) \\
&= (\nu-\rho+1) + \frac{(\sigma-\rho)(\sigma-\rho+1)}{2}(p-1)p^{\rho-1} + (\nu-\sigma)(\sigma-\rho)(p-1)p^{\rho-1} + (\nu-\rho+1)(p^\rho-1) \\
&= p^{\rho-1}\left((\sigma-\rho)(p-1)\frac{1+2\nu-\rho-\sigma}{2} + (\nu-\rho+1)p\right)
\end{aligned} \tag{3.6}$$

Case 2: Suppose that $\nu-\rho < d \leq \nu-1$ and $h \neq \sigma+d-\nu$.

Let $i \in X_h$. Then $v_p(p^\sigma + ip^{\nu-d}) = \min(\sigma, h+\nu-d)$. If $v_p(l_i) \neq \min(\sigma, h+\nu-d)$ then $p = 2 \neq i$, $\mu = \nu+\rho$ and $l_i = 2^\sigma + i(2^{\nu-d}+2^{\mu-1})$. Then, from $\rho \geq 1$ and $d > \nu-\rho \geq 0$ we deduce $\mu - 1 = v_2(l_i - (2^\sigma + i2^{\nu-d})) = \min(v_2(l_i), v_2(2^\sigma + i2^{\nu-d})) = \min(v_2(l_i), \sigma, \nu-d) \leq \nu - d = \mu-\rho-d < \mu-1$, a contradiction. This proves that $v_p(l_i) = \min(\sigma, h+\nu-d)$. Therefore $h_i = \min(\mu, v_p(l_i), \rho+d, \rho+h) = \min(\sigma, h+\nu-d, \rho+d, \rho+h) = \min(\sigma, h+\nu-d, \rho+h) =$

$\min(\sigma, h+\nu-d) \leq \mu$ because $\sigma \leq \nu < \rho + d$ and $h + \nu - d < h + \rho$, by condition (B) in Theorem 3.3 and the assumption. Hence, by Lemma 3.4, each class inside X_h with $\sigma > h \neq \sigma + d - \nu$ contains $p^{\mu - \min(\sigma, h+\nu-d)}$ elements. This proves the following

$$\text{if } \sigma > h \neq \sigma + d - \nu \text{ then } N_{d,h} = \frac{\varphi(p^{\mu-h})}{p^{\mu-\min(\sigma,h+\nu-d)}} = (p-1)p^{\min(\sigma-h,\nu-d)-1}.$$

Then

$$\begin{aligned}
&\sum_{d=\nu-\rho+1}^{\nu-1}\left(1 + \sum_{h=0, h\neq\sigma+d-\nu}^{\sigma-1} N_{d,h}\right) \\
&= \sum_{d=\nu-\rho+1}^{\nu-1}\left(1 + (p-1)\left(\sum_{h=0}^{\sigma+d-\nu-1} p^{\nu-d-1} + \sum_{h=\sigma+d-\nu+1}^{\sigma-1} p^{\sigma-h-1}\right)\right) \\
&= \sum_{x=1}^{\rho-1}\left(1 + (p-1)\sum_{h=0}^{\sigma-x-1} p^{x-1} + (p-1)\sum_{h=\sigma-x+1}^{\sigma-1} p^{\sigma-h-1}\right) \\
&= \sum_{x=1}^{\rho-1}\left(1 + (\sigma-x)(p-1)p^{x-1} + (p-1)\sum_{y=0}^{x-2} p^y\right) = \sum_{x=1}^{\rho-1}\left((\sigma-x)p^x - (\sigma-x)p^{x-1} + p^{x-1}\right) \\
&= \sum_{x=1}^{\rho-1}(\sigma-x)p^x - \sum_{x=0}^{\rho-2}(\sigma-x-1)p^x + \sum_{x=0}^{\rho-2}p^x = (\sigma-\rho+1)p^{\rho-1} + 2\sum_{x=1}^{\rho-2}p^x - (\sigma-1) + 1 \\
&= (1-\rho)p^{\rho-1} + \sigma(p^{\rho-1}-1) + 2\frac{p^{\rho-1}-1}{p-1}
\end{aligned} \tag{3.7}$$

Case 3: Finally, suppose that $\nu - \rho < d \leq \nu - 1$ and $h = \sigma + d - \nu$.

Then, $h < \sigma$ and by condition (B) if $i \in X_h$ then $v_p(i) = h \geq \rho + d - \nu > 0$ and hence $l_i = p^\sigma + ip^{\nu-d} = p^\sigma(1 + ip^{-h})$. Therefore $v_p(l_i) = \sigma + v_p(1 + ip^{-h})$. Also, by condition (B) we have $\rho \leq \sigma \leq \nu$, and therefore $h \leq d$. Thus $h_i = \min(k_i, \rho + h)$. Observe that, as $1 \leq i \leq p^\mu$, we have that $0 \leq v_p(1 + ip^{-h}) \leq \mu - h$. For $0 \leq l \leq \mu - h$ we set

$$Y_l = \{i \in X_h : v_p(1 + ip^{-h}) = l\} \quad \text{and} \quad Z_l = \bigcup_{t=l}^{\mu-h} Y_t.$$

The sets Y_l with $l = 0, 1, \ldots, \mu - h$ form a partition of X_h. A straightforward argument show that

$$|Y_l| = \begin{cases} (p-2)p^{\mu-h-1}, & \text{if } l = 0; \\ \varphi(p^{\mu-h-l}), & \text{if } 1 \leq l < \mu - h; \\ 1, & \text{if } l = \mu - h; \end{cases} \quad \text{and} \quad |Z_l| = \begin{cases} \varphi(p^{\mu-h}), & \text{if } l = 0; \\ p^{\mu-h-l}, & \text{if } 1 \leq l \leq \mu - h. \end{cases}$$

For each $i \in Y_l$ we have $k_i = \min(\mu, \sigma + l)$. Therefore, if $i \in Y_l$ then

$$h_i = \begin{cases} \min(\mu, \rho + h), & \text{if } i \in Z_{\mu-\sigma}; \\ \min(\sigma + l, \rho + h), & \text{otherwise.} \end{cases}$$

By Lemma 3.4, each $\sim_d$-class inside X_h is contained either in some Y_l with $l < \mu - \sigma$ or in $Z_{\mu-\sigma}$. Moreover two elements i and j in Y_l with $l < \mu - \sigma$ belong to the same class if and only if $i \equiv j \mod p^{\min(\sigma+l,\rho+h)}$ while two elements in $Z_{\mu-\sigma}$ are in the same class if and only if $i \equiv j \mod p^{\min(\mu,\rho+h)}$. Recalling that $h = \sigma + d - \nu$ we deduce that if $l < \min(\mu - \sigma, \rho + d - \nu)$ then each class inside Y_l has cardinality $p^{\mu-(\sigma+l)}$, while every class contained in $Z_{\min(\mu-\sigma,\rho+d-\nu)}$ has cardinality $p^{\mu-\min(\mu,\rho+h)}$. Having in mind that $\frac{|Z_{\min(\mu-\sigma,\rho+d-\nu)}|}{p^{\mu-\min(\mu,\rho+\sigma+d-\nu)}} = \frac{|Z_{\min(\mu-\sigma,\rho+d-\nu)+1}|}{p^{\mu-\min(\mu,\rho+\sigma+d-\nu)}} + \frac{|Y_{\min(\mu-\sigma,\rho+d-\nu)}|}{p^{\mu-(\sigma+\min(\mu-\sigma,\rho+d-\nu))}}$ we have

$$N_{d,\sigma+d-\nu} = \frac{|Z_{\min(\mu-\sigma,\rho+d-\nu)+1}|}{p^{\mu-\min(\mu,\rho+\sigma+d-\nu)}} + \sum_{l=0}^{\min(\mu-\sigma,\rho+d-\nu)} \frac{|Y_l|}{p^{\mu-(\sigma+l)}}$$

$$= p^{\nu-d-1} + (p-2)p^{\nu-d-1} + \sum_{l=1}^{\min(\mu-\sigma,\rho+d-\nu)} \frac{\varphi(p^{\mu-\sigma+\nu-d-l})}{p^{\mu-\sigma-l}}$$

$$= (p-1)p^{\nu-d-1} + \min(\mu-\sigma, \rho+d-\nu)(p-1)p^{\nu-d-1} = (1 + \min(\mu-\sigma, \rho+d-\nu))(p-1)p^{\nu-d-1}$$

Thus

$$
\begin{aligned}
&\sum_{d=\nu-\rho+1}^{\nu-1} N_{d,\sigma+d-\nu} = (p-1)\sum_{d=\nu-\rho+1}^{\nu-1}(1+\min(\mu-\sigma,\rho+d-\nu))p^{\nu-d-1}\\
&=(p-1)\sum_{x=0}^{\rho-2}(1+\min(\mu-\sigma,\rho-x-1))p^x\\
&=(p-1)\left(\sum_{x=0}^{\rho+\sigma-\mu-2}(1+\mu-\sigma)p^x+\sum_{x=\rho+\sigma-\mu-1}^{\rho-2}(\rho-x)p^x\right)\\
&=(1+\mu-\sigma)(p^{\rho+\sigma-\mu-1}-1)+\sum_{x=\rho+\sigma-\mu-1}^{\rho-2}(\rho-x)p^{x+1}-\sum_{x=\rho+\sigma-\mu-1}^{\rho-2}(\rho-x)p^x\\
&=(1+\mu-\sigma)(p^{\rho+\sigma-\mu-1}-1)+\sum_{x=\rho+\sigma-\mu}^{\rho-1}(\rho-x+1)p^x-\sum_{x=\rho+\sigma-\mu-1}^{\rho-2}(\rho-x)p^x\\
&=(1+\mu-\sigma)(p^{\rho+\sigma-\mu-1}-1)+2p^{\rho-1}+\sum_{x=\rho+\sigma-\mu}^{\rho-2}p^x-(\mu+1-\sigma)p^{\rho+\sigma-\mu-1}\\
&=(\sigma-1-\mu)+2p^{\rho-1}+p^{\rho+\sigma-\mu}\sum_{x=0}^{\mu-\sigma-2}p^x=(\sigma-1-\mu)+2p^{\rho-1}+p^{\rho+\sigma-\mu}\frac{p^{\mu-\sigma-1}-1}{p-1}\\
&=(\sigma-1-\mu)+2p^{\rho-1}+\frac{p^{\rho-1}-p^{\rho+\sigma-\mu}}{p-1}.
\end{aligned}
\tag{3.8}
$$

Combining (3.5), (3.6), (3.7). and (3.8), and recalling that $N_\nu=\mu+1$, we finally obtain that the number of conjugacy classes of cyclic subgroups of G

$$\begin{aligned}
\sum_{d=0}^{\nu} N_d =&\mu+1+\sum_{d=0}^{\nu-\rho} N_d+\sum_{d=\nu-\rho+1}^{\nu-1}\left(1+\sum_{h=0,h\neq\sigma+d-\nu}^{\min(\sigma,\rho+d)} N_{d,h}+N_{d,\sigma+d-\nu}\right)\\
=&\mu+1+p^{\rho-1}\left((\sigma-\rho)(p-1)\frac{1+2\nu-\rho-\sigma}{2}+(\nu-\rho+1)p\right)\\
&+(1-\rho)p^{\rho-1}+\sigma(p^{\rho-1}-1)+2\frac{p^{\rho-1}-1}{p-1}+(\sigma-1-\mu)+2p^{\rho-1}+\frac{p^{\rho-1}-p^{\rho+\sigma-\mu}}{p-1}\\
=&p^{\rho-1}\sigma\left[1+(p-1)\frac{1+2\nu-\rho-\sigma}{2}\right]+p^{\rho-1}\left(-\rho(p-1)\frac{1+2\nu-\rho-\sigma}{2}+(\nu-\rho+1)p\right)\\
&+(1-\rho)p^{\rho-1}+2\frac{p^{\rho-1}-1}{p-1}+2p^{\rho-1}+\frac{p^{\rho-1}-p^{\rho+\sigma-\mu}}{p-1}\\
=&p^{\rho-1}\sigma\left[1+(p-1)\frac{1+2\nu-\sigma}{2}\right]-\frac{p^{\rho+\sigma-\mu}}{p-1}\\
&+\frac{3p^{\rho-1}-2}{p-1}+p^{\rho-1}\frac{6-2\rho-\rho(p-1)(1+2\nu-\rho)+2(\nu-\rho+1)p}{2}\\
=&p^{\rho-1}\sigma\left[1+(p-1)\frac{1+2\nu-\sigma}{2}\right]-\frac{p^{\rho+\sigma-\mu}}{p-1}\\
&+\frac{3p^{\rho-1}-2}{p-1}+p^{\rho-1}\frac{6-\rho+2\nu\rho-\rho^2+p(\rho^2+2\nu-3\rho-2\nu\rho+2)}{2}=A_\sigma+A.
\end{aligned}\tag{3.9}$$

□

In the following lemma with compute the number of conjugacy classes of a finite metacyclic group when $\epsilon=-1$. This is not as in the previous case where we computed the number of conjugacy classes *of cyclic subgroups*. We present two original proofs for this result. The first of them uses the same tools as in Lemma 3.5 and is the one that we thought of originally. The second proof uses a theorem of Berman [Ber55] on the number of conjugacy classes and was suggested to us by an anonymous referee, to which we offer our thanks.

Lemma 3.6. *If $\epsilon=-1$ then the number of conjugacy classes of G is $3\cdot 2^{\nu-1}+2^{\rho-1}(3\cdot 2^{\nu-1}-2^{\nu+\rho-\mu})$.*

Proof. Every element of G is of the form b^ja^i with $0\leq j<2^\nu$ and $0\leq i<2^\mu$. As $G/\langle a\rangle$ is cyclic of order 2^ν, if b^ja^i and $b^{j'}a^{i'}$ are conjugate then $j=j'$. Let $R=-1+2^\rho$ and $d_j=\gcd(2^\mu,R^j-1)$. Then

$$(b^ja^i)^{b^ya^x}=b^ja^{x(1-R^j)+iR^y}$$

This shows that $b^j a^i$ and $b^j a^{i'}$ belong to the same conjugacy class if and only if the congruence equation $X(1-R^j)+iR^y \equiv i' \mod 2^\mu$ has a solution if and only if $i' \equiv iR^y \mod d_j$ if and only if i and i' belong to the same R-cyclotomic class modulo d_j. Therefore the number of conjugacy classes of elements of the form $b^j a^i$ is C_{R,d_j}, the number of R-conjugacy classes modulo d_j. By Lemma 1.1.(2a) we have

$$d_j = \begin{cases} 2, & \text{if } 2 \nmid j; \\ 2^{\min(\mu,\rho+v_2(j))}, & \text{otherwise.} \end{cases}$$

Using Lemma 3.2 and having in mind that $R+1=2^\rho$ with $2 \le \rho \le \mu$, we have

$$C_{R,d_j} = \begin{cases} 2, & \text{if } j \nmid 2; \\ 1+2^{\rho-1}(1+\min(\mu-\rho, v_2(j))), & \text{otherwise.} \end{cases}$$

Therefore, as the number of integers $1 \le j \le 2^\nu$ with $v_2(j)=k$ is $\varphi(2^{n-k})$, we deduce that that the number of conjugacy classes of G is

$$\begin{aligned}
\sum_{j=1}^{2^\nu} C_{R,d_j} &= 2^\nu + \sum_{k=1}^{\nu} \varphi(2^{\nu-k})(1+2^{\rho-1}(1+\min(\mu-\rho,k))) \\
&= 2^\nu + (1+2^{\rho-1})\sum_{k=1}^{\nu}\varphi(2^{\nu-k}) + 2^{\rho-1}\sum_{k=1}^{\nu}\varphi(2^{\nu-k})\min(\mu-\rho,k) \\
&= 2^\nu + (1+2^{\rho-1})2^{\nu-1} + 2^{\rho-1}\sum_{k=1}^{\mu-\rho-1} 2^{\nu-k-1}k + 2^{\rho-1}\sum_{k=\mu-\rho}^{\nu}\varphi(2^{\nu-k})(\mu-\rho) \\
&= 3\cdot 2^{\nu-1} + 2^{\rho+\nu-2} + 2^{\rho-1}\sum_{k=1}^{\mu-\rho-1} 2^{\nu-k-1}k + (\mu-\rho)2^{\nu+2\rho-\mu-1}
\end{aligned}$$

We calculate separately the sum in the third summand. If $\mu=\rho$ or $\mu=\rho+1$ the summand is zero, so we assume $\mu \ge \rho+2$. Then, using (3.1) we obtain

$$\begin{aligned}
2^{\rho-1}\sum_{k=1}^{\mu-\rho-1} 2^{\nu-k-1}k &= 2^{\nu+2\rho-\mu-1}\sum_{k=1}^{\mu-\rho-1} 2^{\mu-\rho-k-1}k \\
&= 2^{\nu+2\rho-\mu-1}\sum_{i=0}^{\mu-\rho-2} 2^i(\mu-\rho-i-1) \\
&= 2^{\nu+2\rho-\mu-1}\left((\mu-\rho-1)\sum_{i=0}^{\mu-\rho-2} 2^i - \sum_{i=0}^{\mu-\rho-2} 2^i i\right) \\
&= 2^{\nu+2\rho-\mu-1}\left((\mu-\rho-1)(2^{\mu-\rho-1}-1) - ((\mu-\rho-3)2^{\mu-\rho-1}+2)\right) \\
&= 2^{\nu+2\rho-\mu-1}(2^{\mu-\rho}-\mu+\rho-1).
\end{aligned}$$

Observe that replacing μ by ρ or $\rho+1$ in the previous expression the result is zero So there is not need to distinguish cases and we finally obtain the desired formula for the number of conjugacy classes of G:

$$\begin{aligned}\sum_{j=1}^{2^\nu} C_{R,d_j} &= 3\cdot 2^{\nu-1}+2^{\rho+\nu-2}+(\mu-\rho)2^{\nu+2\rho-\mu-1}+2^{\nu+2\rho-\mu-1}(2^{\mu-\rho}-\mu+\rho-1)\\ &= 3\cdot 2^{\nu-1}+3\cdot 2^{\rho+\nu-2}-2^{\nu+2\rho-\mu-1}\\ &= 3\cdot 2^{\nu-1}+2^{\rho-1}(3\cdot 2^{\nu-1}-2^{\nu+\rho-\mu})\end{aligned}$$

□

Now let us see an alternative, shorter proof of the result.

Proof. By a Theorem of Berman [Ber55], the number of conjugacy classes of G is $2^\nu\sum_{i=1}^k\frac{1}{h_i}$ where $h_1,\dots,h_k$ are the cardinalities of the conjugacy classes of G contained in $\langle a\rangle$. To compute this cardinalities we first classify the elements of $\langle a\rangle$ by its order. More precisely we set $C_\delta=\{x\in\langle a\rangle : |x|=2^\delta\}$, for $0\le\delta\le\mu$. Each conjugacy class of G contained in $\langle a\rangle$ is contained in some C_δ. Moreover, $a^i\in C_\delta$ if and only if $\frac{2^\mu}{\gcd(i,2^\mu)}=2^\delta$. In that case, if d is the cardinality of the conjugacy class of G containing a^i then $C_G(a^i)=\left\langle a,b^d\right\rangle$ and d is the minimum positive integer with $i(-1+2^\rho)^d\equiv i \mod 2^\mu$ or equivalently $(-1+2^\rho)\equiv 1 \mod 2^\delta$. Thus $d=o_{2^\delta}(-1+2^\rho)$. This shows that each conjugacy class of G contained in C_δ has $o_{2^\delta}(-1+2^\rho)$ elements. As $|C_\delta|=\varphi(2^\delta)$, the list $h_1,\dots,h_k$ is formed by the integers $o_{2^\delta}(-1+2^\rho)$ with this integer repeated $\frac{\varphi(2^\delta)}{o_{2^\delta}(-1+2^\rho)}$ times. Hence Berman result provides the following formula for the number of conjugacy classes of G:

$$2^\nu\sum_{\delta=0}^{\mu}\frac{\varphi(2^\delta)}{o_{2^\delta}(-1+2^\rho)^2}.$$

By Lemma 1.1.(2b),

$$o_{2^\delta}(-1+2^\rho)=\begin{cases}1, & \text{if } \delta\le 1;\\ 2^{\max(1,\delta-\rho)}, & \text{otherwise.}\end{cases}$$

Then $\sum_{\delta=0}^{\rho}\frac{\varphi(2^\delta)}{o_{2^\delta}(-1+2^\rho)^2}=2+\sum_{\delta=2}^{\rho}2^{\delta-3}=2+\frac{1}{2}\sum_{\alpha=0}^{\rho-2}2^\alpha=2+\frac{2^{\rho-1}-1}{2}$ and, if $\rho<\mu$ then

$$\sum_{\delta=\rho+1}^{\mu}\frac{\varphi(2^\delta)}{o_{2^\delta}(-1+2^\rho)^2} = \sum_{\delta=\rho+1}^{\mu}2^{2\rho-\delta-1}=\sum_{\beta=2\rho-\mu-1}^{\rho-2}2^\beta=2^{2\rho-\mu-1}\sum_{\beta=0}^{\mu-\rho-1}2^\beta=2^{2\rho-\mu-1}(2^{\mu-\rho}-1)$$

Observe that if $\rho = \mu$ then the latter is 0. Thus the number of conjugacy classes of G is

$$2^{\nu+1} + 2^{\nu-1}(2^{\rho-1} - 1) + 2^{\nu+2\rho-\mu-1}(2^{\mu-\rho} - 1) = 3 \cdot 2^{\nu-1} + 2^{\rho-1}(3 \cdot 2^{\nu-1} - 2^{\nu+\rho-\mu}).$$

□

The last two of the technical lemmas have to do with a special case. Let us see the example in detail:

Example 3.7. *Let G and H be the following finite metacyclic 2-groups:*

$$G = \left\langle a, b \mid a^8 = 1, b^{16} = a^8, a^b = a^7 \right\rangle$$
$$H = \left\langle a, b \mid a^8 = 1, b^{16} = a^8, a^b = a^3 \right\rangle$$

One can use the package **`wedderga`** *[BCHK+13] from GAP [GAP12] (one way to do it would be using the function* **`WedderburnDecompositionWithDivAlgebras`***, passing as a parameter the result of the function* **`GroupRing(Rationals, G)`***, where G is the group) or do the calculations by hand to obtain the following:*

$$\begin{aligned} \mathbb{Q}G &= 4\mathbb{Q} \oplus 2\mathbb{Q}(i) \oplus 2\mathbb{Q}(\zeta_8) \oplus 2\mathbb{Q}(\zeta_{16}) \\ &\quad \oplus H(\mathbb{Q}) \oplus M_2(\mathbb{Q}) \oplus H(\mathbb{Q}(\sqrt{2})) \oplus M_2(\mathbb{Q}(i)) \oplus M_2(\mathbb{Q}(\sqrt{2})) \oplus 4M_2(\mathbb{Q}(\zeta_8)) \\ \mathbb{Q}H &= 4\mathbb{Q} \oplus 2\mathbb{Q}(i) \oplus 2\mathbb{Q}(\zeta_8) \oplus 2\mathbb{Q}(\zeta_{16}) \\ &\quad \oplus H(\mathbb{Q}) \oplus M_2(\mathbb{Q}) \oplus 2M_2(\mathbb{Q}(\sqrt{-2})) \oplus M_2(\mathbb{Q}(i)) \oplus 4M_2(\mathbb{Q}(\zeta_8)), \end{aligned}$$

As one can check fairly quick, the commutative parts are isomorphic (for convenience of the reader, the commutative components are the ones in the first row), the number of simple components is 19 in both cases, the dimensions are the same, and the dimensions of the center are the same as well. In an equivalent way, one can check that $|G| = |H|$, that G/G' and H/H' are isomorphic, that the number of conjugacy classes of both groups is the same and that the number of conjugacy classes of cyclic subgroups coincides as well.

The original plan for the proof was to use this four invariants to determine the group, but this example proves that these invariants are not enough. The good thing is *that, as we will see in the proof of Theorem 3.10, these cases are fairly isolated, and we can deal with them in the two following technical lemmas.*

Lemma 3.8. *Suppose that $\epsilon = -1$, $\rho \geq \mu - 1$ and $\mu \geq 3$. Then the following statements hold:*

(1) $\mathbb{Q}G$ has a simple component with center $\mathbb{Q}(\zeta_{2^\mu} + \zeta_{2^\mu}^{-1})$ if and only if $\rho = \sigma = \mu$.

(2) $\mathbb{Q}G$ has a simple component with center $\mathbb{Q}(\zeta_{2^\mu} - \zeta_{2^\mu}^{-1})$ if and only if $\rho = \mu - 1$ and $\sigma = \mu$.

Proof. Let $H = C_G(a)$ and $K_0 = \langle b^2 \rangle$. The assumption $\rho \geq \mu - 1$ implies that $H = \langle a, b^2 \rangle$ is a maximal abelian subgroup of G. Then (H, K_0) satisfy the conditions in Theorem 1.19 and hence $\mathbb{Q}Ge(G, H, K_0)$ is a simple component of $\mathbb{Q}G$. Moreover, by Proposition 1.18 we have

$$Z(\mathbb{Q}Ge(G,H,K_0)) \cong \begin{cases} \mathbb{Q}(\zeta_{2^\mu} + \zeta_{2^\mu}^{-1}), & \text{if } \rho = \sigma = \mu; \\ \mathbb{Q}(\zeta_{2^\mu} - \zeta_{2^\mu}^{-1}), & \text{if } \rho = \mu - 1 \text{ and } \sigma = \mu; \\ \mathbb{Q}(\zeta_{2^{\mu-1}} + \zeta_{2^{\mu-1}}^{-1}), & \text{if } \rho = \sigma = \mu - 1. \end{cases}$$

This proves the reverse implication of (1) and (2).

Conversely suppose that A is a simple component of $\mathbb{Q}G$ with center $\mathbb{Q}(\zeta_{2^\mu} + \zeta_{2^\mu}^{-1})$ or $\mathbb{Q}(\zeta_{2^\mu} - \zeta_{2^\mu}^{-1})$. Since $\mu \geq 3$, this fields are not cyclotomic extensions of $\mathbb{Q}$ and therefore A is not commutative, for otherwise A will be a Wedderburn component of $\mathbb{Q}(G/G')$ and the Wedderburn components of a commutative rational group algebra are cyclotomic extensions of $\mathbb{Q}$. As H is maximal abelian in G and $G/H \cong C_2$ there is a pair (H_1, K) of subgroups of G satisfying the conditions of Theorem 1.19 and $H_1 \in \{H, G\}$. However, $H_1 \neq G$ because A is not commutative. Therefore $H = H_1$. If K is not normal in G then $N_G(K) = H$ and hence $A \cong M_2(\mathbb{Q}(\zeta_{[H:K]}))$ contradicting the fact that the center of A is not cyclotomic. Thus K is normal in G and the center of A has index 2 in $\mathbb{Q}(\zeta_{[H:K]})$. By Proposition 1.18, $\varphi([H : K]) = 2 \dim Z(A) = 2^{\mu-1}$ and hence $[H : K] = 2^\mu$. Another consequence of Proposition 1.18 and the fact that A is not commutative is that $H \neq \langle K, b^2 \rangle$ and as $H/K = \langle aK, b^2K \rangle$ is a cyclic 2-group it follows that $H = \langle K, a \rangle$. As $[H : K] = 2^\mu = |a|$ we have $a^{2^{\mu-1}} \notin K$. Thus $G' \cap K = 1$. As K is normal in G, it follows that $K \subseteq Z(G) = \left\langle a^{2^{\mu-1}}, b^2 \right\rangle$. If $\sigma = \mu - 1$

then $Z(G) = \langle b^2 \rangle$ and its order is 2^ν. Then $K = \langle b^4 \rangle$ which is not possible because $H/\langle b^4 \rangle$ is not cyclic. Thus $\sigma = \mu$ and $Z(G) = \left\langle a^{2^{\mu-1}} \right\rangle \times \langle b^2 \rangle$. Then $K = \langle b^2 \rangle$ or $K = \left\langle a^{2^{\mu-1}} b^2 \right\rangle$. Arguing as in the first paragraph we deduce that $Z(\mathbb{Q}Ge(G,H,K)) = \mathbb{Q}(\zeta_{2^\mu} + \zeta_{2^\mu}^{-1})$ if $\rho = \mu$ and $Z(\mathbb{Q}Ge(G,H,K)) = \mathbb{Q}(\zeta_{2^\mu} - \zeta_{2^\mu}^{-1})$ if $\rho = \mu - 1$. □

Lemma 3.9. *Suppose that $\epsilon = -1$ and $\rho < \mu < \nu + \rho$. Let $F = \{\alpha \in \mathbb{Q}(\zeta_{2^\mu}) : \sigma_{-1+2^\rho}(\alpha) = \alpha\}$. Then $\mathbb{Q}G$ has a simple component of degree $2^{\mu-\rho}$ and center F if and only if $\sigma = \mu$.*

Proof. Let $H = \left\langle a, b^{2^{\mu-\rho}} \right\rangle$. Suppose that $\sigma = \mu$ and let $K = \left\langle b^{2^{\mu-\rho}} \right\rangle$. Then (H,K) satisfies the conditions of Theorem 1.19, and by Proposition 1.18, we have that $\mathbb{Q}Ge(G,H,K)$ has degree $[G:H] = 2^{\mu-\rho}$ and center F.

Otherwise, by condition (C) in Theorem 3.3 we have $\sigma = \mu - 1$. By means of contradiction suppose that $\mathbb{Q}G$ has a simple component A of degree $2^{\mu-\rho}$ and center F. Then $H = \left\langle a, b^{2^{\mu-\rho}} \right\rangle$. As H is maximal abelian subgroup of G with G/H abelian, by Theorem 1.19, we have $A = \mathbb{Q}Ge(G,H_1,K)$ for subgroups H_1 and K satisfying the conditions of Theorem 1.19 and $H_1 \supseteq H$. However, by Proposition 1.18, $[G:H] = 2^{\mu-\rho} = \text{Deg}(A) = [G:H_1]$ and hence $H_1 = H$. As H/K is cyclic, either $H = \langle a, K \rangle$ or $H = \left\langle b^{2^{\mu-\rho}}, K \right\rangle$. In the second case $N_G(K)/K$ is abelian and by Proposition 1.18, the center F of A is a cyclotomic extension of $\mathbb{Q}$, which is not the case. Therefore $H = \langle a, K \rangle$. In particular $[H:K] \le |a| = 2^\mu$. If $a^{2^{\mu-1}} \in K$ then $\left\langle a^{2^{\mu-1}} \right\rangle = \left\langle a, b^{2^{\mu-\rho-1}} \right\rangle' \subseteq K \trianglelefteq \left\langle a, b^{2^{\mu-\rho-1}} \right\rangle$ and $\left\langle a, b^{2^{\mu-\rho-1}} \right\rangle$ contains properly H, in contradiction with the assumption that (H,K) satisfy condition (1) of Theorem 1.19. Therefore $K \cap \langle a \rangle = 1$ and hence $[H:K] \ge |a| = 2^\mu$. So $[H:K] = 2^\mu$. As $N_G(K)/H \cong \text{Gal}(\mathbb{Q}(\zeta_{[H:K]})/F)$, we have $[N_G(K):H] = [\mathbb{Q}(\zeta_{[H:K]}):F] = 2^{\mu-\rho} = [G:H]$ and hence $G = N_G(K)$, i.e. $K \trianglelefteq G$. As $K \cap G' = 1$ it follows that $K \subseteq Z(G) = \left\langle a^{2^{\mu-1}}, b^{2^{\mu-\rho}} \right\rangle = \left\langle b^{2^{\mu-\rho}} \right\rangle$. Finally, the assumption $\mu < \nu + \rho$ implies that H contains $\langle a \rangle$ properly. Therefore $|H| > 2^\mu$ and hence K is a non-trivial subgroup of the cyclic subgroup $\left\langle b^{2^{\mu-\rho}} \right\rangle$. Thus K contains the unique element of order 2 of $Z(G)$, namely $a^{2^{\mu-1}}$, a contradiction. □

We are ready to prove the main result of this section.

Theorem 3.10. *Let p be prime integer. If G_1 and G_2 are finite metacyclic p-groups and $\mathbb{Q}G_1 \cong \mathbb{Q}G_2$ then $G_1 \cong G_2$.*

Proof. Suppose that $\mathbb{Q}G_1 \cong \mathbb{Q}G_2$. By Theorem 3.3, we have $G_i \cong \mathcal{P}_{p,\mu_i,\nu,\sigma_i,\rho_i,\epsilon_i}$ with each list $\mu_i, \nu_i, \sigma_i, \rho_i, \epsilon_i$ satisfying conditions (A)-(C). We will prove that $(\mu_1, \nu_1, \sigma_1, \rho_1, \epsilon_1) = (\mu_2, \nu_2, \sigma_2, \rho_2, \epsilon_2)$.

First of all $p^{\mu_1+\nu_1} = |G_1| = |G_2| = p^{\mu_2+\nu_2}$ and hence $\mu_1 + \nu_1 = \mu_2 + \nu_2$. Moreover, by Theorem 1.14 we have $G_1/G_1' \cong G_2/G_2'$ and from conditions (B) and (C) it follows that

$$G_i/G_i' \cong \begin{cases} C_{p^{\rho_i}} \times C_{p^{\nu_i}}, & \text{if } \epsilon_i = 1, \\ C_2 \times C_{2^{\nu_i}}, & \text{if } \epsilon_i = -1 \end{cases}$$

Suppose that $\epsilon_1 = 1$ and $\epsilon_2 = -1$. Then $C_{2^{\rho_1}} \times C_{2^{\nu_i}} \cong C_2 \times C_{2^{\nu_2}}$, by Theorem 1.14, and by conditions (B) and (C) we have $p = 2$, $\rho_1 \leq \nu_1$, $2 \leq \rho_2$ and $1 \leq \nu_2$. Therefore $\rho_1 = 1$ and hence $\mu_1 = 1$ by condition (A). This implies that G_1 is abelian but G_2 is not abelian, in contradiction with $\mathbb{Q}G_1 \cong \mathbb{Q}G_2$. This proves that $\epsilon_1 = \epsilon_2$, which we denote ϵ from now on.

Moreover, if $\epsilon = 1$ then $C_{p^{\rho_1}} \times C_{p^{\nu_1}} \cong C_{p^{\rho_2}} \times C_{p^{\nu_2}}$ with $\rho_i \leq \nu_i$, and if $\epsilon = -1$ then $C_2 \times C_{2^{\nu_1}} \cong C_2 \times C_{2^{\nu_2}}$ and $1 \leq \nu_1, \nu_2$. Thus, in both cases $\nu_1 = \nu_2$, and hence $\mu_1 = \mu_2$. From now on we set $\mu = \mu_i$ and $\nu = \nu_i$. Suppose that $\epsilon = 1$ then $C_{p^{\rho_1}} \times C_{p^{\nu_1}} \cong C_{p^{\rho_2}} \times C_{p^{\nu_2}}$ and hence $\rho_1 = \rho_2$, which we denote ρ. Moreover, by Artin's Theorem (Theorem 1.11), the number of Wedderburn components of $\mathbb{Q}G_i$ is the number of conjugacy classes of subgroups of G_i. Therefore if A_{σ_1} and A_{σ_2} are as defined in Lemma 3.5 then we have $A_{\sigma_1} = A_{\sigma_2}$. Let

$$B_{\sigma_i} = 2p^{\mu-\rho}(p-1)A_i = -2p^{\sigma_i} + \sigma_i p^{\mu-1}(p-1)(2 + (p-1)(1 + 2\nu - \sigma_i)).$$

Then $B_{\sigma_1} = B_{\sigma_2}$. By means of contradiction, assume without loss of generality that $\sigma_1 < \sigma_2$. By condition (B) we have $\sigma_1 < \sigma_2 \leq \mu \leq \nu + \rho$. If $\sigma_1 < \mu - 1$ then $\min(\sigma_2, \mu - 1) \leq v_p(B_{\sigma_2}) = v_p(B_{\sigma_1}) = \sigma_1 < \mu - 1$, which contradicts the assumption $\sigma_2 > \sigma_1$. Therefore,

$\mu - 1 \le \sigma_1 < \sigma_2 \le \min(\mu, \nu)$, i.e. $\sigma_1 = \mu - 1$ and $\sigma_2 = \mu \le \nu$. Then

$$\begin{aligned}
0 &= B_\mu - B_{\mu-1} \\
&= -2p^\mu + \mu p^{\mu-1}(p-1)(2+(p-1)(2\nu+1-\mu)) \\
&\quad +2p^{\mu-1} - (\mu-1)p^{\mu-1}(p-1)(2+(p-1)(2\nu+1-(\mu-1))) \\
&= p^{\mu-1}(p-1)[-2+\mu(2+(p-1)(2\nu+1-\mu)) - (\mu-1)(2+(p-1)(2\nu+2-\mu))] \\
&= p^{\mu-1}(p-1)[-2+2\mu-2(\mu-1)+\mu(p-1)(2\nu+1-\mu)-(\mu-1)(p-1)(2\nu+2-\mu)] \\
&= p^{\mu-1}(p-1)[\mu(p-1)(2\nu+1-\mu)-\mu(p-1)(2\nu+2-\mu)+(p-1)(2\nu+2-\mu)] \\
&= 2p^{\mu-1}(p-1)^2(\nu+1-\mu) > 0,
\end{aligned}$$

which is the desired contradiction.

Suppose now that $\epsilon = -1$. We first prove that $\rho_1 = \rho_2$. By means of contradiction suppose that $\rho_1 < \rho_2$. It is well known that the dimension over $\mathbb{Q}$ of the center of $\mathbb{Q}G_i$ is the number of conjugacy classes of G_i. Then, by Lemma 3.6 we have

$$2^{\rho_1}(3\cdot 2^{\nu-1} - 2^{\nu+\rho_1-\mu}) = 2^{\rho_2}(3\cdot 2^{\nu-1} - 2^{\nu+\rho_2-\mu})$$

If $\rho_2 < \mu - 1$ then

$$2\rho_2 + \nu - \mu = v_2(2^{\rho_2}(3\cdot 2^{\nu-1} - 2^{\nu+\rho_2-\mu}) = v_2(2^{\rho_1}(3\cdot 2^{\nu-1} - 2^{\nu+\rho_1-\mu})) = 2\rho_1 + \nu - \mu,$$

which contradicts the assumption $\rho_1 < \rho_2$. Therefore $\rho_2 \ge \mu - 1$. If $\rho_1 < \mu - 1$ then using that $\mu \ge 2$, by condition (C), we have

$$\rho_2 + \nu - 1 \le v_2(2^{\rho_2}(3\cdot 2^{\nu-1} - 2^{\nu+\rho_2-\mu}) = v_2(2^{\rho_1}(3\cdot 2^{\nu-1} - 2^{\nu+\rho_1-\mu})) = 2\rho_1 + \nu - \mu < \rho_1 + \nu - 1,$$

again in contradiction with the assumption $\rho_1 < \rho_2$. Therefore $\rho_1 = \mu - 1$ and $\rho_2 = \mu$ and hence $\mu \ge 3$, by condition (A). If $\sigma_2 = \mu$ then, by Lemma 3.8, $\mathbb{Q}G_2$ has a simple component with center isomorphic to $\mathbb{Q}(\zeta_{2^\mu} + \zeta_{2^\mu})$ while $\mathbb{Q}G_1$ does not. Therefore $\sigma_2 = \mu - 1$. This implies that $\nu = 1$, by condition (C). Therefore G_2 is the quaternion group of order $2^{\mu+1}$. If $\sigma_1 = \mu$ then G_1 is the dihedral group of order $2^{\mu+1}$. Otherwise $\sigma_1 = \mu - 1$ and if $b_1 = ba$ then $b_1^2 = 1$ so that G_1 is the semidihedral group $\left\langle a, b_1 \mid a^{2^{\mu-1}} = b_1^2 = 1, a^{b_1} = a^{-1+2^{\mu-1}} \right\rangle$. Looking at the Wedderburn decomposition of the rational group algebras of dihedral, semidihedral groups and quaternion group in [JdR16, 19.4.1] we deduce that $\mathbb{Q}G_2$ has a simple component isomorphic to the quaternion algebra $\mathbb{H}(\mathbb{Q}(\zeta_{2^\mu}+\zeta_{2^\mu}))$, which is a non-commutative division algebra, while $\mathbb{Q}G_1$ does not have any Wedderburn component which is a non-commutative division algebra. This yields the desired contradiction in this case.

So we can set $\rho = \rho_1 = \rho_2$ and it remains to prove that $\sigma_1 = \sigma_2$. Otherwise, we may assume that $\sigma_1 = \mu - 1$ and $\sigma_2 = \mu < \nu + \rho$, by condition (C). If $\rho < \mu$ then we obtain a contradiction with Lemma 3.9. Thus $\rho = \mu$. If $\mu \geq 3$ then the contradiction follows from Lemma 3.8. Thus $\mu = 2$ but then G_1 is the quaternion group of order 8 and G_2 is the dihedral group of order 8 and again $\mathbb{Q}G_1$ has Wedderburn component which is a non-commutative division algebra but $\mathbb{Q}G_2$ does not, yielding to the final contradiction. □

3.3 ISO for finite metacyclic nilpotent groups

In this section we will solve the Isomorphism Problem for rational group algebras for finite metacyclic nilpotent groups. The solution will heavily rely on the result for p-groups. First of all we need to introduce the concept of p-component.

Definition 3.11 (p-component)**.** *Let G be a finite group. We say that a Wedderburn component of $\mathbb{Q}G$ is a* p-component *if its degree is a power of p and its center embeds in $\mathbb{Q}(\zeta_{p^n})$ for some non-negative integer n.*

The concept of p-component arises naturally when one analyzes the rational group algebra $\mathbb{Q}G$ and tries to see which Wedderburn components are also in $\mathbb{Q}G_p$. The result which encompasses this is Lemma 3.15. This is important to reduce the problem from nilpotent to p-groups but, to achieve it, we need to present some auxiliary lemmas first.

Lemma 3.12. *Let G be a finite group and (L,K) a strong Shoda pair of G. Then $\mathbb{Q}Ge(G,L,K)$ is a p-component if and only if $[G:L]$ is a power of p and $[L:K]_{p'} \in \{1,2\}$.*

Proof. The reverse implication is a direct consequence of Proposition 1.18. Conversely, set $A = \mathbb{Q}Ge(G,L,K)$ and suppose that A is a p-component. Let $d = [G:L]$ and $c = [L:K]$. As d is the degree of A, then it is a power of p. Moreover the center of A is isomorphic to the Galois correspondent $F_{G,L,K} = \mathbb{Q}(\zeta_c)^{\text{Im }(\alpha)}$ of a subgroup of $\text{Gal}(\mathbb{Q}(\zeta_c)/\mathbb{Q})$ isomorphic to $N_G(K)/L$ (Remark 1.17). The assumption implies that $F \subseteq \mathbb{Q}(\zeta_{c_p})$. As $[N_G(K) : L]$ is a power of p, then so is $[\mathbb{Q}(\zeta_c) : F_{G,L,K}]$ and hence $\varphi(c_{p'}) = [\mathbb{Q}(\zeta_c) : \mathbb{Q}(\zeta_{c_p})]$ is a power of p. Then $c_{p'}$ is either 1 or 2. □

Remark 3.13. *If G is metacyclic and p is the smallest prime dividing $|G|$ then $p \in \pi_G$. In particular, $2 \notin \pi'_G$.*

Proof. Let $\pi = \pi_G$ and $\pi' = \pi'_G$. If $p \in \pi'$ then by Lemma 2.4.(2), G'_p has a non-central element h of order p. Therefore G contains an element g such that $[g, h] \neq 1$ and we may assume that $|g|$ is a power of a prime q. Then $\text{Aut}(\langle h \rangle)$ has an element of order q. As $\text{Aut}(\langle h \rangle)$ has order $p - 1$ it follows that $q \mid p - 1$ and in particular $q > p$. Thus p is not the smallest prime dividing $|G|$. □

Lemma 3.14. *If G and H are metacyclic groups with $\mathbb{Q}G \cong \mathbb{Q}H$ then $\pi'_G = \pi'_H$ and $\pi_G = \pi_H$.*

Proof. Let $\pi = \pi_G$ and $\pi' = \pi'_G$. We claim that $\pi' = \{p \in \pi(G') : (G/G')_p \text{ is cyclic}\}$. Let $A = \langle a \rangle \trianglelefteq G$ and $B = \langle b \rangle \leq G$ with $G = AB$. By Lemma 2.4.(5), $\langle a_p, b_p \rangle$ is a Sylow p-subgroup of G, $A_{\pi'} = G'_{\pi'}$ and $G = A_{\pi'} \rtimes \left(B_{\pi'} \times \prod_{q \in \pi} A_q B_q\right)$. Therefore, if $p \in \pi'$ then $(G/G')_p$ is cyclic. If $p \in \pi' \setminus \pi(G')$ then $A_{\pi'} \rtimes \left(B_{\pi' \setminus \{p\}} \times \prod_{q \in \pi} A_q B_q\right)$ is a normal Hall p'-subgroup of G and hence $p \in \pi$, a contradiction. This proves that $\pi' \subseteq \{p \in \pi(G') : (G/G')_p \text{ is cyclic}\}$. Conversely, if $p \in \pi$ then $[b_{p'}, a_p] = 1$ and therefore $G'_p = \langle a_p, b_p \rangle'$. Then $(G/G')_p \cong \langle a_p, b_p \rangle / \langle a_p, b_p \rangle'$. Therefore, if $(G/G')_p$ is cyclic then so is $\langle a_p, b_p \rangle$ by the Burnside Basis Theorem. In that case $1 = \langle a_p, b_p \rangle = G'_p$, i.e. $p \notin \pi(G')$. This finishes the proof of the claim.

By Theorem 1.14, the assumption implies that $G/G' \cong H/H'$ and hence $|G'| = |H'|$. Then $G' \cong H'$ as both G' and H' are cyclic. Then, using the claim for G and H we deduce that $\pi'_G = \{p \in \pi(G') : (G/G')_p \text{ is cyclic}\} = \{p \in \pi(H') : (H/H')_p \text{ is cyclic}\} = \pi'_H$ and $\pi_G = \pi(|G|) \setminus \pi'_G = \pi(|H|) \setminus \pi'_H = \pi_H$. □

Lemma 3.15. *If G is metacyclic and $p \in \pi_G$ then the sum of the p-components of $\mathbb{Q}G$ is isomorphic to a direct product of k copies of $\mathbb{Q}G_p$, where*

$$k = \begin{cases} 1, & \text{if } p = 2; \\ [G_2 : G_2' G_2^2], & \text{otherwise.} \end{cases}$$

Proof. Let $\pi = \pi_G$ and $\pi' = \pi_G'$ and suppose that $p \in \pi$. By Remark 3.13, $2 \notin \pi'$ and hence G has a normal Hall $\{2, p\}'$-subgroup N. Let e be a primitive central idempotent such that $\mathbb{Q}Ge$ is a p-component of G. Then $e = e(G, L, K)$ for some strong Shoda pair (L, K) of G and, by Lemma 3.12 $[G : K]$ is either a power of p or 2 times a power of p. In particular $N \subseteq K$. Then $\widehat{N}\widehat{M} = \widehat{M}$ for every subgroup M containing K and as N is normal in G we also have $\widehat{N}\widehat{M}^g = 0$ for every $g \in G$. This implies that $\widehat{N}e = e$. This proves that every p-component of $\mathbb{Q}G$ is contained in $\mathbb{Q}G\widehat{N}$. Therefore $\mathbb{Q}G\widehat{N} = A \oplus B$ where A is the sum of the p-components of $\mathbb{Q}G$, and B is the sum of the Wedderburn components of $\mathbb{Q}G\widehat{N}$ which are not p-components. We want to prove that $\mathbb{Q}(G_p)^k \cong A$.

Suppose first that $p = 2$. Therefore $N = G_{2'}$ and hence $G/N \cong G_2$. Thus G/N is a 2-group and hence every Wedderburn component of $\mathbb{Q}(G/N)$, and $\mathbb{Q}G\widehat{N}$, is a p-component. Therefore $\mathbb{Q}(G_2) \cong \mathbb{Q}G\widehat{N} = A$, as desired.

Suppose that $p \neq 2$. Then $G/N = U_2 \times U_p'$ with $U_2 = G_{p'}/N \cong G_2$, and $U_p = G_{2'}/N \cong G_p$. Let $F_2 = U_2' U_2^2$, the Frattini subgroup of U_2. Then $F_2 = L/N$ for some subgroup L of $G_{p'}$ and by Lemma 3.12 it follows that $L \subseteq K$ and the argument in the first paragraph shows that every p-component of $\mathbb{Q}G$ is contained in $\mathbb{Q}G\widehat{L}$. Thus $\mathbb{Q}G\widehat{L} = A \oplus C$ where C is the sum of the Wedderburn components of $\mathbb{Q}G\widehat{L}$ which are not p-components. Moreover, $G/L \cong U_p \times E$ for E an elementary abelian 2-group of order k. Then $\mathbb{Q}E \cong \mathbb{Q}^k$ and hence $\mathbb{Q}G\widehat{L} \cong \mathbb{Q}(G/L) \cong (\mathbb{Q}U_p)^k$. Moreover, as U_p is a p-group, every Wedderburn component of $\mathbb{Q}U_p$ is a p-component. In other words, $C = 0$ and hence $A \cong (\mathbb{Q}U_p)^k = (\mathbb{Q}G_p)^k$, as desired. □

Lemma 3.16. *Let G and H be finite metacyclic groups with $\mathbb{Q}G \cong \mathbb{Q}H$, let $p \in \pi_G$ and let G_p and H_p be Sylow subgroups of G and H respectively. Then $\mathbb{Q}G_p \cong \mathbb{Q}H_p$.*

Proof. Let $\pi = \pi_G$ and $\pi' = \pi'_G$ and let k be as in Lemma 3.15. As $2 \not\in \pi'$, by Remark 3.13, and $G/G_{\pi'}$ is nilpotent, it follows that $G_2/G_2'G_2^2$ is isomorphic to the Sylow 2-subgroup of the quotient G/G' by its Frattini subgroup. Since $G/G' \cong H/H'$, the value of k is the same whether it is computed for G or H. Let A_G and A_H be the sum of the Wedderburn p-components of $\mathbb{Q}G$ and $\mathbb{Q}H$. Since $\mathbb{Q}G \cong \mathbb{Q}H$ then $A_G \cong A_H$. By Lemma 3.15, $(\mathbb{Q}G_p)^k \cong A_G \cong A_H \cong (\mathbb{Q}H_p)^k$ an therefore $\mathbb{Q}G_p \cong \mathbb{Q}H_p$. □

We are ready to proof our main result:

Proof of Theorem D. By Lemma 3.14 we have $\pi_G = \pi_H$ and from now on we denote the latter by π. Then the Hall π-subgroups of G and H are nilpotent and hence it is enough to prove that if $p \in \pi$ then the Sylow p-subgroups G_p of G and H_p of H are isomorphic. However, $\mathbb{Q}G_p \cong \mathbb{Q}H_p$, by Lemma 3.16, and hence $G_p \cong H_p$, by Theorem 3.10. □

If G is nilpotent then $\pi'_G = \emptyset$ and hence Corollary E follows directly from Theorem D.

CHAPTER 4

The General Case

In this chapter we will prove the general case of the positive answer to the Isomorphism Problem of group algebras of finite metacyclic groups. Formally,

Theorem F. *Let G and H be finite metacyclic groups. If $\mathbb{Q}G \cong \mathbb{Q}H$, then $G \cong H$.*

In the first section we present the sketch of the proof and the rest of the sections will be dedicated to showing that the invariants of the group can be obtained from the group algebra. The results of this chapter are contained in [GBdR23c].

4.1 Introduction and sketch of the proof

A first step to the proof was obtained in Corollary E, where it was proved for nilpotent. This will be an important tool in our proof of Theorem F.

It was said for the nilpotent case in Section 3.1, but it bears repeating that in Theorem F it is not sufficient to assume that only one of the two groups G or H is metacyclic because the groups from Example 3.1 have isomorphic rational group algebras while the first is metacyclic and the second is not.

For the proof of Theorem F we fix two finite metacyclic groups G and H such that the rational group algebras $\mathbb{Q}G$ and $\mathbb{Q}H$ are isomorphic. By Theorem A, proving that G and H are isomorphic is equivalent to show that $\mathrm{MCINV}(G) = \mathrm{MCINV}(H)$. This can be expressed by saying that $\mathrm{MCINV}(G)$ is determined by the isomorphism type of $\mathbb{Q}G$. We will work most of the time with the group G and we will show how the different entries of $\mathrm{MCINV}(G)$ are determined by the isomorphism type of $\mathbb{Q}G$. This way, we need to prove that all of the invariants of G are determined by the isomorphism type of $\mathbb{Q}G$, which we abbreviate as "determined by $\mathbb{Q}G$". For example, $|G|$ is determined by $\mathbb{Q}G$, because $|G| = \dim_{\mathbb{Q}} \mathbb{Q}G$. So, as $m^G n^G = |G|$, to prove that m^G and n^G are determined by $\mathbb{Q}G$ it suffices to prove it for one of them. By Theorem D, π_G, π'_G and the isomorphism type of the Hall π_G-subgroups of G are determined by $\mathbb{Q}G$. Thus we can simplify the notation by setting $\pi = \pi_G = \pi_H$ and $\pi' = \pi'_G = \pi'_H$, and for every $p \in \pi$, the isomorphism type of the Sylow p-subgroup of G is determined by $\mathbb{Q}G$.

It is easy to see that the kernel of the natural homomorphism $\mathbb{Q}G \to \mathbb{Q}(G/G')$ is the minimal ideal I of $\mathbb{Q}G$ with $\mathbb{Q}G/I$ commutative. Therefore any isomorphism $\mathbb{Q}G \to \mathbb{Q}H$ maps that ideal of $\mathbb{Q}G$ to the corresponding ideal of $\mathbb{Q}H$, and hence $\mathbb{Q}(G/G') \cong \mathbb{Q}(H/H')$. Then, $G/G' \cong H/H'$, by the Perlis-Walker Theorem (1.12). This shows that the isomorphism type of G/G' is determined by $\mathbb{Q}G$, and in particular so is $[G : G']$ and $|G'| = \frac{|G|}{[G:G']}$. Moreover, $m_{\pi'} = |G'|_{\pi'}$, by Lemma 2.4.(3), so that $m_{\pi'}$ is determined by $\mathbb{Q}G$. Therefore $n_{\pi'} = \frac{|G|_{\pi'}}{m_{\pi'}}$ is determined by $\mathbb{Q}G$. We collect this information for future use:

Proposition 4.1. *If G and H are finite metacyclic groups with $\mathbb{Q}G \cong \mathbb{Q}H$, then $G/G' \cong H/H'$, $\pi_G = \pi_H$, $\pi'_G = \pi'_H$, $(m^G)_{\pi'} = (m^H)_{\pi'}$, $(n^G)_{\pi'} = (n^H)_{\pi'}$ and for every $p \in \pi(G)$, the p-Sylow subgroups of G and H are isomorphic.*

We denote $R^G = T_G(G'_{\pi'})$. In Section 4.2, we prove that R^G is determined by $\mathbb{Q}G$ and then k^G is determined by $\mathbb{Q}G$, since $k^G = |R^G|$. In Section 4.3, we prove that s^G and ϵ^G are determined by $\mathbb{Q}G$. In Section 4.4, we prove that m^G, n^G and r^G are determined by $\mathbb{Q}G$. Finally we prove that Δ^G is determined by $\mathbb{Q}G$ in Section 4.5. Summarizing, $\mathrm{MCINV}(G) = (m^G, n^G, s^G, \Delta^G) = (m^H, n^H, s^H, \Delta^H) = \mathrm{MCINV}(H)$ and hence $G \cong H$ by Theorem A.

Along the chapter we fix a minimal metacyclic factorization $G = \langle a \rangle \langle b \rangle$ of G. We also fix the notation $m = m^G$, $n = n^G$, $s = s^G$, $\Delta = \Delta^G$, $r = r^G$, $\epsilon = \epsilon^G$, $k = k^G$, $R = R^G$, and m' is as defined in (1.4). Then $\mathrm{Inn}_G(\langle a \rangle)$ is cyclic, say generated by γ, and G is given by the following presentation:

$$G = \left\langle a, b \mid a^m = 1, b^n = a^s, a^b = \gamma(a) \right\rangle. \tag{4.1}$$

Now, by Lemma 2.4.(5),

$$G'_{\pi'} = \langle a_{\pi'} \rangle \quad \text{and} \quad G = \langle a_{\pi'} \rangle \rtimes \left(\langle b_{\pi'} \rangle \times \prod_{p \in \pi} \langle a_p, b_p \rangle \right). \tag{4.2}$$

4.2 $\mathbb{Q}G$ determines R^G

In this section we use the following notation:

$$L_0 = C_G(G'_{\pi'}), \quad L_1 = \left\langle a, b^{2k} \right\rangle \quad \text{and} \quad F_0 = (\mathbb{Q}_{m_{\pi'}})^R.$$

As $a \in L_0$, $L_0 = C_G(a_{\pi'}) = \left\langle a, b^k \right\rangle$. Moreover, $L_1 \subseteq L_0$, $[L_0 : L_1] \le 2$ and $L_0 = L_1$ if and only if $[L_0 : \langle a \rangle]$ is odd.

We consider the following conditions for a field F:

(A1) F can be embedded in a subfield of $\mathbb{Q}_{m_{\pi'}}$.

(A2) The only roots of unity of F are 1 and -1.

Lemma 4.2. *(1) F_0 satisfies (A1) and (A2).*

(2) Let $K = \left\langle a_\pi, b^k \right\rangle$. Then (L_0, K) is a strong Shoda pair of G and if $A = \mathbb{Q}Ge(G, L_0, K)$, then $\mathrm{Deg}(A) = k$ and $Z(A) \cong F_0$.

(3) Suppose that k is odd, $\epsilon = -1$ and $a_2^2 \notin \langle b^4 \rangle$, and let

$$\overline{K} = \begin{cases} \left\langle a_\pi^4, b^{2k} \right\rangle, & \text{if } a_2^2 \notin \langle b^2 \rangle; \\ \left\langle a_\pi^4, b^{4k} \right\rangle, & \text{otherwise.} \end{cases}$$

Then $(L_1, \overline{K})$ is a strong Shoda pair of G and if $\bar{A} = \mathbb{Q}Ge(G, L_1, \overline{K})$, then $\mathrm{Deg}(\bar{A}) = 2k$ and $Z(\bar{A}) \cong F_0$.

Proof. (1) Clearly, F_0 satisfies (A1). If F_0 does not satisfy condition (A2), then it contains a root of unity of order p with p an odd prime. Then p divides $m_{\pi'}$, so that $p \in \pi'$ and $G'_{\pi'} \cap Z(G) = \langle a_{\pi'} \rangle \cap Z(G)$ has an element of order p, in contradiction with Lemma 2.4.(2).

(2) Clearly L_0/K is cyclic generated by $a_{\pi'}K$, $\langle a_{\pi'} \rangle \cap K = 1$, by (4.2), and $[g, a_{\pi'}] \in \langle a_{\pi'} \rangle$ for every $g \in G$. Then $[g, a_{\pi'}] \notin K$ for every $g \in G \setminus L_0$. Moreover, $K \trianglelefteq G$, because $a_\pi^b \in \langle a_\pi \rangle$ and $[b^k, a] = [b^k, a_\pi] \in \langle a_\pi \rangle$. This proves that (L_0, K) satisfies the hypothesis of Theorem 1.19 and hence (L_0, K) is a strong Shoda pair of G. By Proposition 1.18, $\operatorname{Deg}(A) = [G : L_0] = k$ and as $[L_0 : K] = m_{\pi'}$ and K is normal in G, A is isomorphic to the cyclic algebra $(\mathbb{Q}_{m_{\pi'}}/F_0, R, 1)$ whose center is F_0.

(3) Suppose now that the conditions of (3) hold. The assumption $\epsilon = -1$ implies that $4 \mid m$ and $a^b = a^t$ with $t \equiv -1 \mod 4$, or equivalently $\langle a \rangle$ has a non-central element of order 4. In particular, $|b \langle a \rangle|$ is even. Since k is odd, we have that $[G : L_1] = 2k$. Using that $[b, a_2] \in \langle a_2^2 \rangle$ and $[b^k, a_{\pi'}] = 1$, it follows that $[b^{2k}, a] \in \langle a_\pi^4 \rangle$, i.e. $\langle a_2^2 \rangle = \left\langle b_2^{2k} \right\rangle$ and therefore $\overline{K} \trianglelefteq G$ and $L_1' \subseteq \overline{K}$.

We claim that $L_1/\overline{K}$ is cyclic generated by $a\overline{K}$. This is clear from the definition of $\overline{K}$, if $a_2^2 \notin \left\langle b^{2k} \right\rangle$. Otherwise, as $a_2^2 \notin \left\langle b^{4k} \right\rangle$ by hypothesis, $a_2^2 \in \left\langle b^{2k} \right\rangle \setminus \left\langle b^{4k} \right\rangle$ and hence $a_2^2 = b_2^{2ki}$ for some odd integer i. Therefore $b_2^{2k} \in \langle a \rangle$. As $b_{2'}^k \in \overline{K}$ it follows that $b^{2k} \in \left\langle a, \overline{K} \right\rangle$. Then $L_1/\overline{K} = \left\langle a\overline{K} \right\rangle$, as desired.

In order to prove that $(L_1, \overline{K})$ satisfies the conditions of Theorem 1.19 it remains to prove that if B is a subgroup of G containing L_1 properly, then $B' \not\subseteq \overline{K}$. Assume otherwise. Then there is $g \in G \setminus L_1$ with $[L_1, g] \subseteq \overline{K}$. If $g \notin \left\langle a, b^k \right\rangle$, then $1 \neq [a_{\pi'}, g] \in \overline{K} \cap \langle a_{\pi'} \rangle = 1$, a contradiction. Thus $g \in \left\langle a, b^k \right\rangle$ and $\langle L_1, g \rangle = \left\langle a, b^k \right\rangle$, so that $[b^k, a] \in \overline{K}$ and therefore $[b^k, a_2] \in \overline{K}$. On the other hand, $[b^k, a_2] = a_2^{t^k - 1}$ and $v_2(t^k - 1) = 1$, because k is odd (cf. Lemma 1.1.(1a)). Then $a_2^2 \in \overline{K}$. Moreover, $\langle a_\pi, b \rangle = \langle b_{\pi'} \rangle \times \prod_{p \in \pi} \langle a_p, b_p \rangle$, a nilpotent group. Thus $\overline{K}$ is nilpotent and hence $a_2^2 \in \overline{K}_2$. Suppose first that $a_2^2 \notin \left\langle b^{2k} \right\rangle$. Then $\overline{K}_2 = \left\langle a_2^4, b_2^{2k} \right\rangle$ and hence $a_2^2 = a_2^{4i} b_2^{2kj}$ for some integers i, j. Hence $\langle a_2^2 \rangle = \left\langle a_2^{2-4i} \right\rangle = \left\langle b_2^{2kj} \right\rangle \subseteq \left\langle b_2^{2k} \right\rangle$, yielding a contradiction. Thus $a_2^2 \in \left\langle b^{2k} \right\rangle$, and as k is odd we have that $a_2^2 \in \langle b_2^2 \rangle \setminus \langle b_2^4 \rangle$, by assumption. Then $\langle a_2^2 \rangle = \langle b_2^2 \rangle$ and, in particular, a_2^2 commutes with b. This implies that a_2 has order 4, because $\epsilon = -1$. Thus $a_2^2 = b_2^2$, so that the two generators a_π^{4k} and b^{4k} of $\overline{K}$ have odd order. As $\overline{K}$ is nilpotent, we deduce that $\overline{K}$ a 2′-group. This yields a contradiction with the fact that a_2^2 is an element of order 2 in $\overline{K}$.

Then $(L_1, \overline{K})$ satisfies the conditions of Theorem 1.19 and hence it is a strong Shoda pair of G. By Proposition 1.18, $\mathrm{Deg}(\bar{A}) = [G : L_1] = 2k$ and as $[L_1 : \overline{K}] = 4m_{\pi'}$ and $L_1/\overline{K}$ is generated by $a\overline{K}$, the center of $\bar{A}$ is $F = (\mathbb{Q}_{4m_{\pi'}})^{\mathrm{Res}_{4m_{\pi'}}(T_G(\langle a \rangle))}$. Moreover, $F_0 = F \cap \mathbb{Q}_{m_{\pi'}} \subseteq F \subseteq \mathbb{Q}_{4m_{\pi'}}$ and $[\mathbb{Q}_{4m_{\pi'}} : F_0] = [\mathbb{Q}_{4m_{\pi'}} : \mathbb{Q}_{m_{\pi'}}]\,[\mathbb{Q}_{m_{\pi'}} : F_0] = 2k = [G : \bar{L}_0] = [\mathbb{Q}_{4m_{\pi'}} : F]$ and therefore $F = F_0$. □

In Lemma 4.2 we have encountered some Wedderburn components of $\mathbb{Q}G$ with center satisfying conditions (A1) and (A2). In order to analyze which other Wedderburn components of $\mathbb{Q}G$ satisfy the same properties we need the following two lemmas. In their proofs we often use that if (L, K) is a strong Shoda pair of G and $e = e(G, L, K)$, then $\{g \in G : ge = e\} = \mathrm{Core}_G(K)$ (cf. Proposition 1.18).

Lemma 4.3. *Let (L, K) be a strong Shoda pair of G with $a \in L$. Let $C = \mathrm{Core}_G(K)$ and $A = \mathbb{Q}Ge(G, L, K)$. Let p be an odd prime such that the center of A does not have elements of order p. Then $b_p^k \in C$. If, moreover, $p \in \pi$, then $a_p \in C$.*

Proof. Let $e = e(G, L, K)$ and $F = Z(\mathbb{Q}Ge)$. Since A is generated by Ge as $\mathbb{Q}$-algebra, the assumption implies that Ge does not have central elements of order p and hence if g is a p-element of G with $ge \in Z(Ge)$, then $g \in C$. If $p \in \pi'$, then $b_p^k \in Z(G)$ and hence $b_p^k \in C$. Suppose that $p \in \pi$. If $a_p \notin C$, then $p \in \pi_{Ge}$ and hence $\langle a \rangle e$ has an element of order p which is central in Ge, which is not possible. Thus $a_p \in C$. Then $b_p^k e \in Z(Ge)$ and hence $b_p^k \in C$. □

Of course every field of characteristic 0 has a root of unity of order 2 and therefore a similar lemma for $p = 2$ makes no sense. However we have the following:

Lemma 4.4. *Let (L, K) be a strong Shoda pair of G with $a \in L$. Let $C = \mathrm{Core}_G(K)$ and $A = \mathbb{Q}Ge(G, L, K)$. Suppose that $Z(A)$ can be embedded in $\mathbb{Q}_t$ for some odd integer t. Then*

(1) $a_2^4, b_2^{4k} \in C$ and $b_2^{2k} \in L$.

(2) If $\epsilon = 1$, then $a_2^2 \in C$.

(3) If $a_2^2 \in C$ or k is even, then $b_2^{2k} \in C$ and $b_2^k \in L$.

(4) If $2 \nmid k$, $\epsilon = -1$ and $a_2^2 \in \langle b^{2k} \rangle \setminus C$, then $\langle a_2, b_2 \rangle$ is the quaternion group of order 8.

Proof. We use the same notation as in the proof of Lemma 4.3. Now $F \cong (\mathbb{Q}_h)^T$ with $h = [L : K]$ and T a cyclic subgroup of $\mathcal{U}_h$, and by assumption F can be embedded in $\mathbb{Q}_t$ with t an odd integer. Then $(\mathbb{Q}_h)^T \subseteq \mathbb{Q}_t$. The latter implies that F does not have elements of order 4 and hence neither does $Z(Ge)$. As in the previous proof, this implies that if $g \in G$ with $ge \in Z(Ge)$, then $g^4 \in C$.

(1) Suppose that $a_2^4 \notin C$. As $\langle a_2^4 \rangle$ is normal in G, this implies that $a_2^4 \notin K$ and hence h is multiple of 8. Therefore $\mathbb{Q}_h$ contains a primitive 8-th root of unity. As $\mathrm{Gal}(\mathbb{Q}_8/\mathbb{Q})$ is not cyclic, it follows that $(\mathbb{Q}_h)^T$ contains a subfield of $\mathbb{Q}_8$ other than $\mathbb{Q}$ and this is not compatible with $(\mathbb{Q}_h)^T \subseteq \mathbb{Q}_t$, because t is odd. Therefore $a_2^4 \in C$. Then $b_2^{2k}e \in Z(Ge)$ and therefore $b_2^{4k} \in C$. Moreover, as $b_2^{2k}e \in Z(Ge)$, $[b_2^{2k}, a] \in C \subseteq K$ and hence $\langle L, b_2^{2k} \rangle / K$ is an abelian subgroup of $N_G(K)/K$. Thus $b^{2k} \in L$, since L/K is maximal abelian in $N_G(K)/K$.

(2) Suppose that $a_2^2 \notin C$. By (1) the order of a_2e is 4 and the hypotheses imply that $a_2e \notin Z(Ge)$ so that $a_2^be = a_2^{-1}e$. Hence $4 \mid |a|$ and $\langle a \rangle$ has an element of order 4 which is not central in G. Thus $\epsilon = -1$.

(3) Suppose that $a_2^2 \in C$ or k is even. Then b_2^ke is central Ge, so that $b_2^{2k} \in C$ and $[b_2^k, a] \in C \subseteq K$. Therefore $b_2^k \in L$, because L/K is maximal abelian in $N_G(K)$.

(4) Suppose that $2 \nmid k$, $\epsilon = -1$ and $a_2^2 \in \langle b^{2k} \rangle \setminus C$. Then a_2^2 commutes with b and as $\epsilon = -1$ the order of a_2^2 is 2, i.e. a_2 has order 4 and $a_2^b = a_2^{-1}$. Furthermore, as $a_2^2 \in \langle b_2^{2k} \rangle \setminus C$ but $b_2^{4k} \in C$, it follows that $a_2^2 \in \langle b_2^{2k} \rangle \setminus \langle b_2^{4k} \rangle$ and hence $a_2^2 = b_2^{2k} = b_2^2$. This shows that $\langle a_2, b_2 \rangle$ is the quaternion group of order 8. □

Lemma 4.5. *Let A be a Wedderburn component of $\mathbb{Q}G$ with center F. Suppose that F satisfies conditions (A1) and (A2) and the degree of A is maximum among the degrees of the Wedderburn components of $\mathbb{Q}G$ with center satisfying (A1) and (A2). Then F*

can be embedded in F_0 *and*

$$\mathrm{Deg}(A) = \begin{cases} 2k, & \textit{if } \epsilon = -1, 2 \nmid k \textit{ and } a_2^2 \not\in \langle b^4 \rangle\,; \\ k, & \textit{otherwise.} \end{cases}$$

Proof. By Theorem 1.19, $A = \mathbb{Q}Ge(G, L, K)$ for a strong Shoda pair (L, K) of G with $a \in L$ and $\mathrm{Deg}(A) = [G : L]$. Let $C = \mathrm{Core}_G(K)$. Observe that (L, K) satisfies the hypothesis of Lemma 4.3 for every $p \in \pi \setminus \{2\}$ and the hypothesis of Lemma 4.4, because $2 \not\in \pi'$, since the minimal prime dividing $|G|$ is always in π, and hence $m_{\pi'}$ is odd. Therefore $a_\pi^4, b^{4k} \in C$ and $b^{2k} \in L$. The latter implies that $L_1 \subseteq L$. Therefore $[G : L]$ divides $[G : L_1]$ and

$$[G : L_1] = \begin{cases} 2k, & \text{if } 2 \mid [L_0 : \langle a \rangle]; \\ k, & \text{otherwise.} \end{cases}$$

In view of Lemma 4.2, the maximality of $\mathrm{Deg}(A)$ implies that L is either L_0 or L_1. Therefore $\mathrm{Deg}(A) = [G : L] = \{k, 2k\}$. By Lemma 4.2(3), if $2 \nmid k$, $\epsilon = -1$ and $a_2^2 \not\in \left\langle b^{4k} \right\rangle$, then $\mathrm{Deg}(A) = 2k$. Conversely, suppose that $\mathrm{Deg}(A) = 2k$. Then $b_2^k \not\in L$ and hence $a_2^2 \not\in C$ and $2 \nmid k$, by Lemma 4.4(3). Therefore $\epsilon = -1$ by Lemma 4.4(2) and $a_2^2 \not\in \left\langle b^{4k} \right\rangle$, by Lemma 4.4(1). This proof the statement about $\mathrm{Deg}(A)$.

The following observations will be relevant for the remainder of the proof. Firstly, $a_2^2 \in K$ if and only if $a_2^2 \in C$ because $\langle a_2 \rangle$ is normal in G. Secondly, by (4.2), $L_0 = \langle a_{\pi'} \rangle \times \left\langle b_{\pi'}^k \right\rangle \times \prod_{p\in\pi} \left\langle a_p, b_p^k \right\rangle$ and in particular L_0 is nilpotent. Finally, $[b, a] \in \langle a^2 \rangle$, because if $|a|$ is even, then $a^b = a^x$ with x odd.

We consider the following subgroup of G:

$$M = \begin{cases} \left\langle a_\pi^2, b^{2k} \right\rangle, & \text{if } a_2^2 \in K; \\ \left\langle a_\pi^4, b^{2k} \right\rangle, & \text{if } a_2^2 \not\in K \text{ and } 2 \mid k; \\ \left\langle a_\pi^4, b^{4k} \right\rangle, & \text{otherwise.} \end{cases}$$

By Lemma 4.3 and Lemma 4.4, we have that $M \subseteq C$. Moreover, M is normal in G because $\langle a_\pi \rangle$ is normal in G and, using Lemma 1.1.(1a) and Lemma 1.1.(2a) it is easy to see that given an integer c, $[b^{ck}, a] \subseteq \langle a_\pi^c \rangle$ and, if k is even, then $[b^{ck}, a] \subseteq \langle a_\pi^{2c} \rangle$. On the other hand, as $\left\langle a_{\pi\setminus\{2\}}, b_{2'}^k \right\rangle \subseteq M \subseteq C \subseteq K \subseteq L \subseteq L_0$, the Hall $2'$-subgroup of L/M is cyclic generated by

$a_{\pi'}M$ and therefore the Hall $2'$-subgroup of L/K is generated by $a_{\pi'}K$. On the other hand $(L/K)_2$ is a cyclic quotient of L/M.

We consider separately four cases:

Case 1. Suppose that $a_2^2 \in K$.

Then the Sylow 2-subgroup of L/M is elementary abelian of order at most 4 and hence the Sylow 2-subgroup of L/K has order at most 2. Thus $[L:K] \in \{l, 2l\}$ with $l \mid m_{\pi'}$ and the $2'$-part of L/K is generated by $a_{\pi'}K$. If $g = a^i b^{kj}$ with i and j integers, then $[a,g] \in \langle a_\pi^2 \rangle \subseteq M$ and $[b,g] = [b,a^i] = a^{2ix} \equiv a^{2ix}b^{2jkx} \equiv g^{2x} \mod M$ for some integer x. This shows that every subgroup of L containing M is normal in G. In particular, K is normal in G. By Proposition 1.18, $F \cong \mathbb{Q}_l^{\mathrm{Res}_l(\gamma)} \subseteq (\mathbb{Q}_{m_{\pi'}})^R = F_0$, as desired.

Case 2. Suppose that $a_2^2 \notin K$ and $2 \mid k$.

Then L/M has a cyclic normal Hall $2'$-subgroup (generated by $a_{2'}M$), and its Sylow 2-subgroups have order dividing 8 and exponent 4. If the Sylow 2-subgroup of L/M is not abelian, then $a_2^2 \in L'M \subseteq K$, in contradiction with the hypothesis $a_2^2 \notin K$. Thus the Sylow 2-subgroup of L/M is isomorphic to C_4 or $C_4 \times C_2$. As k is even, $[b^k, a] \in \langle a_\pi^4 \rangle \subseteq M$. Hence, arguing as in the previous case it follows that every subgroup of L containing M is normal in G. In particular K is normal in G and as $a_2^2 \notin K$ it follows that $a_{\{2\}\cup\pi'}K$ is a generator of L/K and $F \cong \mathbb{Q}_l^{\mathrm{Res}_l(\gamma)}$ with $l \mid 4m_{\pi'}$. As, by assumption, F can be embedded in $\mathbb{Q}_{m_{\pi'}}$, so does $\mathbb{Q}_l^{\mathrm{Res}_l(\gamma)}$ and as both $\mathbb{Q}_{m_{\pi'}}$ and $\mathbb{Q}_l^{\mathrm{Res}_l(\gamma)}$ are Galois extensions of $\mathbb{Q}_l$ it follows that $\mathbb{Q}_l^{\mathrm{Res}_l(\gamma)} \subseteq (\mathbb{Q}_{m_{\pi'}})^R = F_0$. Thus F can be embedded in F_0, as desired.

Case 3. Suppose that $a_2^2 \in \left\langle b^{2k} \right\rangle \setminus K$ and $2 \nmid k$.

Then $\epsilon = -1$, by Lemma 4.4.(2) and $\langle a_2, b_2 \rangle = Q_8$, by Lemma 4.4.(4). The latter also implies that $a_2^2 \notin \langle b^4 \rangle$ and hence the conditions of Lemma 4.2.(3) hold. Therefore, $L = \left\langle a, b^{2k} \right\rangle = \langle a, M \rangle$, so that L/M is cyclic generated by aM. Moreover, the π-parts of M and K coincide because $a_2^2 \notin K$. Therefore $[L:K] = 4l$ with l a divisor of $m_{\pi'}$. Now it is easy to see that K is normal in G and arguing as in the previous case we deduce that F is isomorphic to a subfield of $(\mathbb{Q}_{m_{\pi'}})^R = F_0$.

Case 4. In the remaining cases $a_2^2 \notin (\left\langle b^{2k} \right\rangle \cup K)$ and $2 \nmid k$.

As in the previous case $\epsilon = -1$ and $L = \left\langle a, b^{2k} \right\rangle$. On the other hand by the definition of M and the assumption $a_2^2 \notin \left\langle b^{2k} \right\rangle$ we have that the Sylow 2-subgroup of L/M is $\langle a_2 M \rangle \times$

$\langle b_2^2 M\rangle \cong C_4\times C_2$. We claim that $K \subseteq \left\langle a^2, b^{2k}\right\rangle$ and K is normal in G. If the former fails, then K contains an element of the form $g = a_2 b^{2kl}$. Then, $g^2 \equiv a_2^2 b^{4kl} \equiv a_2^2 \mod M$, so $a_2^2 \in K$, in contradiction with the hypothesis. Then, $K \subseteq \left\langle a^2, b^{2k}\right\rangle$. In order to prove that K is normal in G take $g = a^{2i}b^{2kj}$ with i, j integers. Then, $[a, g] = [a_\pi, b^{2kj}] \in \langle a_\pi^4\rangle \subseteq M \subseteq K$ and there is an integer x such that $[b, g] = [b, a^{2i}] = a^{4ix} \equiv a^{4ix}b^{4kjx} \equiv (a^{2i}b^{2kj})^{2x} \equiv g^{2x} \mod M$. So $[a, g], [b, g] \in \langle g, M\rangle \subseteq K$ and then K is a normal subgroup of G. As $L = \left\langle a, b^{2k}\right\rangle$, L/K is cyclic, the $2'$-Hall subgroup of L/K is generated by $a_{2'}K$, the 2-Sylow subgroup of L/M is isomorphic to $C_4 \times C_2$ with a_2M of order 4, and $K \subseteq \left\langle a^2, b^{2k}\right\rangle$. It follows that L/K is generated by $\langle aK\rangle$ and $[L : K]$ divides $4m_{\pi'}$. Then we can argue as in the previous cases. □

We are ready to prove the main result of this section:

Proposition 4.6. *If G and H are finite metacyclic groups with $\mathbb{Q}G \cong \mathbb{Q}H$, then $R^G = R^H$.*

Proof. Suppose that $\mathbb{Q}G \cong \mathbb{Q}H$ and let $L_G = (\mathbb{Q}_{m_{\pi'}})^{R^G}$ and $L_H = (\mathbb{Q}_{m_{\pi'}})^{R^H}$. By Lemma 4.2 and Lemma 4.5, among the Wedderburn components of $\mathbb{Q}G$ (respectively, $\mathbb{Q}H$) whose center satisfy conditions (A1) and (A2) there is one with maximum degree and center L_G (respectively, L_H). Denote those Wedderburn components A_G and A_H. As $\mathbb{Q}G \cong \mathbb{Q}H$, $\mathrm{Deg}(A_G) = \mathrm{Deg}(A_H)$. Then, by Lemma 4.5, $Z(A_G) \cong L_G \subseteq L_H$ and $Z(A_H) \cong L_H \subseteq L_G$. As L_G and L_H are Galois extensions of $\mathbb{Q}$ it follows that $L_G = L_H$. Then $R^G = \mathrm{Gal}(\mathbb{Q}_{m_{\pi'}}/L_G) = \mathrm{Gal}(\mathbb{Q}_{m_{\pi'}}/L_H) = R^H$, by Galois Theory. □

4.3 $\mathbb{Q}G$ determines s^G and ϵ^G

In this section we first prove that s^G is determined by $\mathbb{Q}G$ and latter that so is ϵ^G. Recall that we have fixed notation $s = s^G, \epsilon = \epsilon^G, m = m^G, \dots$ In the proof that s is determined by $\mathbb{Q}G$ we work prime by prime, so we fix a prime p and we will prove that s_p is determined by $\mathbb{Q}G$. As $s_{\pi'} = m_{\pi'} = |G'_{\pi'}|$ and G' and π' are determined by $\mathbb{Q}G$, if $p \in \pi'$, then s_p is determined by $\mathbb{Q}G$. Thus, we may assume that $p \in \pi$. Recall that $G_p = \langle a_p, b_p\rangle$ is a Sylow p-subgroup of G. Let $\mathrm{MCINV}(G_p) = (p^\mu, p^\nu, p^\sigma, \langle e + p^\rho\rangle_{p^\mu})$. Then $\mu, \nu, \sigma, \rho, e$ satisfy the conditions of Theorem 3.3 and G_p is given by the following presentation

$$G_p = \left\langle c, d \mid c^{p^\mu} = 1, c^d = c^{e+p^\rho}, d^{p^\nu} = c^{p^\sigma} \right\rangle,$$

and $G_p = \langle c \rangle \langle d \rangle$ is a minimal metacyclic factorization of G_p. As $p \in \pi$, by Proposition 4.1, the isomorphism type of G_p is determined by $\mathbb{Q}G$ and hence so are μ, ν, σ, ρ and e. Observe that $T_G(\langle c \rangle) = T_{G_p}(\langle c \rangle) = \langle e + p^\rho \rangle_{p^\mu}$, since $p \in \pi$.

Lemma 4.7. *(1) $m_p n_p = p^{\mu+\nu}$, $p^\mu \mid m_p$ and $s_p = p^\sigma$*

(2) $p^\mu = m_p$ if and only if $p^\nu = n_p$. In that case $p^\rho = r_p$.

(3) Suppose that $e^{p-1} = 1$. Then

(a) If $p = 2$, then $\epsilon = 1$.

(b) $\frac{m_p}{r_p} = p^{\mu-\rho}$ and $\exp(G_p) = \frac{m_p n_p}{s_p} = p^{\mu+\nu-\sigma}$.

(c) If $m_p \neq p^\mu$, then $k_p > 1$, $\mu \neq 0$, $\rho = \sigma$ and $k_p s_p > n_p$.

(4) Suppose that $e = -1$ and $p = 2$. Then

(a) $\epsilon = -1$ if and only if $m_2 = 2^\mu$.

(b) If $\epsilon = 1$, then $2 = n_2 = k_2 < 2^\nu$, $\sigma = 1$, $\mu = 2$, $m_2 = 2^{\nu+1}$ and $r_2 = 2^\nu$.

Proof. Recall that $G = \langle a \rangle \langle b \rangle$ and $G_p = \langle c \rangle \langle d \rangle$ are minimal metacyclic factorizations. Moreover, $G_p = \langle a_p \rangle \langle b_p \rangle$ is a metacyclic factorization, $|a| = m$, $[G : \langle b \rangle] = s$, $|c| = p^\mu$ and $[G_p : \langle d \rangle] = p^\sigma$. In particular, $p^{\mu+\nu} = |G_p| = m_p n_p$ and $p^\mu \mid m_p$. Therefore $m_p = p^\mu$ if and only if $n_p = p^\nu$. This proves the first two statements of (1) and the first one of (2). For the remainder of the proof we distinguish cases.

Case 1. Suppose that $e^{p-1} = 1$.

Then μ, ν, σ and ρ satisfy the conditions (A) and (B) of Theorem 3.3.

We first prove that if $p = 2$, then $\epsilon = 1$. This is clear, if $\mu \leq 1$. Otherwise $4 \mid 2^\rho = [\langle c \rangle : G_2']$. As $|c| = 2^\mu \mid m_2$, $[\langle a_2 \rangle : G_2']$ is also multiple of 4 and hence $\epsilon = 1$, as desired. This proves (3a).

On the other hand, we have $\frac{m_p}{r_p} = |G'_p| = |(G_p)'| = p^{\mu-\rho}$. In particular, if $m_p = p^\mu$, then $r_p = p^\rho$. This, together with the first paragraph, completes the proof of (2) in this case.

Let $g \in G_p$. Then $g = b_p^x a_p^y$ for some positive integers x and y. If $a_p^{b_p^x} = a_p^z$, then using Lemma 1.1.(1a) and (1.1) we deduce that $g^{\frac{m_p n_p}{s_p}} = a^{y\mathcal{S}\left(z|\frac{m_p n_p}{s_p}\right)} = 1$, as $s_p \mid n_p$ by Theorem B.(2d). This proves that the exponent of G_p is $\frac{m_p n_p}{s_p}$ and a similar argument with c and d shows that the exponent of G_p is $p^{\mu+\nu-\sigma}$. As we already know that $m_p n_p = p^{\mu+\nu}$ we deduce that $s_p = p^\sigma$. This proves (3b) and, together with the first paragraph, completes the proof of (1), in this case.

To prove (3c) we first suppose that $k_p = 1$ or $\mu = 0$. Then $[c, a_{\pi'}] = 1$ and hence $G = \langle a_{p'} c \rangle \langle b_{p'} d \rangle$ is a metacyclic factorization of G. As $G = \langle a \rangle \langle b \rangle$ is a minimal metacyclic factorization, we have $m_p = |a_p| \leq |c| = p^\mu \leq m_p$ and hence $m_p = p^\mu$. Now suppose that $\rho < \sigma$. Then $1 \leq \rho < \sigma \leq \mu$. Moreover, $p^\rho \mid \frac{m_p}{p^\mu} p^\rho = r_p$. As $G_p / \langle a_p \rangle$ is cyclic, we have that $a_p = d^y c^z$ with either $p \nmid y$ or $p \nmid z$ and $\left\langle c^{p^\rho} \right\rangle = G'_p \subseteq \langle a_p \rangle$. If $p \mid z$, then $p \nmid y$ and hence $c^{p^\rho} \in \langle a_p \rangle = \langle dc^x \rangle$ for some x. However $\langle dc^x \rangle \cap \langle c \rangle = \left\langle c^{p^\sigma + x\mathcal{S}(1+p^\rho|p^\nu)} \right\rangle$ and $\sigma \leq \nu$. Thus $p^\sigma + x\mathcal{S}\left(1 + p^\rho \mid \mu\right)$ is multiple of p^σ, by Lemma 1.1.(1a), so that it does not divides p^ρ. Hence $c^{p^\rho} \notin \langle a_p \rangle$, a contradiction. Therefore $p \nmid z$ and this implies that $\langle a_p \rangle = \langle d^x c \rangle$ for some integer $0 \leq x < p^\nu$. If $x = 0$, then $\langle c \rangle = \langle a_p \rangle$ and hence $m_p = p^\mu$. Suppose otherwise that $x > 0$ and let $u = v_p(x)$ and $c^{d^x} = c^{(1+p^\rho)^x}$. Then $|a_p \langle c \rangle| = |d^x c \langle c \rangle| = p^{\nu-u}$ and $c^{p^\rho} \in (G_p)' \subseteq \langle a_p \rangle \cap \langle c \rangle = \left\langle (d^x c)^{p^{\nu-u}} \right\rangle = \left\langle c^{xp^{\sigma-u} + \mathcal{S}\left((1+p^\rho)^x | p^{\nu-u}\right)} \right\rangle$. Therefore $v_p(xp^{\sigma-u} + \mathcal{S}\left((1+p^\rho)^x \mid p^{\nu-u}\right)) \leq \rho < \sigma = v_p(xp^{\sigma-u})$ and hence $v_p(xp^{\sigma-u} + \mathcal{S}\left((1+p^\rho)^x \mid p^{\nu-u}\right)) = v_p(\mathcal{S}\left((1+p^\rho)^x \mid p^{\nu-u}\right)) = \nu - u$. Thus again $m_p = |a_p| = p^\mu$, as desired. Suppose that $m_p \neq p^\mu$. Then $\sigma \leq \rho$. Moreover, $m_p > p^\mu$, by the second statement of (1), and $r_p > p^\rho$ by (3b). Therefore, $s_p = p^\sigma \leq p^\rho < r_p$. Then $n_p < s_p k_p$, by Theorem B.(2d). This completes the proof of (3).

Case 2. Suppose that $e = -1$ and $p = 2$.

Then μ, ν, σ and ρ satisfy the conditions (A) and (C) of Theorem 3.3.

We claim that $s_2 \leq 2^\sigma$. By means of contradiction suppose that $s_2 > 2^\sigma$. As $G_2 / \langle a_2 \rangle$ is cyclic, either $\langle a_2 \rangle = \langle d^i c \rangle$ or $\langle a_2 \rangle = \langle dc^{2i} \rangle$ for some integer i. If G_2 contains a cyclic normal subgroup contained in $C_{G_2}(a_{2'})$ and of the form $\langle d^i c \rangle$ for some integer i, then $G = \langle a_{2'} d^i c \rangle \langle b_{2'} d \rangle$ is a metacyclic factorization of G and therefore $s_2 = [G_2 : \langle b_2 \rangle] \leq [G_2 :

$\langle d\rangle] = 2^s$, against the assumption. Thus, $\langle a_2\rangle = \langle dc^{2i}\rangle$ for some integer i. Moreover, $\langle c^2\rangle = G_2' \subseteq \langle dc^{2i}\rangle$. Thus, $\langle c^2\rangle = \langle dc^{2i}\rangle \cap \langle c\rangle = \left\langle (dc^{2i})^{2^\nu}\right\rangle = \left\langle c^{2^\sigma+2i\mathcal{S}(-1+2^\rho|2^\nu)}\right\rangle$. As $\rho \geq 2$ and $\mu \geq 1$, by Lemma 1.1.(2a), $v_2(2i\mathcal{S}\,(-1+2^\rho \mid 2^\nu)) = v_2(i)+\rho+\nu \geq 3$ and hence $\sigma = v_2(2^\sigma + 2i\mathcal{S}\,(-1+2^\rho \mid 2^\nu)) = 1$. As $1 \leq \mu-1 \leq \sigma = 1$, it follows that $\mu = 2$ and hence $(dc)^2 = d^2$. Thus $|dc| = |d|$ and $\langle a_{2'}dc^{2i}\rangle \langle b_{2'}dc\rangle$ is a metacyclic factorization of G. Then $s_2 = [G_2 : \langle a_2\rangle] \leq [G_2 : \langle dc\rangle] = [G_2 : \langle d\rangle] = 2^\sigma$. This finishes the proof of the claim.

If $\epsilon = -1$, then G_2' has index 2 both in $\langle c\rangle$ and in $\langle a_2\rangle$ and therefore $m_2 = 2^\mu$. Conversely, if $m_2 = 2^\mu$, then $\epsilon = -1$ by Lemma 2.5. This proves (4a).

Suppose that $m_2 = 2^\mu$. Since $G_2 = \langle a_2\rangle \langle b_2\rangle$ is a metacyclic factorization and $G_2 = \langle c\rangle \langle d\rangle$ is a minimal metacyclic factorization with $|a_2| = m_2 = 2^\mu = |c|$, we have $2^\sigma = [G_2 : \langle d\rangle] \leq [G_2 : \langle b_2\rangle] = s_2$. Then $s_2 = 2^\sigma$, by the claim above. This completes the proof of (1) in the case where $\epsilon = -1$.

Suppose that $m_2 = 2^\mu$ and $r_2 \neq 2^\rho$. Then $\text{Res}_{m_2}(\langle\gamma\rangle)_2 = \langle -1+r_2\rangle_{m_2}$ and $T_{G_2}(\langle c\rangle) = \langle -1+2^\rho\rangle_{m_2}$. By Theorem B.(2c), $s_2 \neq r_2n_2$ and, by condition (C) of Theorem 3.3, $\sigma \neq \rho+\nu$. By Lemma 2.6, the hypothesis $r_2 \neq 2^\rho$ implies that 4 divides n_2, 8 divides m_2, $k_2 < n_2$, $s_2 = 2^\sigma = 2^{\mu-1}$ and m_2 divides both $2r_2$ and $2^{\rho+1}$. Since both r_2 and 2^ρ divides m_2 and they are different it follows that either $m_2 = r_2$ or $\rho = \mu$. This contradicts either Theorem B.(2c) or condition Theorem 3.3.(C)(b). This completes the proof of (2).

Suppose $\epsilon = 1$. We still need to prove that $s_2 = 2^\sigma = 2$, $k_2 = 2 = n_2$, $\mu = 2$, $m_2 = 2^{\nu+1}$ and $r_2 = 2^\nu$. By (4a) we have $2^\mu < m_2$. Then $[a_{\pi'}, c] \neq 1$ for otherwise $\langle a_{2'}c\rangle \langle b\rangle$ is a metacyclic factorization of G and, as $G = \langle a\rangle \langle b\rangle$ is a minimal metacyclic factorization, we have that $|a| = m \leq |a_{2'}c| = m_{2'}2^\mu$, so that $m_2 \leq 2^\mu$, a contradiction. Therefore, $k_2 \neq 1$. On the other hand, $\langle c^2\rangle = G_2' \subseteq \langle a_2\rangle \cap \langle c\rangle = \left\langle a_2^{|a_2\langle c\rangle|}\right\rangle$ and therefore $[a_{\pi'}, c^2] = 1$. Suppose that $\langle a_2\rangle = \langle d^ic\rangle$ for some integer i and let $u = v_2(i)$. Then $u < \nu$ for otherwise $a_2 \in \langle c\rangle$ and hence $m_2 = |a_2| \leq |c| = 2^\mu$, a contradiction. Moreover, $|a_2\langle c\rangle| = 2^{\nu-u}$ and $\langle c^2\rangle = G_2' \subseteq \langle c\rangle \cap \langle a_2\rangle = \left\langle a_2^{2^{\nu-u}}\right\rangle = \left\langle c^{2^\sigma\frac{i}{2^u}+\mathcal{S}\left((-1+2^\rho)^i|2^{\nu-u}\right)}\right\rangle \subseteq \langle c^2\rangle$, since $1 \leq \sigma$ and $2 \mid \mathcal{S}\,((-1+2^\rho)^i \mid 2^{\nu-u})$, by Lemma 1.1.(2a). Thus $2^{\mu-1} = |c^2| = |a_2^{2^{\nu-u}}| = m_2 2^{u-\nu}$. Therefore $m_2 < 2^\mu = m_2 2^{1+u-\nu} \leq m_2$, a contradiction. Therefore $\langle a_2\rangle = \langle dc^{2i}\rangle$, for an integer i. Then $[d, a_{\pi'}] = [c^{-2i}, a_{\pi'}] = 1$. Moreover, $|a_2\langle c\rangle| = 2^\nu$ and $a_2^{2^\nu} = c^{2^\sigma+2i\mathcal{S}(-1+2^\rho|2^\nu)}$. Since $2 \leq v_2(2i\mathcal{S}\,(-1+2^\rho \mid 2^\nu))$, $\sigma \geq \mu-1 \geq 1$ and $c^2 \in \left\langle a_2^{2^\nu}\right\rangle$, necessarily $\sigma = 1$ and

$\mu = 2$. Then $m_2 = |a_2| = 2^{\nu+1}$, $n_2 = 2$ and $r_2 = 2^\nu$. As $2 \le k_2 \le n_2$, $k_2 = 2$. Moreover, $|d| = |dc| = 2^{\nu+1}$ and $|G_2| = 2^{\nu+2}$. Therefore $\exp(G_2) = |d|$. Then $G = \langle a \rangle \langle b_{2'} d \rangle$ is a minimal metacyclic factorization, so that $s_2 = 2 = 2^\sigma$. □

The first statement of the next Proposition shows that s^G is determined by $\mathbb{Q}G$. The remaining statements will be used in the proof of Proposition 4.9, which shows that ϵ^G is determined by $\mathbb{Q}G$.

Proposition 4.8. *Let G and H be a metacyclic finite groups such that $\mathbb{Q}G \cong \mathbb{Q}H$ and let $p \in \pi$. Then*

(1) $s^G = s^H$.

(2) If $(k^G)_p = 1$, then $(m^G)_p = (m^H)_p = m^{G_p}$ and $(r^G)_p = (r^H)_p = r^{G_p}$.

(3) If $\epsilon^{G_\pi} = 1$, then $\epsilon^G = \epsilon^H = 1$.

(4) If $\epsilon^{G_p} = 1$ and either $m^{G_p} = 1$ or $r^{G_p} < s^{G_p}$, then $(m^G)_p = (m^H)_p = m^{G_p}$ and $(r^G)_p = (r^H)_p = r^{G_p}$.

(5) If $\epsilon^{G_2} = -1$ and, $s^{G_2} \neq 2$, $n^{G_2} = (k^G)_2$ or $m^{G_2} \neq 4$, then $\epsilon^G = \epsilon^H = -1$, $(m^G)_2 = (m^H)_2$ and $(r^G)_2 = (r^H)_2$.

Proof. Suppose that $\mathbb{Q}G \cong \mathbb{Q}H$. Then $\pi = \pi_G = \pi_H$, $\pi' = \pi'_G = \pi'_H$ and $G_\pi \cong H_\pi$, by Proposition 4.1. Let $p \in \pi$ and $s^{G_p} = p^\sigma$.

(1) By Lemma 4.7, $(s^G)_p = (s^H)_p = p^\sigma$. Since this holds for every $p \in \pi$ and $(s^G)_{\pi'} = (m^G)_{\pi'} = (G')_{\pi'} = (H')_{\pi'} = (m^H)_{\pi'} = (s^H)_{\pi'}$, we conclude that $s^G = s^H$.

Statements (2) to (5) are direct consequences of Lemma 4.7. □

Proposition 4.9. *Let G and H be finite metacyclic groups. If $\mathbb{Q}G \cong \mathbb{Q}H$, then $\epsilon^G = \epsilon^H$.*

Proof. By means of contradiction, assume that $\mathbb{Q}G \cong \mathbb{Q}H$ and, without loss of generality suppose that $\epsilon^G = 1$ and $\epsilon^H = -1$. By Proposition 4.8, $s^G = s^H$, which we denote s and by Proposition 4.6, $k^G = k^H$, which we denote k. By Lemma 4.7, $\epsilon^{G_2} = \epsilon^{H_2} = -1$,

$\mathrm{MCINV}(G_2) = \mathrm{MCINV}(H_2) = (4, 2^\nu, 2, \langle -1 \rangle_4)$, with $\nu \ge 2$, $(m^G)_2 = 2^{\nu+1}$, $(n^G)_2 = k_2 = (s^G)_2 = 2$, $(r^G)_2 = 2^\nu$, $(m^H)_2 = (r^H)_2 = 4$ and $(n^H)_2 = 2^\nu$.

In the remainder of the proof, E is either G or H and $E = \langle a \rangle \langle b \rangle$ is a minimal metacyclic factorization of E. Moreover, we adopt the notation $m = m^E$, $n = n^E$, etc. Since $m_2 \in \{r_2, 2r_2\}$ and $k_2 = 2$, it follows that $b_2^k \in Z(G)$ and $[b^k, a_2] = 1$.

We are going to compute the number of simple components A of $\mathbb{Q}E$ satisfying the following conditions:

(B1) $\mathrm{Deg}(A) = k$

(B2) The center of A does not contain roots of unity of order p for every $p \in \pi \setminus \{2\}$.

Set $L = \left\langle a, b^k \right\rangle = C_E(a_{\pi'}) = C_E(a_{\pi' \cup \{2\}})$. Observe that L is nilpotent and $L_p = \left\langle a_p, b_p^k \right\rangle$ for every prime p.

By Theorem 1.19, the Wedderburn components of $\mathbb{Q}E$ satisfying condition (B1) are those of the form $\mathbb{Q}Ee(E, L, K)$ with K a subgroup of E such that

$$L \text{ is maximal in } \{B \le E : C_E(a) \le B, B' \le K \le B\} \text{ and } L/K \text{ is cyclic} \qquad (4.3)$$

Observe that the maximality condition on L is equivalent to $[b^k, a] \in K$ but $[b^{\frac{k}{p}}, a] \notin K$ for any $p \in \pi(k)$.

For every subgroup K of L satisfying (4.3) let $A_K = \mathbb{Q}Ee(E, L, K)$.

Claim 1. The subgroups K of L satisfying (4.3) and such that A_K satisfies condition (B2) are precisely those of the form $L_{\pi\setminus\{2\}} \times K_{\pi'} \times K_2$ with

(KB1) $K_{\pi'}$ is a cocyclic subgroup of $L_{\pi'}$;

(KB2) K_2 a cocyclic subgroup of L_2; and

(KB3) $[b^{\frac{k}{p}}, a] \notin K$ for every prime $p \mid k$.

Indeed, suppose that K satisfies (4.3) and A_K satisfies condition (B2). By Lemma 4.3, we have that $L_{\pi\setminus\{2\}} \subseteq \mathrm{Core}_G(K)$ and therefore $K = L_{\pi\setminus\{2\}} \times K_{\pi'} \times K_2$ satisfies conditions (KB1)-(KB3). Conversely, let $K = L_{\pi\setminus\{2\}} \times K_{\pi'} \times K_2$ satisfy conditions (KB1)-(KB3). Then (L, K) satisfy (4.3) and hence $A_K = \mathbb{Q}Ge(G, L, K)$ is a simple component of $\mathbb{Q}G$. On the other hand by Proposition 1.18, the center of A_K is isomorphic to a field contained in $\mathbb{Q}_{[L:K]}$ and $\pi([L:K]) \subseteq \pi' \cup \{2\}$. Therefore A_K satisfies condition (B2). This finishes the proof of the claim.

As $s_2 = 2$, $k_2 = 2$ and $\nu \geq 2$,

$$L_2 = \left\langle a_2, b_2^2 \right\rangle = \begin{cases} \langle a_2 \rangle \cong C_{2^{\nu+1}}, & \text{if } E = G; \\ \left\langle a_2^{-1} b_2^{2^{\nu-1}} \right\rangle \times \langle b_2^2 \rangle \cong C_2 \times C_{2^\nu}, & \text{if } E = H. \end{cases}$$

Therefore, if $E = G$, then every subgroup of L_2 is normal in G. Otherwise, i.e. if $E = H$, then E_2' is the socle of $\langle b_2^2 \rangle$ and hence the only subgroups of L_2 which are not normal in H are $\left\langle a_2^{-1} b_2^{2^{\nu-1}} \right\rangle$ and $\left\langle a_2 b_2^{2^{\nu-1}} \right\rangle$. Moreover, these two subgroups are conjugate in G.

Claim 2: Let $K = L_{\pi \setminus \{2\}} \times K_{\pi'} \times K_2$ satisfy conditions (KB1) and (KB2). Then K satisfies condition (KB3) if and only if one of the following conditions hold:

(1) $[b^{\frac{k}{p}} : a_{\pi'}] \not\in K_{\pi'}$ for every $p \in \pi(k)$.

(2) $[b^{\frac{k}{p}} : a_{\pi'}] \not\in K_{\pi'}$ for every $p \in \pi(k) \setminus \{2\}$ and $[b^{\frac{k}{2}} : a_{\pi'}] \in K_{\pi'}$ and either $E = G$ and $K_2 = 1$ or $E = H$ and K_2 is either $\left\langle a_2^{-1} b_2^{2^{\nu-1}} \right\rangle$ or $\left\langle a_2 b_2^{2^{\nu-1}} \right\rangle$.

Indeed, clearly, if K satisfies condition (1), then it also satisfies condition (KB3). Suppose that K satisfies condition (2). Then condition (KB3) holds for every prime $p \neq 2$. Moreover, as $v_2(k) = 1$, if $E = G$, then $[b^{\frac{k}{2}}, a_2] = a_2^{2^\nu} \not\in K_2$ and if $E = H$, then $[b^{\frac{k}{2}}, a_2] = a_2^2 \not\in K_2$. Therefore $[b^{\frac{k}{2}}, a] \not\in K$. Therefore K satisfies condition (KB3), as desired. Finally suppose K satisfy neither (1) nor (2). Then $[b^{\frac{k}{p}}, a_{\pi'}] \in K_p$ for some $p \in \pi(k)$. Suppose that $p \neq 2$. Then $[b^{\frac{k}{p}}, L_2] = 1$ and $[b^{\frac{k}{p}}, L_{\pi \setminus \{2\}}] \subseteq \left\langle a_{\pi \setminus \{2\}} \right\rangle \subseteq K$. Then $[b^{\frac{k}{p}}, L] \subseteq K$ and, in particular, $[b^{\frac{k}{p}}, a] \in K$. Therefore (KB3) does not hold. Suppose $p = 2$ and $[b^{\frac{k}{p}}, a_{\pi'}] \not\in K_{\pi'}$ for every $p \in \pi(k) \setminus \{2\}$. As condition (2) does not hold, either $E = G$ and $K_2 \neq 1$ or $E = H$ and K_2 is neither $\left\langle a_2^{-1} b_2^{2^{\nu-1}} \right\rangle$ nor $\left\langle a_2 b_2^{2^{\nu-1}} \right\rangle$. In both cases K_2 contains G_2' and therefore $[b^{\frac{k}{2}}, a_2] \in K]$ As also $[b^{\frac{k}{2}}, a_{\pi'}] \in K_{\pi'}$ and $[b^{\frac{k}{2}}, a_{\pi \setminus \{2\}}] \in \left\langle a_{\pi \setminus \{2\}} \right\rangle \subseteq K]$, it follows that $[b^{\frac{k}{2}}, a] \in K$. Therefore condition (KB3) fails. This finishes the proof of Claim 2.

As L is normal in G, by [JdR16, Problem 3.4.3], if $K = L_{\pi \setminus \{2\}} \times K_{\pi'} \times K_2$ and $M = L_{\pi \setminus \{2\}} \times M_{\pi'} \times M_2$ are two subgroups of L satisfying conditions (KB1)-(KB3), then $A_K = A_M$

if and only if K and M are conjugate in G if and only if $K_{\pi'}$ and $M_{\pi'}$ are conjugate in G and K_2 and M_2 are conjugate in G.

Let d denote the number of conjugacy classes of cocyclic subgroups $K_{\pi'}$ of $L_{\pi'}$ which satisfy condition (1), and let d_1 denote the number of conjugacy classes of cocyclic subgroups of $L_{\pi'}$ which satisfy the first part of condition (2). As $R^G = R^H$, d and d_1 is independent of E. Let h denote the number of cocyclic subgroups of K_2. Then

$$h = \begin{cases} \nu + 2, & \text{if } E = G; \\ 2(\nu + 1); & \text{if } E = H. \end{cases}$$

By Claim 2, combined with the discussion about the conjugacy classes in G of subgroups of L_2, the number of simple components of $\mathbb{Q}G$ satisfying conditions (B1) and (B2) is

$$N_E = \begin{cases} dh + d_1 = d(\nu + 2) + d_1, & \text{if } E = G \\ d(h - 1) + d_1 = d(2\nu + 1) + d_1, & \text{if } E = H. \end{cases}$$

As $\langle a_{\pi'} \rangle \cap \langle b_{\pi'} \rangle = 1$, $K_\pi = \left\langle b_{\pi'}^k \right\rangle$ satisfies condition (1) and hence $d \geq 1$. Moreover, $\nu \geq 2$, and therefore $N_G < N_H$ and hence $\mathbb{Q}G \not\cong \mathbb{Q}H$, a contradiction. □

4.4 $\mathbb{Q}G$ determines m^G, n^G and r^G

In this section we prove that m^G, n^G and s^G are determined by $\mathbb{Q}G$, i.e. we prove the following proposition.

Proposition 4.10. *Let G and H be finite metacyclic groups such that $\mathbb{Q}G \cong \mathbb{Q}H$. Then $m^G = m^H$, $n^G = n^H$ and $r^G = r^H$.*

Proof. We will be working all the time with the group G and a minimal metacyclic factorization $G = \langle a \rangle \langle b \rangle$. Recall that we have fixed notation $m = m^G, n = n^G, s = s^G, r = r^G, \epsilon = \epsilon^G, \dots$ and the goal is proving that m, n and r are determined by $\mathbb{Q}G$. We work prime by prime, i.e. we fix a prime p and we have to prove that m_p, n_p and r_p are determined by $\mathbb{Q}G$. We keep the notation for MCINV(G_p) as in the previous section, i.e.

$$m^{G_p} = p^\mu, \quad n^{G_p} = p^\nu, \quad r^{G_p} = p^\rho \quad e = \epsilon^{G_p}.$$

We first obtain some reductions: As $(r^G)_{\pi'} = 1$ and $(m^G)_{\pi'}$ and $(n^G)_{\pi'}$ are determined by $\mathbb{Q}G$ (Proposition 4.1), we may assume that $p \in \pi$. If $e = -1$, then $p = 2$ and, by Lemma 4.7,

$$(m_2, n_2, r_2) = \begin{cases} (2^{\nu+1}, 2, 2^\nu) & \text{if } \epsilon = 1; \\ (2^\mu, 2^\nu, 2^\rho), & \text{if } \epsilon = -1 \end{cases}$$

Thus we may assume that $e = 1$ and hence $\epsilon = 1$. Hence $m_p n_p = p^{\mu+\nu}$ and $\frac{m_p}{r_p} = p^{\mu-\rho}$. Therefore, it is enough to prove that one of the three m_p, n_p or r_p is determined by $\mathbb{Q}G$. For future use we express m_p and r_p in terms of n_p:

$$m_p = \frac{p^{\mu+\nu}}{n_p} \quad \text{and} \quad r_p = \frac{p^{\nu+\rho}}{n_p}. \tag{4.4}$$

Observe that $p^{\mu-\rho} = \frac{m_p}{r_p} \le n_p$, by Theorem B.(2d). If $\mu = 0$, then $m_p = 1$, by Proposition 4.8. Thus we may assume that $\mu > 0$ and hence $\rho > 0$. Therefore $m_p \ge r_p > 1$. Let

$$l = \operatorname{lcm}(k, p^{\mu-\rho}) \quad \text{and} \quad L = C_G(a_{\pi' \cup \{p\}}).$$

Then

$$L = \langle a, b^l \rangle = \langle a_{\pi'} \rangle \times \langle b_{\pi'}^k \rangle \times \prod_{q \in \pi \setminus \{p\}} \langle a_q, b_q^k \rangle \times \left\langle a_p, b_p^{\max(k_p, p^{\mu-\rho})} \right\rangle.$$

Moreover, $l_p \le n_p \le p^\nu$ and $l_p \le (n^H)_p \le p^\nu$. Therefore, if $l_p = p^\nu$, then $(n^H)_p = n_p$, as desired. Hence, we may assume that $l_p < p^\nu$. If $k_p = 1$, $\mu = 0$ or $\rho < \sigma$, then $(m^H)_p = m_p$, by Proposition 4.8. Thus we may also assume that $k_p > 1$, $\mu > 0$ and $\rho = \sigma$. Therefore $\frac{m_p}{s_p} = p^{\mu-\sigma} \le p^\rho = p^\sigma = s_p$, by (B). Moreover, $s_p \le n_p \le p^\nu$ and $s_p \le (n^H)_p \le p^\nu$, by Theorem B.(2d). Therefore, if $\rho = \nu$, then $(n^H)_p = n_p$, as desired. Hence, we also may assume that $\rho < \nu$. If $n_p \ne p^\nu$, then $n_p < p^\nu$, hence $m_p > p^\mu$, so that $r_p > p^\rho = s_p$ and thus $n_p < k_p s_p = k_p p^\rho$, by Theorem B.(2d). This proves that $n_p = p^\nu$ or $n_p < \min(p^\nu, p^\rho k_p)$.

Summarizing, in the remainder of the proof we assume the following:

(U1) $e = \epsilon = 1$.

(U2) $k_p > 1$, $0 < \mu \le 2\rho$, $1 \le \rho = \sigma < \nu$, $l_p < p^\nu$, $(s^H)_p = s_p = p^\rho$ and $\max(l_p, p^\rho) \le n_p$.

(U3) Either $n_p = p^\nu$ or $n_p < \min(p^\nu, p^\rho k_p)$. In particular, if $n_p \ge l_p p^\rho$, then $n_p = p^\nu$.

The strategy is similar to the one in the previous section, namely we analyze how are the Wedderburn components of $\mathbb{Q}G$ of a certain kind. In this case, we consider Wedderburn components A of $\mathbb{Q}G$ satisfying the following conditions:

(C1) $\mathrm{Deg}(A) = l$.

(C2) The center F of A does not contain roots of unity of order $q \in \pi \setminus \{p, 2\}$.

(C3) If $p \neq 2$, then F does not contain a root of unity of order 4.

We denote by N_G the number of Wedderburn components of $\mathbb{Q}G$ satisfying conditions (C1)-(C3). We will obtain a formula for N_G and use it to prove that N_G determines $(n^G)_p$. As N_G is determined by $\mathbb{Q}G$, this will show that so is $(n^G)_p$ as desired.

We start characterizing the Wedderburn components of $\mathbb{Q}G$ satisfying conditions (C1)-(C3) in terms of some subgroups of L.

Lemma 4.11. *The Wedderburn components of $\mathbb{Q}G$ satisfying conditions (C1)-(C3) are the algebras of the form $A_K = \mathbb{Q}Ge(G, L, K)$ for a subgroup K of L satisfying the following conditions:*

(KC1) $K_{\pi\setminus\{p,2\}} = L_{\pi\setminus\{p,2\}}$.

(KC2) $K_{\pi'}$ *and* K_p *are cocyclic subgroups of* $L_{\pi'}$ *and* L_p*, respectively.*

(KC3) $[b^{\frac{l}{q}}, a_{\pi'}] \notin K_{\pi'}$*, for every* $q \in \pi(k) \setminus \{p\}$.

(KC4) If $[b^{\frac{l}{p}}, a_{\pi'}] \in K_{\pi'}$*, then* $[b^{\frac{l}{p}}, a_p] \notin K_p$.

(KC5) If $p \neq 2$*, then* K_2 *is a subgroup of* L_2 *of index at most* 2.

If K_1 and K_2 are subgroups of L satisfying (KC1)-(KC4), then $A_{K_1} = A_{K_2}$ if and only if K_1 and K_2 are conjugate in G.

Proof. By Proposition 1.18 and Theorem 1.19 the Wedderburn components of $\mathbb{Q}G$ satisfying condition (C1) are those of the form $A_K = \mathbb{Q}Ge(G, L, K)$ with K a cocyclic subgroup K of L such that L is maximal in $\{B \leq G : C_G(a) \subseteq B, B' \leq K \leq B\}$. As L is nilpotent, a subgroup K of L is cocyclic in L if and only if $K_{\pi'}$, $K_{\pi\setminus\{p,2\}}$, K_p and K_2 are cocyclic in

$L_{\pi'}$, $L_{\pi\setminus\{p,2\}}$, L_p and L_2 respectively. Moreover, by Lemma 4.3, if A_K satisfies (C2), then K satisfies (KC1). Conversely, if condition (KC1) holds, then $\pi([L:K]) \subseteq \pi' \cup \{p,2\}$ and as the center of A_K is isomorphic to a subfield of $\mathbb{Q}_{[L:K]}$, A satisfies condition (C2). A similar argument, using Lemma 4.4, shows that A_K satisfies condition (C3) if and only if $[L_2 : K_2] \leq 2$, because if $p \neq 2$, then $L_2 = \left\langle a_2, b_2^k \right\rangle$ and hence $L_2 / \left\langle a_2^2, b_2^{2k} \right\rangle$ is an elementary abelian 2-group. Observe that if conditions (KC1) and (KC5) hold, then $[b^{\frac{l}{q}}, a_{\pi\setminus\{p\}}] \in K$. Then L is maximal in $\{B \leq G : C_G(a) \subseteq B, B' \leq K \leq B\}$ if and only if for every $q \mid l$, $[b^{\frac{l}{q}}, a_{\pi'\cup\{p\}}] \notin K$, and using that $\langle a \rangle$ is normal in G, it is easy to see that this is equivalent to the combination of conditions (KC3) and (KC4). This finishes the proof of the first statement of the lemma. The last one is a direct consequence of [JdR16, Problem 3.4.3] (see also [OdRS06, Proposition 1.4]). □

Our next goal is describing the cocyclic subgroups of L_p and their normalizers in G. To that end we introduce the following positive integers:

$$v = \min\left(\frac{n_p}{l_p}, p^\rho\right), \qquad u = \frac{|L_p|}{v} = \frac{p^{\mu+\nu}}{vl_p}, \qquad t = \frac{p^{\nu+2\rho}}{v^2 l_p}.$$

Remarks 4.12. *(1) $u \leq up^{2\rho-\mu} = vt$.*

(2) If $v = p^\rho$, then $n_p = p^\nu$, $r_p = p^\rho$ and $v = r_p \leq t \leq u$.

(3) If $v \neq p^\rho$, then $v < u$ and $v \leq \frac{r_p}{p} \leq \frac{t}{p^2}$.

(4) If $k_p \leq p^{\mu-\rho}$, then $v < u$ and $u \geq t$.

Proof. (1) By (U2), $\mu \leq 2\rho$. Thus $vt = \frac{p^{\nu+2\rho}}{vl_p} = \frac{p^{\mu+\nu}}{vl_p} p^{2\rho-\mu} = up^{2\rho-\mu} \geq u$.

(2) Suppose that $v = p^\rho$. Then $n_p \geq l_p p^\rho$ and hence $n_p = p^\nu$, by (U3). Then, by (4.4), $r_p = p^\rho = v \leq \frac{n_p}{l_p} = \frac{p^\nu}{l_p} = t \leq \frac{p^{\mu+\nu-\rho}}{l_p} = u$.

(3) Suppose that $v \neq p^\rho$. Then, as $n_p \leq p^\nu$, we have $v = \frac{n_p}{l_p} < p^\rho \leq p^\mu \leq \frac{p^{\mu+\nu}}{n_p} = u$, and using (4.4) and that $l_p \leq n_p$ and $\mu \leq 2\rho$, it follows that $v = \frac{n_p}{l_p} \leq p^{\rho-1} \leq \frac{r_p}{p} \leq \frac{l_p p^\rho}{n_p} \frac{r_p}{p^2} = \frac{l_p p^{\nu+2\rho}}{n_p^2 p^2} = \frac{t}{p^2}$.

(4) Assume that $k_p \leq p^{\mu-\rho}$. Then $l_p = p^{\mu-\rho}$. By means of contradiction suppose that $v \geq u$. Then $v = p^\rho$, by (3), so $n_p = p^\nu$, by (2). As $\rho < \nu$, by (U2), we get $p^{2\rho} = v^2 \geq$

$vu = \frac{p^{\mu+\nu}}{l_p} = p^{\nu+\rho} > p^{2\rho}$, a contradiction. Again by means of contradiction, suppose that $t > u$. Then, by (2), $v = \frac{n_p}{l_p} < p^\rho$, by (U2), $n_p \geq p^\rho$, and, as $l_p = p^{\mu-\rho}$, it follows that $t = \frac{p^{\rho+\mu+\nu}}{n_p^2} \leq \frac{p^{\mu+\nu}}{n_p} = u$, a contradiction. □

Lemma 4.13. *Set*

$$g = \begin{cases} a_p, & \text{if } n_p \leq l_p p^\rho; \\ b_p^{l_p}, & \text{otherwise;} \end{cases} \quad \text{and} \quad h = \begin{cases} b_p^{l_p} a_p^{-\frac{l_p p^\rho}{n_p}}, & \text{if } n_p \leq l_p p^\rho; \\ b_p^{p^{\nu-\rho}} a_p^{-1}, & \text{otherwise.} \end{cases}$$

Then

(1) $L_p = \langle g \rangle \times \langle h \rangle$, $G'_p = \left\langle a_p^{r_p} \right\rangle \subseteq \langle g \rangle$, $|g| = u$ *and* $|h| = v$.

(2) Let

$$C_{L_p} = \left\{ (i, y, x) : i \in \{1, 2\}, \quad 1 \leq x \leq y \quad \text{and} \quad \begin{cases} y \mid v, & \text{if } i = 1; \\ y \mid u, p \mid x \text{ and } p \mid y \mid vx, & \text{if } i = 2 \end{cases} \right\}.$$

Then

$$(i, y, x) \mapsto K_{i,y,x} = \begin{cases} \langle gh^x, h^y \rangle, & \text{if } i = 1; \\ \langle g^x h, g^y \rangle, & \text{if } i = 2; \end{cases}$$

defines a bijection from C_{L_p} *to the set of cocyclic subgroups of* L_p.

(3) If $(i, y, x) \in C_{L_p}$*, then* $N_G(K_{i,y,x}) = \begin{cases} \left\langle a, b^{\frac{y}{t}} \right\rangle; & \text{if } i = 2 \text{ and } y \geq t; \\ G; & \text{otherwise.} \end{cases}$.

Proof. (1) L_p is an abelian group generated by a_p and $b_p^{l_p}$, $l_p = \max(k_p, p^{\mu-\rho}) = \max(k_p, \frac{m_p}{r_p}) \leq n_p$ and $s_p = p^\rho \leq r_p$ by (U2). Then $\langle b_p \rangle \cap \langle a_p \rangle = \left\langle b_p^{l_p} \right\rangle \cap \langle a_p \rangle = \left\langle b_p^{n_p} \right\rangle = \left\langle a_p^{p^\rho} \right\rangle \supseteq \left\langle a_p^{r_p} \right\rangle = (G_p)' = G'_p$.

Suppose first that $n_p \leq l_p p^\rho$. Then $|b_p^{l_p}| = \frac{n_p}{l_p} \frac{m_p}{p^\rho} \leq m_p = |a_p|$, $\left(b_p^{l_p} a_p^{-\frac{l_p p^\rho}{n_p}} \right)^{\frac{n_p}{l_p}} = 1$ and $\langle a_p \rangle \cap \left\langle b_p^{l_p} a_p^{-\frac{l_p p^\rho}{n_p}} \right\rangle = 1$. Therefore $L_p = \langle a_p \rangle \times \left\langle b_p^{l_p} a_p^{-\frac{l_p p^\rho}{n_p}} \right\rangle = \langle g \rangle \times \langle h \rangle$, $|h| = |b_p^{l_p} a_p^{-\frac{l_p p^\rho}{n_p}}| = \frac{n_p}{l_p} = v$ and $m_p = |g| = \frac{|L_p|}{v} = u$.

Otherwise, $n_p > l_p p^\rho \geq k_p p^\rho$ and hence $n_p = p^\nu$, by (U3). Then $(b_p^{p^{\nu-\rho}} a_p^{-1})^{p^\rho} = 1$, $|g| = |b_p^{l_p}| = \frac{p^{\mu+\nu-\rho}}{l_p} > p^\mu \geq p^\rho$ and, as $|b_p^{p^{\nu-\rho}} a_p^{-1} \langle b_p \rangle| = s_p = p^\sigma \geq p^\rho$, it follows that $\langle g \rangle \cap \langle h \rangle = \left\langle b_p^{l_p} \right\rangle \cap \left\langle b_p^{p^{\nu-\rho}} a_p^{-1} \right\rangle = 1$. Therefore $L_p = \langle g \rangle \times \langle h \rangle$, $|h| = p^\rho = v$ and $|g| = \frac{|L_p|}{v} = u$.

(2) follows at once from Lemma 1.7.

(3) Here we use Lemma 1.7 and Remarks 4.12 without specific mention. Fix an integer such that $2 \leq w \leq m_p + 1$ $a_p^{b_p} = a_p^w$. As $\text{Res}_{m_p}(\gamma) = \langle 1 + r_p \rangle_{m_p}$, we have $v_p(w-1) = v_p(r) \geq \rho$. Let $(i, y, x) \in C_{L_p}$. As $[a, L_p] = 1$ and $[b_{p'}, G_p] = 1$, $a, b_{p'} \in N_G(K_{i,y,x})$. Therefore $N_G(K_{i,y,x}) = \left\langle a, b^{p^\delta} \right\rangle$ for some positive integer δ.

Suppose first that $n_p \leq l_p p^\rho$. Then $v = \frac{n_p}{l_p}$, $g^b = g^w$ and $h^b = g^{-(w-1)\frac{l_p p^\rho}{n_p}} h$. Suppose that $i = 1$. Then $y \mid v$, $1 \leq x \leq y$, $[h^y, b] = h^{-y}(h^b)^y = g^{-(w-1)y\frac{l_p p^\rho}{n_p}} \in \left\langle g^{\frac{y}{x_p}} \right\rangle \subseteq K_{1,y,x}$ and $[gh^x, b] = g^{(w-1)(1-x\frac{l_p p^\rho}{n_p})} \in \langle g^{w-1} \rangle \subseteq \langle g^y \rangle \subseteq K_{1,y,x}$ because $v_p(w-1) = v_p(r) \geq \rho \geq v_p(n) - v_p(l) = v_p(v) \geq v_p(y)$. Thus $K_{1,y,x}$ is normal in G, as desired. Suppose that $i = 2$. Thus $y \mid u$ and $\max(p, \frac{y}{v}) \mid x$. Then $[g^y, b] \subseteq \langle g^y \rangle \subseteq K_{2,y,x}$. Therefore δ is the minimum integer satisfying $[g^x h, b^{p^\delta}] \in \langle g^y \rangle$. Using (1.1), we have $[g^x h, b^{p^\delta}] = g^{x(w^{p^\delta}-1)-(w-1)\frac{l_p p^\rho}{n_p}\mathcal{S}(w|p^\delta)} = g^{(w-1)\mathcal{S}(w|p^\delta)(x-\frac{l_p p^\rho}{n_p})}$. On the other hand, $y \mid y\frac{l_p p^\rho}{n_p} = \frac{yp^\rho}{v} \mid rx$ and hence $y \mid (w-1)x$. Therefore $g^{(w-1)\mathcal{S}(w|p^\delta)x} \in \langle g^y \rangle = \langle g \rangle \cap K_{2,y,x}$, and thus, using (4.4), we deduce that $[g^x h, b^{p^\delta}] \in \langle g^y \rangle$ if and only if $g^{(w-1)\mathcal{S}(w|p^\delta)\frac{l_p p^\rho}{n_p}} \in \langle g^y \rangle$ if and only if $y \mid p^\delta r_p \frac{l_p p^\rho}{n_p} = \frac{p^{\delta+\nu+2\rho} l_p}{n_p^2} = tp^\delta$ if and only if $y \mid t$ or $\frac{y}{t} \mid p^\delta$. Therefore $N_G(K_{2,y,x}) = \langle a, b^{\max(1,\frac{y}{t})} \rangle$, and (3) follows at once from this equality.

Suppose otherwise that $n_p > l_p p^\rho$. Then $v = p^\rho = r_p$ and $n_p = p^\nu$ so that $\nu - \rho > v_p(l_p)$. Hence $\langle a_p^{w-1} \rangle = \langle a_p^{r_p} \rangle = \langle b_p^{p^\nu} \rangle = \left\langle g^{\frac{p^\nu}{l_p}} \right\rangle = \langle g^t \rangle \subseteq \langle g^{p^\rho} \rangle$. Moreover, $g^b = g$ and $h^b = a_p^{1-w} h$. Suppose that $i = 1$. Then $y \mid v$, $[h^y, b] = a_p^{(1-w)y} \in \left\langle g^{y\frac{p^\nu}{l_p}} \right\rangle$ and $[gh^x, b] = a_p^{x(1-w)} \in \left\langle g^{p^\rho} \right\rangle \subseteq \langle g^y \rangle \subseteq K_{1,y,x}$. Therefore $K_{1,y,x}$ is normal in G, as desired. Suppose now that $i = 2$. Therefore $y \mid u$. Since $[g^y, b] = 1$, $N_G(K_{2,y,x}) = \left\langle a, b^{p^\delta} \right\rangle$ with δ be the minimum integer with $[g^x h, b^{p^\delta}] \in \langle g^y \rangle$. As $\left\langle [g^x h, b^{p^\delta}] \right\rangle = \left\langle a_p^{(1-w)^{p^\delta}} \right\rangle = \left\langle g^{tp^\delta} \right\rangle$ it follows that $p^\delta = \max(1, \frac{y}{t})$. Thus $N_G(K_{2,y,x}) = \langle a, b^{\max(1,\frac{y}{t})} \rangle$. □

If $p \neq 2$ and K is a subgroup of L, then K satisfies conditions (KC1)-(KC5) if and only $K_{2'}$ satisfies (KC1)-(KC4) and $[L_2 : K_2] \leq 2$. In that case K_2 is normal in G. On the other hand, if P be a subgroup of $L_{\pi'}$, then $P \subseteq L_{\pi'} \subseteq Z(L)$ and therefore $N_G(P) = \left\langle a, b^d \right\rangle$ for some $d \mid l$. We use this and Lemma 4.13 to classify the subgroups K of L satisfying conditions (KC1)-(KC4) as follows: For each $d \mid l$ denote

$$\mathcal{K}_d = \{P \leq L_{\pi'} \text{ with } P \text{ cocyclic, } N_G(P) = \left\langle a, b^d \right\rangle \text{ and } [b^{\frac{l}{q}}, a_{\pi'}] \notin P \text{ for every } q \in \pi(l) \backslash \{p\}\},$$

$$\mathcal{K}_{d,1} = \{P \in \mathcal{K}_d : [b^{\frac{l}{p}}, a_{\pi'}] \notin P\} \quad \text{and} \quad \mathcal{K}_{d,2} = \{P \in \mathcal{K}_d : [b^{\frac{l}{p}}, a_{\pi'}] \in P\}.$$

Remark 4.14. *Observe that* $\left\langle b_{\pi'}^{l} \right\rangle \in \mathcal{K}_{1,1}$ *because* $b_{\pi'}^{k} \in Z(G)$, $\langle a_{\pi'} \rangle \cap \langle b_{\pi'} \rangle = 1$ *and if* $q \in \pi(l)$, *then* $[b_{\pi'}^{\frac{l}{q}}, a_{\pi'}] \in \langle a_{\pi'} \rangle \setminus \{1\}$.

A subgroup K of L satisfies (KC1)-(KC4) if and only if $K_{\pi \backslash \{p,2\}} = L_{\pi \backslash \{p,2\}}$, $K_{\pi'} \in \mathcal{K}_d$ for some $d \mid l$, $K_p = K_{(i,y,x)}$ for some $(i, y, x) \in C_{L_p}$ and if $K_{\pi'} \in \mathcal{K}_{d,2}$, then $[b^{\frac{l}{p}}, a] \notin K$. In that case, by Lemma 4.13, we have

$$N_G(K) = \begin{cases} \left\langle a, b^{\operatorname{lcm}(d, \frac{y}{t})} \right\rangle, & \text{if } i = 2 \text{ and } y > t; \\ \left\langle a, b^d \right\rangle, & \text{otherwise.} \end{cases} \tag{4.5}$$

Combining this information with Lemma 4.11 and having in mind that the number of conjugates of K in G is $[G : N_G(K)]$, we obtain the following formula for N_G.

$$N_G = O \sum_{d \mid l} (|\mathcal{K}_{d,1}| M(d) + |\mathcal{K}_{d,2}| N(d). \tag{4.6}$$

where

$$O = \begin{cases} \text{number of subgroups of } L_2 \text{ of index at most 2,} & \text{if } p \neq 2; \\ 1, & \text{if } p = 2. \end{cases}$$

and $M(d)$ and $N(d)$ are defined as follows: first let

$$\begin{aligned} M_1 &= \text{number of elements } (1, y, x) \text{ in } C_{L_p} \quad \text{and} \\ N_1 &= \text{number of elements } (1, y, x) \text{ in } C_{L_p} \text{ with } [b_p^{\frac{l}{p}}, a_p] \notin K_{2,y,x}. \end{aligned}$$

Then for each $y \mid v$ let

$$\begin{aligned} M'_y &= \text{number of elements } (2,y,x) \text{ in } C_{L_p} \quad \text{and} \\ N'_y &= \text{number of elements } (2,y,x) \text{ in } C_{L_p} \text{ with } [b_p^{\frac{l}{p}}, a_p] \notin K_{2,y,x}, \end{aligned}$$

Finally set

$$M_2 = \sum_{y \mid t} M'_y, \quad N_2 = \sum_{y \mid t} N'_y$$

and

$$M(d) = \frac{M_1 + M_2}{d} + \sum_{y, pt \mid y \mid u} \frac{M'_y}{\operatorname{lcm}\left(d, \frac{y}{t}\right)} \quad \text{and} \quad N(d) = \frac{N_1 + N_2}{d} + \sum_{y, pt \mid y \mid u} \frac{N'_y}{\operatorname{lcm}\left(d, \frac{y}{t}\right)}.$$

The next goal consists in expressing $M(d)$ and $N(d)$ in terms of d and v. Clearly,

$$M_1 = \frac{pv-1}{p-1}; \quad M'_y = \begin{cases} \frac{y}{p}, & \text{if } p \mid y \mid v; \\ v, & \text{otherwise}; \end{cases} \quad \text{and} \quad M_2 = \sum_{p \mid y \mid v} \frac{y}{p} + \sum_{pv \mid y \mid t} v = \frac{v-1}{p-1} + v \log_p \left(\frac{t}{v}\right).$$

Moreover, by Remarks 4.12, $v \mid t$ and therefore if $pt \mid y$, then $M'_y = v$. Thus

$$\begin{aligned} \sum_{pt \mid y \mid u} \frac{M'_y}{\operatorname{lcm}\left(d, \frac{y}{t}\right)} &= \frac{v}{d_{p'}} \left(\sum_{pd_pt \mid y \mid u} \frac{t}{y} + \sum_{pt \mid y \mid \min(td_p, u)} \frac{1}{d_p} \right) \\ &= \begin{cases} \frac{vt}{d_{p'}u} \sum_{z \mid \frac{u}{ptd_p}} z + \frac{v}{d} \sum_{pt \mid y \mid td_p} 1, & \text{if } td_p < u; \\ \frac{v}{d} \sum_{pt \mid y \mid u} 1, & \text{otherwise}; \end{cases} \\ &= \begin{cases} \frac{vt}{d_{p'}u} \frac{\frac{u}{td_p} - 1}{p-1} + \frac{v}{d}(1 + \log_p(d_p)), & \text{if } td_p < u; \\ \frac{v}{d} \log \frac{u}{t}, & \text{if } t < u \leq td_p; \\ 0, & \text{if } u \leq t; \end{cases} \\ &= \begin{cases} \frac{v}{du} \left(\frac{u - d_pt}{p-1} + (1 + \log_p(d_p)) \right), & \text{if } td_p < u; \\ \frac{v}{d} \log \frac{u}{t}, & \text{if } t \leq u \leq td_p; \cdot \\ 0, & \text{if } u < t. \end{cases} \end{aligned}$$

Therefore, if $td_p < u$, then

$$\begin{aligned} dM(d) &= \frac{pv-1}{p-1} + \frac{v-1}{p-1} + v\log_p\left(\frac{t}{v}\right) + \frac{v}{u}\left(\frac{u-d_pt}{p-1} + (1+\log_p(d_p))\right) \\ &= 1+(p+1)\frac{v-1}{p-1} + v\log_p\left(\frac{p^{\nu+2\rho}}{v^3l_p}\right) + \frac{l_pv^2}{p^{\mu+\nu}}\left(\frac{\frac{p^{\mu+\nu}}{vl_p} - d_p\frac{p^{\nu+2\rho}}{v^2l_p}}{p-1} + (1+\log_p(d_p))\right) \\ &= 1+(p+1)\frac{v-1}{p-1} + v(\nu+2\rho-v_p(v^3l)) + \frac{v-d_pp^{2\rho-\mu}}{p-1} + \frac{l_pv^2}{p^{\mu+\nu}}(1+\log_p(d_p)), \end{aligned}$$

if $t \leq u \leq td_p$, then

$$dM(d) = \frac{pv-1}{p-1} + \frac{v-1}{p-1} + v\log_p\left(\frac{t}{v}\right) + v\log_p\left(\frac{u}{t}\right) = 1+(p+1)\frac{v-1}{p-1} + v(\mu+\nu-v_p(v^2l)),$$

and, if $u < t$, then

$$dM_d = \frac{pv-1}{p-1} + \frac{v-1}{p-1} + v\log_p\left(\frac{t}{v}\right) = 1+v(p+1)+v\log$$

Summarizing, we obtain the following formula for $M(d)$

$$M(d) = \frac{1}{d}(f_d(v)+h_d(v)) \tag{4.7}$$

where

$$(f_d(v), h_d(v)) = \begin{cases} \left(v\left(\frac{p+2}{p-1}+\nu+2\rho-v_p(v^3l)\right), \frac{l_pv^2}{p^{\mu+\nu}}(1+\log_p(d_p)) - \frac{2+d_pp^{2\rho-\mu}}{p-1}\right), & \text{if } td_p < u; \\ \left(v\left(\frac{p+1}{p-1}+\mu+\nu-v_p(v^2l)\right), -2\right), & \text{if } t \leq u \leq td_p; \\ (v\left(\frac{p+1}{p-1}+\nu+2\rho-v_p(v^3l)\right), 0), & \text{if } u < t. \end{cases}$$

With the aim to obtain a formula for $N(d)$ we first prove the following claim:

$$N_1 = 0, \quad \text{and} \quad N_y = \begin{cases} v, & \text{if } k_p \leq p^{\mu-\rho} \text{ and } y = u; \\ 0, & \text{otherwise.} \end{cases}$$

This is clear if $k_p > p^{\mu-\rho}$, because in that case $[b_p^{\frac{l}{p}}, a_p] = 1$. So, suppose that $k_p \leq p^{\mu-\rho}$. Then $1 < l_p = p^{\mu-\rho} = \frac{m_p}{r_p}$. Moreover, $v < u \geq t$, by Remarks 4.12.(4). The first implies that $|[b_p^{\frac{l}{p}}, a_p]| = |a_p^{r_p\frac{m_p}{pr_p}}| = p$ and from $v < u$ we get $N_u = |\{x \geq 1 : \frac{u}{v} \mid x \leq u\}| = v$. Let $(i,y,x) \in C_{L_p}$. Using $[G, a_p] = \left\langle a_p^{r_p}\right\rangle \subseteq \langle g\rangle$ and Lemma 1.7, it follows that $[b_p^{\frac{l}{p}}, a_p] \notin K_{i,y,x}$ if and only if $\left\langle a_p^{r_p}\right\rangle \cap K_{i,y,x} = 1$ if and only if $\langle g\rangle \cap K_{i,y,x} = 1$, if and only if either $(i,y,x_p) = (1,u,1)$

or $(i,y)=(2,u)$. However, if $i=1$ and $y=u$, then $u=y\mid v<u$, a contradiction. Thus, $N_1=0$ and if $y\neq u$, then $N_y=0$. This finishes the proof of the claim.

Having in mind that $\frac{u}{t}=p^{\mu-2\rho}v$, the previous claim yields the following formula for $N(d)$:

$$N(d)=g_d(v)=\begin{cases}\frac{v}{d}, & \text{if } k_p\le p^{\nu-\rho} \text{ and } d_p\ge \frac{u}{t};\\ \frac{1}{d_{p'}}p^{2\rho-\mu}, & \text{if } k_p\le p^{\nu-\rho} \text{ and } d_p> \frac{u}{t};\\ 0, & \text{otherwise.}\end{cases} \tag{4.8}$$

Combining (4.6), (4.7) and (4.8) we obtain

$$N_G=O\sum_{d\mid l}\left(\frac{|\mathcal{K}_{d,1}|}{d}(f_d(v)+h_d(v))+|\mathcal{K}_{d,2}|g_d(v)\right). \tag{4.9}$$

Now observe that h_d and g_d are increasing functions for $v>0$. Moreover, a straightforward computation shows that

$$f_d(pv)-f_d(v)=\begin{cases}v(p-1)(\nu-v_p(vl)+2(\rho-v_p(v))), & \text{if } t\le u;\\ v(p-1)(\nu-v_p(vl)+2(\rho-v_p(v))-1), & \text{otherwise.}\end{cases}$$

If v is a proper divisor of $\min\left(\frac{p^\nu}{l_p},p^\rho\right)$, then $\nu-v_p(vl)+2(\rho-v_p(v))-1>0$ and hence the previous calculation shows that $f_d(pv)>f_d(v)$. These shows that $f_d(v)$ is a increasing function on the set of divisors of v of $\min\left(\frac{p^\nu}{l_p},p^\rho\right)$. This, together with formula (4.9) and the facts that $O>0$, $\mathcal{K}_{1,1}>0$ (see Remark 4.14), $\mathcal{K}_{1,2}\ge 0$ and $h_d(v)$ and $g_d(v)$ are non-decreasing functions for $v>0$ shows that v is determined by N_G and, hence it is determined by $\mathbb{Q}G$.

To complete the proof of Proposition 4.10, it only remains to show that v determines n_p, and for that it is enough to show that n_p is the unique positive integer satisfying the following conditions: $q\mid p^\nu$, $v=\min\left(\frac{q}{l_p},p^\rho\right)$ and, if $v=p^\rho$, then $q=p^\nu$. Indeed, observe that n_p satisfies this conditions by Remarks 4.12. By means of contradiction let q satisfy the conditions with $n_p\neq q$. Then $\min(q,n_p)\neq p^\nu$ and hence $v<p^\rho$. Thus $\min\left(\frac{\max(q,n_p)}{l_p},p^\rho\right)=v=\frac{\min(q,n_p)}{l_p}<\frac{\max(q,n_p)}{l_p}$ and hence $v=\min\left(\frac{\max(q,n_p)}{l_p},p^\rho\right)=p^\rho$, a contradiction. This finishes the proof of Proposition 4.10. □

4.5 $\mathbb{Q}G$ determines Δ^G

In this section we complete the proof of Theorem F by proving the following proposition.

Proposition 4.15. *Let G and H be finite metacyclic groups such that $\mathbb{Q}G \cong \mathbb{Q}H$. Then $\Delta^G = \Delta^H$.*

Proof. Suppose that G and H satisfy the hypothesis of the proposition. By the results of the previous sections we can use a common notation for most of the invariants of G and H: $m = m^G = m^H$, $n = n^G = n^H$, $s = s^G = s^H$, $r = r^G = r^H$, $R = R^G = R^H$, $k = k^G = k^H$, $\epsilon = \epsilon^G = \epsilon^H$ and m' is defined as explained in Equation (1.4). We abuse the notation by denoting with the same symbols the generators a and b of minimal metacyclic factorizations $G = \langle a \rangle \langle b \rangle$ and $H = \langle a \rangle \langle b \rangle$.

As Δ^G and Δ^H are cyclic subgroups of $\mathcal{U}_{m'}$ to prove that they are equal we can we work prime by prime, i.e. we will prove that $(\Delta^G)_p = (\Delta^H)_p$ for every prime p. If $p \in \pi'$ or $m'_p = 1$, then, by Proposition 4.6, $(\Delta^G)_p = R^G_p = R^H_p = (\Delta^H)_p$. Also, if $r_p \le m'_p$, then $(\Delta^G)_p = (\Delta^H)_p$ and hence we also may assume that $m'_p > r_p$. The latter implies that $r_p > 1$.

So in the remainder of the proof $p \in \pi$ and $m'_p > r_p$, which implies that $r_p > 1$ and $s_p > 1$, and we have to prove that $(\Delta^G)_p = (\Delta^H)_p$. We will consider three cases and in each one the proof is going to proceed in the following way: We consider distinguished simple components of $\mathbb{Q}G$ (and $\mathbb{Q}H$) depending on the case. Each component of that kind is going to be of the form $\mathbb{Q}Ge(G, L, K)$ for a fixed subgroup L of G and various subgroups K of L so that (L, K) satisfies the conditions of Theorem 1.19. We prove that there is at least one component of that kind, parametrized by some particular K_0, and then we analyze some properties of the other possible K's yielding such components. The arguments for G are valid for H and as $\mathbb{Q}G$ and $\mathbb{Q}H$ are isomorphic, $\mathbb{Q}H$ has another component $\mathbb{Q}He(H, L, K) \cong \mathbb{Q}Ge(G, L, K_0)$. Using the description of these algebras in Proposition 1.18 we will obtain the desired conclusion with the help of the Main Theorem of Galois Theory, because $(\Delta^G)_p$ will be identified with the p-th part of the Galois group of a certain field extension $\mathbb{Q}_d/F$ where d is common for G and H and F is the center of A. As some of the arguments are similar in the different cases, we will only explain all the details in Case 1, and in Cases 2 and 3, we only elaborate arguments which are significantly different than in previous cases.

We work most of the time with G, which is given by the presentation in (4.1) and simplify the notation for this group by setting $\Delta = \Delta^G$.

Case 1: Suppose that $\epsilon^{p-1} = 1$ and $s_p \geq m'_p$.

<u>Claim 1</u>. In this case $m'_p = \min(m_p, k_p r_p, \max(r_p, s_p, r_p \frac{k_p s_p}{n_p}))$, $r_p \leq s_p$ and one of the following hold $k_p r_p \leq n_p$ or $s_p = m_p$.

Proof. The first equality follows from the definition of m' (1.4). Assume $r_p > s_p$. By Theorem B.(2d), $s_p \leq n_p < k_p s_p$. Then, $\max(r_p, s_p, r_p \frac{k_p s_p}{n_p}) = \frac{k_p s_p}{n_p} r_p \leq k_p r_p$, so $m'_p = \min(m_p, \frac{k_p s_p}{n_p} r_p)$. If $m'_p = m_p$, then $s_p \geq m'_p = m_p$ so $s_p = m_p$, which yields the contradiction $m_p \geq r_p > s_p = m_p$. Otherwise, $m'_p = \frac{k_p s_p}{n_p} r_p$ that also yields a contradiction because $s_p \geq \frac{k_p s_p}{n_p} r_p > r_p > s_p$. So we have proved that $s_p \geq r_p$. Now let us assume $k_p r_p > n_p$ and $s_p < m_p$. Then, $m'_p \neq m_p$, as $s_p \geq m'_p$. In addition, $s_p < \frac{k_p s_p}{n_p} r_p \leq k_p r_p$, so $\max(r_p, s_p, \frac{k_p s_p}{n_p} r_p) = \frac{k_p s_p}{n_p} r_p$ and $m'_p = \frac{k_p s_p}{n_p} r_p > s_p \geq m'_p$, again a contradiction. □

In this case we fix the following notation

$$c = \operatorname{lcm}\left(k, \frac{s_p}{r_p}\right) \quad \text{and} \quad L = \langle a, b^c \rangle ,$$

and the distinguished Wedderburn components A of $\mathbb{Q}G$ are those with a center isomorphic to a subfield F of $\mathbb{C}$ satisfying the following conditions:

(D1) F is contained in $\mathbb{Q}_{m_{\pi'} s_p}$ and $\operatorname{Deg}(A) = [\mathbb{Q}_{m_{\pi'} s_p} : F] = c$.

(D2) $F \cap \mathbb{Q}_{m_{\pi'}} = (\mathbb{Q}_{m_{\pi'}})^R$ and $F \cap \mathbb{Q}_{s_p} = \mathbb{Q}_{r_p}$.

We first show that such Wedderburn component occurs.

<u>Claim 2</u>. If $K_0 = \langle a_{\pi \setminus \{p\}}, b^c \rangle$, then (L, K_0) is a strong Shoda pair of G and $A = \mathbb{Q}Ge(G, L, K_0)$ satisfies (D1) and (D2).

Proof. Indeed, first of all $[b^c, a] = [b^c_\pi, a_\pi] \in \left\langle a_{\pi \setminus \{p\}}, a_p^{\max(k_p r_p, s_p)} \right\rangle \subseteq K_0$, because $a_p^{s_p} = (b_p^c)^{n_p / \max(k_p, s_p/r_p)} \in K_0$. This proves that K_0 is normal in G. Moreover, $L = \langle a, K_0 \rangle$, and hence L/K_0 is cyclic. In addition, $K_0 \cap \langle a \rangle = \left\langle a_{\pi \setminus \{p\}}, a_p^{s_p} \right\rangle$. Finally, if $x \in G \setminus L$, then $x = a^i b^t$ for t a proper divisor of c. If $k \nmid t$, then $1 \neq [x, a_{\pi'}] \in \langle a_{\pi'} \rangle$ and hence $[x, a_{\pi'}] \notin K_0$. Otherwise

$\frac{s_p}{r_p} \nmid t$ and hence $\langle [x, a_p] \rangle = \left\langle a_p^{t_p r_p} \right\rangle \not\subseteq K_0$. This proves that (L, K_0) is a strong Shoda pair of G, by Theorem 1.19. Now we take $e = e(G, L, K_0)$ and $A = \mathbb{Q}Ge$. As K_0 is normal in G and L/K_0 is cyclic of order $m_{\pi'} s_p$ and generated by aK_0, it follows that A is isomorphic to a cyclic algebra $(\mathbb{Q}_{m_{\pi'} s_p} / \mathbb{Q}_{m_{\pi'} s_p}^{\mathrm{Res}_{m_{\pi'} s_p}(\gamma)}, \left\langle \mathrm{Res}_{m_{\pi'} s_p}(\gamma) \right\rangle, a)$. Therefore $\mathrm{Deg}(A) = [G : L] = c$ and its center is isomorphic to $F = \mathbb{Q}_{m_{\pi'} s_p}^{\mathrm{Res}_{m_{\pi'} s_p}(\gamma)}$, which clearly satisfies (D1) and (D2). □

The next goal is to describe the Wedderburn components of $\mathbb{Q}G$ satisfying conditions (D1) and (D2). Let A be such a component. By Theorem 1.19 and condition (D1), $A = \mathbb{Q}Ge(G, L, K)$ for a subgroup K of L the conditions of Theorem 1.19 hold. Then the following statements hold where $C = \mathrm{Core}_G(K)$:

(V1) $a_{\pi \setminus \{p\}}^4, b_{p'}^{4c} \in \mathrm{Core}_G(K)$.

(V2) If either $v_2(|a|) \leq 1$ or $\langle a \rangle$ has an element of order 4 which is central in G, then $a_{\pi \setminus \{p\}}^2 \in C$.

(V3) If $a_{\pi \setminus \{p\}}^2 \in C$ or k is even, then $b_{p'}^{2c} \in C$.

(V4) $a_p^{\max(k_p r_p, s_p)} \in K$.

Indeed, suppose that F has a root of unity of order q with q prime. The hypothesis $F \subseteq \mathbb{Q}_{m_{\pi'} s_p}$ implies that $q \in \pi' \cup \{2, p\}$. However, the hypothesis $F \cap \mathbb{Q}_{m_{\pi'}} = (\mathbb{Q}_{\pi'})^R$ implies that $q \notin \pi'$ because $\langle a \rangle$ does not have central elements of order q. Therefore $q \in \{2, p\}$ and hence (V1)-(V3) follow directly from Lemma 4.3 and Lemma 4.4. Statement (V4) is easy because $a_p, b_p^{\max(k_p, s_p/r_p)} \in L$ and hence $a_p^{\max(k_p r_p, s_p)} = [b^{\max(k_p, s_p/r_p)}, a_p] \in K$.

Let $M = \left\langle a_{\pi \setminus \{p\}}^4, a_p^{\max(k_p r_p, s_p)}, b_{p'}^{4c} \right\rangle$. Observe that M is normal in G because $[b_{p'}^{4c}, a] = [b_{p'}^{4c}, a_{\pi \setminus \{p\}}] \in \left\langle a_{\pi \setminus \{p\}}^4 \right\rangle \subseteq M$.

Claim 3. L_p/K_p is generated by either $a_p K$ or $b_p^c K$, K is normal in G and $\varphi([L : K]) = \varphi(m_{\pi'} s_p)$.

Proof. As L/K is cyclic, so is $L_p/K_p \cong (L/K)_p = L_p K/K$. Moreover, $L_p = \langle a_p, b_p^c \rangle$, and hence $(L/K)_p = L_p K/K$ is generated by either $a_p K$ or $b_p^c K$.

We now prove that K is normal in G. Observe that L is nilpotent because $a_{\pi'} \in Z(L)$ and $[b_{\pi'}, a_\pi] = 1$. As M is normal in G and $M \subseteq K$ we may assume without loss of generality that $M = 1$. Then $L_{\pi'} = \langle a_{\pi'} \rangle$ and $\pi \subseteq \{2, p\}$. Using that L is nilpotent, $K \trianglelefteq L$ and $a \in L$, it is enough to prove that b_q normalizes K_l for every pair of primes q and l. This is clear if $l \in \pi'$ because $L_{\pi'} = \langle a_{\pi'} \rangle$. It is also clear if $q \in \pi'$ because $[b_{\pi'}, a_\pi] = 1$. Moreover as G_π is nilpotent the result is also clear if $q \neq l$ and $q, l \in \pi$. It remains to consider the case $q = l \in \pi$.

Let us first consider the case $q = l \neq p$, i.e. $q = l = 2$. Then L_2 is either abelian of exponent at most 4 or L_2 is either D_8, Q_8 or $C_4 \rtimes C_4$ with $L_2' = \langle a_2^2 \rangle \subseteq K_2$. In the second case, b_2 normalizes K_2 so we assume that L_2 is abelian. Now, by assumption $a_2^4 = 1$ so it follows that G_2 is either abelian or $|a_2| = 4$ and $a_2^{b_2} = a_2^{-1}$. In the first case clearly b_2 normalizes every subgroup of L_2. In the second case either $a_2^2 \in K$ or c is even and $K_2 \subseteq \langle a_2^2, b_2^c \rangle \subseteq C_G(b_2)$. In both cases K_2 is normalized by b_2.

It remains to show that b_p normalizes K_p. Otherwise $p \mid d$, where $d = [G : N]$ and $N = N_G(K) = \left\langle a, b^d \right\rangle$. As L/K is cyclic, $L = \langle u, K \rangle$ for some u and $A \cong M_{[G:N]}(\mathbb{Q}_h * \langle \rho \rangle)$ with $h = [L : K]$ and $\rho(\zeta_h) = \zeta_h^x$, if $u^{b^d} K = u^x K$. Moreover, as $L_p = \left\langle a_p, b_p^c \right\rangle$, $(L/K)_p = L_p K/K$ is generated by either $a_p K$ or $b_p^c K$. So we may assume that u_p is either a_p or b_p^c. In the second case, $(L/K)_p$ is central in $(N_G(K)/K)_p$ and hence $h_p \leq s_p$ by condition (D1) and $h_p = r_p$ by condition (D2). In the first case, $\langle x \rangle_{h_p} = \left\langle (1 + r_p)^d \right\rangle_{h_p}$ and if $r_p < h_p$, then $v_p((1 + r_p)^d) > v_p(r_p)$ as $p \mid d$. Hence if pr_p divides h_p, then F has a central element of order pr_p in contradiction with (D2). This proves that h_p divides r_p. Therefore $a_p^{r_p} \in K$ so that $[b_p, a_p] \in K_p$. This implies that $[b_p, G_p] \subseteq K_p$ and hence b_p normalizes K_p, as desired. This finishes the proof of the normality of K in G.

As K is normal in G, $A \cong \mathbb{Q}_{[L:K]} * G/L$ and $G/L = \langle bL \rangle$ where the action ρ of the crossed product is given by $\rho(\zeta_{[L:K]}) = \zeta_{[L:K]}^x$, if $L = \langle u, K \rangle$ and $u^b \in u^x K$. Moreover, $[G : L] = \mathrm{Deg}(A) = c = [\mathbb{Q}_{m_{\pi'} s_p} : F] = \frac{\varphi(m_{\pi'} s_p)}{\dim_{\mathbb{Q}}(F)}$. Thus

$$c\varphi([L : K]) = [G : L]\varphi([L : K]) = \dim_{\mathbb{Q}}(A) = c^2 \dim_{\mathbb{Q}} F = c\varphi(m_{\pi'} s_p)$$

and therefore $\varphi([L : K]) = \varphi(m_{\pi'} s_p)$, as desired. □

Claim 4. One of the following conditions holds:

(i) $[L : K] = m_{\pi'} s_p$ or $p \neq 2$ and $[L : K] = 2m_{\pi'} s_p$,

(ii) $p \neq 2$ and $[L:K] = 4\frac{m_{\pi'}}{q}p^t$, with $p^t \geq s_p$, $q = 1 + 2\frac{p^t}{s_p} \in \pi'$ and $v_q(m_{\pi'}) = 1$.

(iii) $p = 2$ and $[L:K] = \frac{m_{\pi'}}{q_1 \cdots q_l}2^t$, with $l \geq 1$, $2^t > s_2$, $q_1, ..., q_l \in \pi'$, $\varphi(q_1 \cdots q_l) = \frac{2^t}{s_2}$ and $v_{q_i}(m_{\pi'}) = 1$ for every i.

Proof. By (V1), $[L:K]_{\pi'}$ divides $m_{\pi'}$. Let $[L:K]_p = p^t$, $[L:K]_{\pi'} = p_1^{\alpha_1} \cdots p_w^{\alpha_w}$ and $m_{\pi'} = p_1^{\beta_1} \cdots p_w^{\beta_w} q_1^{\gamma_1} \cdots q_l^{\gamma_l}$ with $p_1, \dots, p_w, q_1, \dots, q_l$ the different elements of π'.

Let us first assume that $p \neq 2$. By (V1), $[L:K]_2$ divides 4. By condition (D2), $r_p \mid p^t$ and hence $t \geq 1$. By Claim 3, $\varphi([L:K]) = \varphi(m_{\pi'}s_p)$ and therefore

$$\varphi([L:K]_2)p^t p_1^{\alpha_1 - 1} \cdots p_w^{\alpha_w - 1} = s_p p_1^{\beta_1 - 1} \cdots p_w^{\beta_w} q_1^{\gamma_1 - 1} \cdots q_l^{\gamma_l - 1}(q_1 - 1) \cdots (q_l - 1).$$

Then $\alpha_i = \beta_i$ for every $i = 1, \dots, w$ and as $[L:K]_2 \mid 4$ and q_i is odd for every i it follows that $s_p \leq p^t$ and either $l = 0$, $s_p = p^t$ and $[L:K]_2 \mid 2$ or $[L:K]_2 = 4$, $l = 1$, $q_1 = 1 + 2\frac{p^t}{s_p}$ and $\gamma_1 = 1$. This proves that either (i) or (ii) holds.

Now, let us consider the case when $p = 2$. Then the equality $\varphi([L:K]) = \varphi(m_{\pi'}s_2)$ yields

$$2^t p_1^{\alpha_1 - 1} \cdots p_w^{\alpha_w - 1} = s_2 p_1^{\beta_1 - 1} \cdots p_w^{\beta_w - 1} q_1^{\gamma_1 - 1} \cdots q_l^{\gamma_l - 1}(q_1 - 1) \cdots (q_l - 1).$$

Again $\alpha_i = \beta_i$ for every $i = 1, ..., w$ and, as each q_i is odd, $\gamma_i = 1$ for every $i = 1, ..., l$. So the equation gets reduced to:

$$2^t = s_2(q_1 - 1) \cdots (q_l - 1).$$

If $l = 0$, then condition (i) holds, and otherwise condition (iii) holds. □

Now we have enough information to prove that $(\Delta^G)_p \cong (\Delta^H)_p$ in this case. Recall that both G and H are given by a presentation as in (4.1) with the same parameters m, n, s but now the automorphism γ differs for G and H. We denote them γ^G and γ^H respectively. We know that $R^G = R^H$, i.e. $\langle \text{Res}_{m_{\pi'}}(\gamma^G) \rangle = \langle \text{Res}_{m_{\pi'}}(\gamma^H) \rangle$ and hence we may assume without loss of generality that $\text{Res}_{m_{\pi'}}(\gamma^G) = \text{Res}_{m_{\pi'}}(\gamma^H)$.

In the remainder of the proof we will consider restrictions of γ^G and γ^H to several cyclotomic fields $\mathbb{Q}_d$ with $d \mid m$. For shortness we will abuse the notation and simplify $\mathbb{Q}_d^{\text{Res}_d(\gamma^G)}$ by writing $\mathbb{Q}_d^{\gamma^G}$, and similarly for H. We fix the Wedderburn component $A = \mathbb{Q}Ge(G, L, K_0)$

of KG with K_0 as in Claim 2. Then the center of A is isomorphic to $\mathbb{Q}(m_{\pi'}s_p)^{\gamma^G}$. As $\mathbb{Q}G \cong \mathbb{Q}H$, $\mathbb{Q}H$ has a Wedderburn component $\mathbb{Q}He(H,L,K)$ isomorphic to A with (L,K) a strong Shoda pair of H. By Claim 3, K is normal in H. Moreover, $[L:K]$ satisfies one of the conditions of Claim 4 and $(L/K)_p$ is generated by either a_pK or b_p^cK. Let $p^t = [L:K]_p$. If $(L/K)_p$ is generated by $b_p^cK_p$, then $\mathbb{Q}_{r_p} = \mathbb{Q}_{s_p}^{\gamma^G} = \mathbb{Q}_{p^t}$ and hence $m'_p > r_p = p^t \geq s_p \geq m'_p$, a contradiction. Therefore, $(L/K)_p$ is generated by a_pK. Thus $(L/K)_{\pi'\cup\{p\}}$ is generated by $a_{\pi'\cup\{p\}}K$. Therefore the center of $\mathbb{Q}Ge(H,L,K)$ is isomorphic to a subfield F of $\mathbb{Q}_{[L:K]}$ such that $F \cap \mathbb{Q}_{[L:K]_{\pi'\cup\{p\}}} = \mathbb{Q}^{\gamma^H}_{[L:K]_{\pi'\cup\{p\}}}$. Then $\mathbb{Q}^{\gamma^G}_{m_{\pi'}s_p} = \mathbb{Q}^{\gamma^H}_{[L:K]_{\pi'\cup\{p\}}}$.

We deal separately with the three cases of Claim 4.

Case (i). Suppose first that either $[L:K] = m_{\pi'}s_p$ or $p \neq 2$ and $[L:K] = 2m_{\pi'}s_p$. Then, $\mathbb{Q}_{m_{\pi'}s_p} = \mathbb{Q}_{[L:K]_{\pi'\cup\{p\}}}$ and hence $\mathbb{Q}^{\gamma_G}_{m_{\pi'}s_p} = \mathbb{Q}^{\gamma_H}_{m_{\pi'}s_p}$. Thus, Galois Theory yields $\left\langle \mathrm{Res}_{m_{\pi'}s_p}(\gamma^G)\right\rangle = \left\langle \mathrm{Res}_{m_{\pi'}s_p}(\gamma^H)\right\rangle$. Since $m'_p \mid s_p$, we have $\mathrm{Res}_{m'_{\pi'\cup\{p\}}}((\Delta^G)_p) = \mathrm{Res}_{m'_{\pi'\cup\{p\}}}(\left\langle\gamma^G\right\rangle_p) = \mathrm{Res}_{m'_{\pi'\cup\{p\}}}(\left\langle\gamma^H\right\rangle_p) = \mathrm{Res}_{m'_{\pi'\cup\{p\}}}((\Delta^H)_p)$. As $\mathrm{Res}_{m'_{\pi\setminus\{p\}}}((\Delta^G)_p) = \mathrm{Res}_{m'_{\pi\setminus\{p\}}}((\Delta^H)_p) = 1$. We conclude that $(\Delta^G)_p = (\Delta^H)_p$, as desired.

Case (ii). Suppose now that $p \neq 2$ and $[L:K] = 4\frac{m_{\pi'}}{q}p^t$, with $p^t \geq s_p$, $q = 1 + 2\frac{p^t}{s_p} \in \pi'$ and $v_q(m_{\pi'}) = 1$. Then $F = \mathbb{Q}^{\alpha}_{4\frac{m_{\pi'}}{q}s_p} = \mathbb{Q}^{\gamma^G}_{m_{\pi'}s_p}$, where $\mathrm{Res}_{\frac{m_{\pi'}}{q}p^t}(\alpha) = \mathrm{Res}_{\frac{m_{\pi'}}{q}p^t}(\gamma^H)$ and $\zeta_4^{\alpha} = \zeta_4^i$, if $u^b = u^i$ with $L/K = \langle uK\rangle$. Thus, $F = \mathbb{Q}^{\gamma^H}_{\frac{m_{\pi'}}{q}s_p} = \mathbb{Q}^{\gamma^G}_{\frac{m_{\pi'}}{q}s_p}$, and by Galois Theory, $\left\langle \mathrm{Res}_{\frac{m_{\pi'}}{q}s_p}(\gamma^G)\right\rangle = \left\langle \mathrm{Res}_{\frac{m_{\pi'}}{q}s_p}(\gamma^H)\right\rangle$. Moreover, $\gamma^H(\zeta_4) = \zeta_4^{-1}$ and, as $\mathrm{Res}_{m_{\pi'}}(\gamma^G) = \mathrm{Res}_{m_{\pi'}}(\gamma^H)$, we have $\mathbb{Q}_q^{\gamma^H} = \mathbb{Q}_q^{\gamma^G} = \mathbb{Q}$. The first implies that $(L/K)_2$ is not generated by $b_2^cK_2$ and hence it is generated by a_2K_2, so we may assume that $\alpha = \gamma^H$.

Assume first that $s_p = p^t$. Then $q = 3$ and $F = \mathbb{Q}^{\gamma^H}_{\frac{m_{\pi'}}{3}s_p} = \mathbb{Q}^{\gamma^G}_{\frac{m_{\pi'}}{3}s_p}$, and by Galois Theory, $\left\langle \mathrm{Res}_{\frac{m_{\pi'}}{3}s_p}(\gamma^G)\right\rangle = \left\langle \mathrm{Res}_{\frac{m_{\pi'}}{3}s_p}(\gamma^H)\right\rangle$. Moreover, $\mathbb{Q}_3^{\gamma^G} = \mathbb{Q}_3^{\gamma^H} = \mathbb{Q}$, so that $\gamma^H(\zeta_3) = \gamma^G(\zeta_3) = \gamma^G(\zeta_3) = \zeta_3^{-1}$. Then $\mathrm{Res}_{m_{\pi'}s_p}(\langle\gamma^G\rangle)_p = \mathrm{Res}_{m_{\pi'}s_p}(\langle\gamma^H\rangle)_p$, as p is odd, and, as in the previous case, we deduce that $(\Delta^G)_p = (\Delta^H)_p$.

Now we assume $p^t > s_p$. Since also $r_p < m'_p \leq s_p$, we have $\frac{p^t}{r_p} > \max(\frac{p^t}{s_p}, \frac{s_p}{r_p})$. If $m_{\pi'} = q$, then $(\mathbb{Q}_{4p^t})^{\gamma^H} = (\mathbb{Q}_{qs_p})^{\gamma^G} = \mathbb{Q}_{r_p}$ and hence $k_p = q - 1 = 2\frac{p^t}{s_p}$. Then $\max\left(\frac{p^t}{s_p}, \frac{s_p}{r_p}\right) = c_p = \mathrm{Deg}(A)_p = [\mathbb{Q}_{4p^t} : \mathbb{Q}_{r_p}]_p = \frac{p^t}{r_p}$, a contradiction. Thus $m_{\pi'} = xq$ with $x > 1$. By (D1) and the description of A (see Proposition 1.18), we have $[\mathbb{Q}_{4xp^t} : F] = [\mathbb{Q}_{qxs_p} : F] = \mathrm{Deg}(A) = c$. By looking at the p-part of these degrees we obtain:

$$c_p = \max\left(\bar{k}_p, \frac{p^t}{r_p}\right) = \max\left(\bar{k}_p, \frac{p^t}{s_p}, \frac{s_p}{r_p}\right), \tag{4.10}$$

where $\bar{k} = |\operatorname{Res}_x(\gamma^G))| = |\operatorname{Res}_x(\gamma^H))|$. As $\frac{p^t}{r_p} > \max\left(\frac{p^t}{s_p}, \frac{s_p}{r_p}\right)$, necessarily $\bar{k}_p \geq \frac{p^t}{r_p}$. So $c_p = \bar{k}_p \geq \frac{p^t}{r_p} > \max\left(\frac{p^t}{s_p}, \frac{s_p}{r_p}\right)$. As $\langle \operatorname{Res}_{xs_p}(\gamma^H)\rangle = \langle \operatorname{Res}_{xs_p})\gamma^G)\rangle$, $\operatorname{Res}_{xs_p}(\gamma^G)_p = (\operatorname{Res}_{xs_p}(\gamma^H)_p)^u$ for certain u coprime with p. As $p \neq 2$ we can even choose u to be odd. Then,

$$\operatorname{Res}_x((\gamma^H)_p) = \operatorname{Res}_x((\gamma^G)_p) = (\operatorname{Res}_x((\gamma^H)_p))^u$$

so $u \equiv 1 \mod |\operatorname{Res}_x(\gamma^H)_p|$. Moreover, $|\operatorname{Res}_x(\gamma^H)_p)| = \bar{k}_p \geq \frac{p^t}{r_p} > \frac{p^t}{s_p}$, so $u \equiv 1 \mod \frac{p^t}{s_p}$ and as u is odd we have $u \equiv 1 \mod 2$. Thus $u \equiv 1 \mod q-1$, and as $\operatorname{Res}_{m_{\pi'}}(\gamma^G) = \operatorname{Res}_{m_{\pi'}}(\gamma^H)$ we have $\operatorname{Res}_q(\gamma^G) = \operatorname{Res}_q(\gamma^H) = \operatorname{Res}_q(\gamma^H)^u$. Then, $(\gamma^G)_p = ((\gamma^H)_p)^u$, because the equality happens both restricting to q and to xs_p. So the p-th parts of γ^G and γ^H generate the same subgroup and as $s_p \geq m'_p$ we obtain the desired conclusion:

$$(\Delta^G)_p = \operatorname{Res}_{m_{\pi'}m'_p}(\langle(\gamma^G)_p\rangle) = \operatorname{Res}_{m_{\pi'}m'_p}(\langle(\gamma^H)_p\rangle) = (\Delta^H)_p.$$

Case (iii). Finally suppose that $p = 2$ and $[L : K] = \frac{m_{\pi'}}{q_1\cdots q_l}2^t$, with $l \geq 1$, $2^t > s_2$, $q_1, ..., q_l \in \pi'$, $\varphi(q_1 \cdots q_l) = \frac{2^t}{s_2}$ and $v_{q_i}(m_{\pi'}) = 1$ for every i. Let $x = \frac{m_{\pi'}}{q_1\cdots q_l}$. Arguing as in the previous case we obtain

$$c_2 = \bar{k}_2 \geq \frac{2^t}{r_2} > \max\left(\frac{2^t}{s_2}, \frac{s_2}{r_2}\right) \geq (q_1 - 1)\cdots(q_l - 1),$$

and, from $2^t > s_2$ we get that $b^l K$ does not generates L/K and then that $F = (\mathbb{Q}_{x2^t})^{\gamma^H} = (\mathbb{Q}_{xs_2})^{\gamma^G}$ Having in mind the previous inequalities the same argument as in the previous case yields the desired conclusion, i.e. $(\Delta^G)_2 = (\Delta^H)_2$.

Case 2. Suppose that $\epsilon^{p-1} = 1$ and $s_p < m'_p$.

Claim 5. In this case $s_p < m_p$, $n_p < k_p r_p$ and $\frac{k_p s_p}{n_p} r_p \geq m'_p$.

Proof. As $s_p < m'_p = \min(m_p, k_p r_p, \max(r_p, s_p, r_p\frac{k_p s_p}{n_p}))$, clearly $s_p < m_p$ and $s_p < \max(s_p, r_p, \frac{k_p s_p}{n_p} r_p)$. If $s_p < r_p$, then, by Theorem B.(2d), we have $n_p < k_p s_p$, so $s_p < r_p < r_p\frac{k_p s_p}{n_p}$, and from this equation we easily get $n_p < k_p r_p$. Otherwise, $s_p < r_p\frac{k_p s_p}{n_p}$ and again we get $n_p < k_p r_p$.

To prove the last inequation, firstly observe that $\max(s_p, r_p, r_p\frac{k_ps_p}{n_p}) \neq s_p$, for otherwise $s_p < m'_p = \min(m_p, r_pk_p, s_p) \leq s_p$, a contradiction. So $\max(s_p, r_p, r_p\frac{k_ps_p}{n_p})$ is either r_p or $r_p\frac{k_ps_p}{n_p}$. In the later case $m'_p = \min(m_p, k_pr_p, r_p\frac{k_ps_p}{n_p}) \leq r_p\frac{k_ps_p}{n_p}$, as desired. Otherwise, $r_p > r_p\frac{k_ps_p}{n_p}$. Then, $k_ps_p < n_p < k_pr_p$, so $s_p < r_p$, in contradiction with Theorem B.(2d). □

In this case the distinguished Wedderburn components A of $\mathbb{Q}G$ are those with center isomorphic to a subfield F of $\mathbb{C}$ satisfying the following conditions:

(E1) F is contained in $\mathbb{Q}_{m_{\pi'}m'_p}$ and $\operatorname{Deg}(A) = [\mathbb{Q}_{m_{\pi'}m'_p} : F] = k$.

(E2) $F \cap \mathbb{Q}_{m_{\pi'}} = (\mathbb{Q}_{m_{\pi'}})^R$ and $F \cap \mathbb{Q}_{m'_p} = \mathbb{Q}_{r_p}$.

We first show that such Wedderburn component exists. By Lemma 1.1.(1a), $v_p\left(\mathcal{S}\left(1 + r_p \mid \frac{n_p}{k_p}\right)\right) = \frac{n_p}{k_p}$. Write $\mathcal{S}\left(1 + r_p \mid \frac{n_p}{k_p}\right) = z\frac{n_p}{k_p}$. Fix an integer y such that

$$z \equiv y\frac{k}{k_p} \mod \frac{m_p}{s_p}.$$

As $p \nmid z$ and $s_p < m_p$, we have $p \nmid y$.

Claim 6. If $L = \langle a, b^k \rangle$ and $K_0 = \left\langle a_{\pi\setminus\{p\}}, a_p^{\frac{r_ps_pk_p}{n_p}}, b^{-yk}a_p^{\frac{s_pk_p}{n_p}}, b_{p'}^k \right\rangle$, then (L, K_0) is a strong Shoda pair of G and $A = \mathbb{Q}Ge(G, L, K_0)$ satisfies (E1) and (E2).

Proof. As $p \in \pi$, $[b_p, a_{\pi\setminus\{p\}}] = 1$. Thus $\left\langle [b_p^{-yk}a_p^{\frac{s_pk_p}{n_p}}, a] \right\rangle = \langle [b_p^{-yk}, a_p] \rangle = \left\langle [b_p^{k_p}, a_p] \right\rangle = \left\langle [a_p^{r_pk_p} \right\rangle \subseteq \left\langle a_p^{\frac{r_ps_pk_p}{n_p}} \right\rangle \in K_0$, since $s_p \mid n_p$. Also, $[b_{p'}^k, a] = [b_{\pi\setminus\{p\}}^k, a_\pi] \in \left\langle a_{\pi\setminus\{p\}} \right\rangle \in K_0$. This proves that K_0 is normal in G. Moreover, $L = \langle a, K_0 \rangle$, and hence L/K_0 is cyclic. In order to prove that L/K_0 is maximal abelian in G/K_0 observe that $|b_p^{-yk}a_p^{\frac{s_pk_p}{n_p}} \langle a \rangle| = |b_p^{yk} \langle a \rangle| = \frac{n_p}{k_p}$ and $(b_p^{-yk}a_p^{\frac{s_pk_p}{n_p}})^{\frac{n_p}{k_p}} = b_p^{-yk\frac{n_p}{k_p}} a_p^{\frac{s_pk_p}{n_p}\mathcal{S}\left(1+r_p \mid \frac{n_p}{k_p}\right)} = a_p^{-ys_p\frac{k}{k_p}+zs_p} = 1$. Then $|b_p^{-yk}a_p^{\frac{s_pk_p}{n_p}} \langle a \rangle| = |b_p^{-yk}a_p^{\frac{s_pk_p}{n_p}}| = \frac{n_p}{k_p}$, and therefore $K_0 \cap \langle a \rangle = \left\langle a_{\pi\setminus\{p\}}, a_p^{\frac{r_ps_pk_p}{n_p}} \right\rangle \subseteq \langle a_\pi \rangle$. If $x \in G \setminus L$, then $x = a^ib^t$ for t a proper divisor of k, and hence $1 \neq [x, a_{\pi'}] \in \langle a_{\pi'} \rangle$. Thus $[x, a_{\pi'}] \notin K_0$. This shows that (L, K_0) is a strong Shoda pair of G.

Now we take $e = e(G, L, K_0)$ and $A = \mathbb{Q}Ge$. As K_0 is normal in G and L/K_0 is cyclic of order $m_{\pi'}m'_p$ and generated by aK_0, it follows that A is isomorphic to a cyclic algebra $\mathbb{Q}_{m_{\pi'}m'_p} * \left\langle \operatorname{Res}_{m_{\pi'}m'_p}(\gamma^G) \right\rangle$. Therefore A satisfies (E1) and (E2). □

The remaining arguments in this case follow exactly as the previous one, except changing s_p by m'_p where it corresponds.

Case 3: Suppose now that $\epsilon^{p-1} = -1$, i.e. $p = 2$ and $\epsilon = -1$. In this case, Theorem B.(2d) gives us the following properties: s divides m, $|\Delta|$ divides n, $\frac{m_2}{r_2} \le n_2$, $m_2 \le 2s_2$ and $s_2 \ne n_2 r_2$. If moreover $4 \mid n$, $8 \mid m$ and $k_2 < n_2$, then $r_2 \le s_2$. Having in mind that $m'_2 \ne r_2$ we have $4 \le k_2$ and $4r_2 \le m_2$. This together with $s_2 \ne n_2 r_2$ implies that

$$m'_2 = \begin{cases} \frac{m_2}{2}, & \text{if } k_2 < n_2 \text{ and } 2s_2 = m_2 < n_2 r_2; \\ m_2, & \text{otherwise.} \end{cases}$$

In this case we take

$$c = \operatorname{lcm}\left(k, \frac{m'_2}{r_2}\right) \quad \text{and} \quad L = \langle a, b^c \rangle$$

and the distinguished Wedderburn components A of $\mathbb{Q}G$ are those with a center isomorphic to a subfield F of $\mathbb{C}$ satisfying the following conditions:

(F1) F is contained in $\mathbb{Q}_{m_{\pi'} m'_2}$ and $\operatorname{Deg}(A) = [\mathbb{Q}_{m_{\pi'} m'_2} : F] = c$.

(F2) $F \cap \mathbb{Q}_{m_{\pi'}} = (\mathbb{Q}_{m_{\pi'}})^R$ and $F \cap \mathbb{Q}_{m'_2} = (\mathbb{Q}_{m'_2})^\sigma$, where $\sigma(\zeta_{m'_2}) = \zeta_{m'_2}^{-1+r_2}$.

Claim 7. Let

$$K_0 = \begin{cases} \left\langle a_{\pi\setminus\{2\}}, b^c \right\rangle, & \text{if } b_2^c \notin \langle a \rangle \\ \left\langle a_{\pi\setminus\{2\}}, b_{2'}^c \right\rangle, & \text{otherwise.} \end{cases}$$

Then (L, K_0) is a strong Shoda pair of G and $A = \mathbb{Q}Ge(G, L, K_0)$ satisfies (F1) and (F2).

Proof. We claim that $[L : K_0] = m_{\pi'} m'_2$. Indeed, first of all observe that

$$K_0 \cap \langle a \rangle = \begin{cases} \left\langle a_{\pi\setminus\{2\}}, a_2^{\frac{m_2}{2}} \right\rangle, & \text{if } b_2^c \notin \langle a \rangle \text{ and } m_2 = 2s_2; \\ \left\langle a_{\pi\setminus\{2\}} \right\rangle; & \text{otherwise.} \end{cases}$$

Therefore

$$[L : K_0] = \begin{cases} m_{\pi'} \frac{m_2}{2}, & \text{if } b_2^c \notin \langle a \rangle \text{ and } m_2 = 2s_2; \\ m_{\pi'} m_2; & \text{otherwise.} \end{cases}$$

Thus, if $m_2 \neq 2s_2$ or $k_2 = n_2$, then $[L : K_0] = m_{\pi'} m_2 = m_{\pi'} m_2'$. Suppose that $m_2 = 2s_2$ and $k_2 \neq n_2$. Then $k_2 < n_2$ and, as $m_2 \leq n_2 r_2$ we have that $m_2' = m_2$ if and only if $m_2 = n_2 r_2$. Then $b_2^c \in \langle a \rangle$ if and only if $\frac{m_2'}{r_2} \geq n_2$ if and only if $m_2 = m_2'$.

We now prove that K_0 is normal in G. This is easy if $b_2^c \in \langle a \rangle$ because $[b_{2'}^c, a] = [b_{2'}^c, a_{\pi \setminus \{2\}}] \subseteq \left\langle a_{\pi \setminus \{2\}} \right\rangle \subseteq K_0$. Suppose otherwise that $b_2^c \not\in \langle a \rangle$. If $[b_2^c, a_2] = 1$, then $[b^c, a] = [b_\pi^c, a_\pi] \in \left\langle a_{\pi \setminus \{2\}} \right\rangle \in K_0$. Otherwise, $\frac{m_2}{r_2} > c_2$ and and recalling that we are assuming that $m_2' \neq r_2$ it follows that $m_2' = \frac{m_2}{2r_2} = c_2$ and $s_2 = \frac{m_2}{2}$. Using Lemma 1.1.(2a), it follows that $[b_2^c, a] = a_2^{\frac{m_2}{2}} \in \langle b_2^c \rangle \subseteq K_0$.

Moreover, $L = \langle a, K_0 \rangle$, and hence L/K_0 is cyclic. In order to prove that L/K_0 is maximal abelian in G/K_0, we argue by contradiction. So we take $x \in G \setminus L$ and assume that $[x, L] \subseteq K_0$. Then $x = a^i b^t$ for t a proper divisor of c. If $k \nmid t$, then $1 \neq [x, a_{\pi'}] \in \langle a_{\pi'} \rangle$ and hence $[x, a_{\pi'}] \not\in K_0$, a contradiction. Thus $k \mid t$ and hence $\frac{m_2'}{r_2} \nmid t$, i.e. $t_2 r_2 < m_2'$. By assumption, $[x, a_2] \in K_0$. Observe that

$$\langle [x, a_2] \rangle = \begin{cases} \langle a_2^2 \rangle, & \text{if } t_2 = 1; \\ \left\langle a_2^{t_2 r_2} \right\rangle, & \text{otherwise.} \end{cases}$$

The assumptions $m_2' \neq r_2$ implies that $m_2 > 2r_2 \geq 4$ and hence $a_2^2 \not\in K_0$. Thus $1 \neq a_2^{t_2 r_2} \in K_0$ and hence $b_2^c \not\in \langle a \rangle$, $m_2 = 2s_2$ and $t_2 r_2 = \frac{m_2}{2} < m_2'$. Therefore $m_2' = m_2$. Since $m_2' \neq r_2$ and $b_2^c \not\in \langle a \rangle$, it follows that $4 \leq k_2 = k_2 < n_2$ and $4r_2 \leq m$. Thus, by the definition of m_2', we have that $s_2 \neq n_2 r_2$ and $m_2 \geq n_2 r_2$. By Theorem B.(2c), $m_2 = n_2 r_2$ and hence $c_2 \geq n_2$, so that $b_2^c \in \langle a \rangle$, a contradiction.

Now we take $e = e(G, L, K_0)$ and $A = \mathbb{Q}Ge$. As K_0 is normal in G and L/K_0 is cyclic of order $m_{\pi'} m_2'$ and generated by aK_0, it follows that A is isomorphic to a cyclic algebra $\mathbb{Q}_{m_{\pi'} m_2'} * \left\langle \mathrm{Res}_{m_{\pi'} m_2'}(\gamma^G) \right\rangle$. Therefore $\mathrm{Deg}(A) = [G : L] = c$ and the center of A satisfies (F1) and (F2). □

As in Case 1 we now consider an arbitrary Wedderburn component A of $\mathbb{Q}H$ with center isomorphic to a field F and satisfying conditions (F1) and (F2). As $\mathrm{Deg}(A) = c$, we have $A = \mathbb{Q}He(H, L, K)$ for a strong Shoda pair (L, K) of H. As L/K is abelian, $\left\langle a_2^{\max(k_2 r_2, m_2')} \right\rangle = \langle [a_2, b_2^c] \rangle \subseteq K$ and combining this with Lemma 4.3 it follows that K contains $M = \left\langle a_{\pi\setminus\{2\}}, a_2^{\max(k_2r_2,m_2')}, b_{2'}^c \right\rangle$. Observe that M is normal in H because $[b_{2'}^c, a] = [b_{2'}^c, a_{\pi\setminus\{2\}}] \in \langle a_{\pi\setminus\{2\}}\rangle \subseteq M$.

We denote $C = \{g \in H : ge = e\} = \mathrm{Core}_H(K)$ and $N = N_H(K) = \langle a, b^t\rangle$ with $t = [H : N]$. Observe that L is nilpotent because $a_{\pi'} \in Z(L)$ and $[b_{\pi'}, a_\pi] = 1$. Moreover, $A \cong M_t(\mathbb{Q}_{[L:K]} * N/L)$ where $N/L = \langle b^t L\rangle$ where the action ρ of the crossed product is given by $\rho(\zeta_{[L:K]}) = \zeta_{[L:K]}^x$, if $L = \langle u, K\rangle$ and $u^{b^t} \in u^x K$. By Lemma 4.4, $a_{\pi\setminus\{2\}} \in K$ and $b_{2'}^c \in K$. Moreover, as L/K is abelian, $\langle [a_2, b_2^c]\rangle = \left\langle a_2^{\max(k_2r_2,m_2')}\right\rangle \subseteq K$. Thus $M \subseteq K$.

Claim 8. K is normal in H, $L = \langle a, K\rangle$ and $\varphi([L:K]) = \varphi(m_{\pi'}m_2')$.

Proof. By condition (F2), $F \cap \mathbb{Q}_{m_2'} = \mathbb{Q}_{m_2'}^\sigma$ where $\sigma(\zeta_{m_2'}) = -1 + r_2$. As $r_2 < m_2'$, it follows that $F \cap \mathbb{Q}_{m_2'}$ is not a cyclotomic field. On the other hand, $F \subseteq \mathbb{Q}_{[L:K]} \cap \mathbb{Q}_{m_{\pi'}m_2'}$, and hence $F \cap \mathbb{Q}_{[L:K]_2} = F \cap \mathbb{Q}_{\max([L:K]_2, m_2')} = F \cap \mathbb{Q}_{m_2'}$. Thus $F \cap \mathbb{Q}_{[L:K]_2}$ is not a cyclotomic field.

Since $L_2K/K = \langle a_2K, b_2^c\rangle$, $(L/K)_2$ is generated by a_2K or b_2^c. In the latter case, $F \cap \mathbb{Q}_{[L:K]_2}$ is a cyclotomic field, contradicting the previous paragraph. Thus $L_2K/K = \langle a_2, K\rangle$ and as $L = \langle K, a_{\pi'}, a_2, b^c\rangle$, it follows that $L = \langle a, K\rangle$

As in the proof of Claim 3, L is nilpotent and to prove that K is normal in H it is enough to show that $[b_2, K_2] \subseteq K_2$. Otherwise, the index d of $N_H(K)$ in H is even and hence, as $(L/K)_2$ is generated by a_2K it follows that $F \cap \mathbb{Q}_{[L:K]_2} = \mathbb{Q}_{[L:K]_2}^\tau$, where $\tau(\zeta_{[L:K]_2}) = \zeta_{[L:K]_2}^{(-1+r_2)^d}$. However, by the discussion on the cyclic p-subgroups of $\mathcal{U}_m$ with m a p-th power in subsection and using Lemma 1.1.(2a), it follows that $\left\langle (-1+r_2)^d \right\rangle_{[L:K]_2} = \langle 1 + r_2d_2\rangle_{[L:K]_2}$. Therefore $F \cap \mathbb{Q}_{[L:K]_2} = \mathbb{Q}_{r_2d_2}$, again a contradiction with the first paragraph of the proof.

The last equality follows by the same arguments as in the last paragraph of the proof of Claim 3. □

As in the previous cases we take $A = \mathbb{Q}Ge(G, L, K_0) \cong \mathbb{Q}He(H, L, K)$ for some strong Shoda pair (L, K) of H. By Claim (8), $A \cong (\mathbb{Q}(\zeta_{[L:K]}) * \langle\rho\rangle)$ and if $Z(A) \cong F$, then $\mathbb{Q}(\zeta_{m_{\pi'}m_2'})^{\gamma^G} = F = \mathbb{Q}(\zeta_{[L:K]})^{\gamma^H}$. As $L = \langle a, K\rangle$ and $a_{\pi'} \in K$ we have that $[L:K] \mid m_{\pi'}m_2$. Combining this with $m_2' \in \left\{m_2, \frac{m_2}{2}\right\}$ and $\varphi([L:K]) = \varphi(m_{\pi'}m_2')$ it is easy to see that either $[L:K] = m_{\pi'}m_2'$ or $m_2' = \frac{m_2}{2}$ and $[L:K] = \frac{m_{\pi'}}{3}m_2$. In the first case, $(\Delta^G)_2 = \left\langle (\sigma^G)_2\right\rangle = \left\langle (\sigma^H)_2\right\rangle = (\Delta^H)_2$, as desired. In the second case, $\mathrm{Res}_{\frac{m_{\pi'}}{3}m_2'}(\sigma^G) = \mathrm{Res}_{\frac{m_{\pi'}}{3}m_2'}(\sigma^H)$

and $\sigma^G(\zeta_3) = \zeta_3^{-1}$. This implies again that $(\Delta_2)^G = \mathrm{Res}_{m_{\pi'} m_2'}(\sigma^G) = \mathrm{Res}_{m_{\pi'} m_2'}(\sigma^H) = (\Delta_2)^H$, as desired.

This finishes the proof of Proposition 4.15 and completes the proof of Theorem F. □

List of Symbols

In this list, m represents an integer, p a prime, G a group, π a set of primes, H a subgroup of G; $g, h, g_1, \ldots, g_n$ are elements of G, and A and B subsets of G. In the column **Page** we have included the page number of the location where the term is defined. The list is not exhaustive, but covers most of the notation used in the document.

Notation	**Description**	**Page**
$\langle A \rangle$	Subgroup generated by A	6
$\lvert A \rvert$	Cardinal of a set A	6
$[A, B]$	Commutator of A and B,	6
	$\{[a, b],$ for every $a \in A, b \in B\}$	
A^g	Set of elements $\{a^g$ for $a \in AG\}$	6
$\mathrm{Aut}(G)$	Automorphism group of a group G	6
$\mathrm{C}_G(H)$	Centralizer of H in G	6
$\mathcal{C}_n$	Cyclic group of order n	2
$\mathrm{Core}_G(H)$	Largest normal subgroup of G contained in H	6
$\exp(G)$	Exponent of G, i. e. the smallest integer n	6
	such that $g^n = 1$ for every $g \in G$	
$\lvert g \rvert$	Order of a group element g	6
G'	Commutator of a group G	6
$\langle g_1, \ldots, g_n \rangle$	Subgroup generated by $g_1, \ldots, g_n$	6
g^G	Conjugacy class of g in G	6
g^h	$h^{-1}gh$, the conjugate of g by h	6
$[g, h]$	$g^{-1}h^{-1}gh$, the commutator of g and h	6

Notation	**Description**	**Page**
$G \times H$	Direct product of G and H	6
$[G : H]$	Index of H in G	6
$G \rtimes_m H$	Semidirect product of G and H with kernel of order m	6
$\mathcal{G}_{m,n,s,t}$	Metacyclic group given by $\left\langle a, b \mid a^m = 1, b^n = a^s, a^b = a^t \right\rangle$	19
$H \leq G$	H is a subgroup of G	6
$N \trianglelefteq G$	N is a normal subgroup of G	6
$N_G(H)$	Normalizer of H in G	6
n_p	Biggest power of a prime p dividing an integer n	2
n_π	If π is a set of primes, $n_\pi = \Pi_{p\in\pi} n_p$	2
$o_n(t)$	Order of $[t]_n$ in U_n, this is, the minimal integer m such that $t^m \equiv 1 \mod n$	2
$\pi(A)$	Set of primes dividing the cardinal of a set A	6
$\pi(n)$	Set of primes dividing an integer n	2
$\mathbb{Q}_n$	The cyclotomic field $\mathbb{Q}(\zeta_n)$	2
Res_q	Natural map $\text{Res}_q : \mathcal{U}_n \to \mathcal{U}_q, \text{Res}_q([t]_n) = [t]_q$, where $q \mid n$	2
$\mathcal{S}\,(a \mid n)$	$\sum_{i=0}^{n-1} a^i$	2
$[t]_n$	Element of $\mathcal{U}_n$ represented by $t \in \mathbb{Z}$ with $\gcd(t, n) = 1$	2
$\langle t \rangle_n$	Subgroup of $\mathcal{U}_n$ generated by $[t]_n$	2
$\mathcal{U}_n$	Group of units of the ring $\mathbb{Z}/n\mathbb{Z}$	2
$v_p(n)$	p-valuation of n: exponent of the biggest power of a prime p dividing an integer n	2
ζ_n	A complex primitive n-th root of the unity	2
$\mathcal{Z}(G)$	Center of a group G	6

Bibliography

[Bag88] Czeslaw Baginski, *The isomorphism question for modular group algebras of metacyclic p-groups*, 1988.

[BCHK$^+$13] O. Broche Cristo, A. Herman, A. Konovalov, A. Olivieri, Olteanu G., Á. del Río, and I. Van Gelder, *Wedderga — wedderburn decomposition of group algebras, version 4.7.2*, 2013.

[Ber55] S. D. Berman, *Group algebras of abelian extensions of finite groups*, Dokl. Akad. Nauk SSSR (N.S.) (1955), 431–434.

[Bey72] F. R. Beyl, *The classification of metacyclic p-groups, and other applictations to homological algebra to group theory*, ProQuest LLC, Ann Arbor, MI, 1972, Thesis (Ph.D.)–Cornell University. MR 2622614

[BN27] R. Brauer and E. Noether, *Über minimale zerfällungskörper irreduzibler darstellungen*, Ak. Berlin S. B., 1927.

[Bra29] R. Brauer, *Über systeme hyperkomplexer zahlen*, Mathematische Zeitschrift **30** (1929), no. 1, 79–107.

[Bra63] Richard Brauer, *Representations of finite groups, in" lectures in modern mathematics, vol. 1" pp. 133–175*, 1963.

[Cay54] A. Cayley, *Vii. on the theory of groups, as depending on the symbolic equation $\theta^n = 1$*, The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science **7** (1854), no. 42, 40–47.

[CR62] Ch. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Pure and Applied Mathematics, Vol. XI, Interscience Publishers, a division of John Wiley & Sons, New York-London, 1962. MR 0144979 (26 #2519)

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

[GAP12] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.5.6*, 2012.

[GBdR23a] À. García-Blázquez and Á. del Río, *A classification of metacyclic groups by group invariants*, Bull. Math. Soc. Sci. Math. Roumanie **66** (2023), no. 114, 2, 209–233.

[GBdR23b] ———, *The Isomorphism Problem for rational group algebras of finite metacyclic nilpotent groups*, http://arxiv.org/abs/2301.09463 (2023), 16 pages.

[GBdR23c] ———, *The Isomorphism Problem for rational group algebras of finite metacyclic groups*, https://arxiv.org/abs/2308.00432 (2023), 26 pages.

[GLMdR22] Diego García-Lucas, Leo Margolis, and Ángel del Río, *Non-isomorphic 2-groups with isomorphic modular group algebras*, Journal für die reine und angewandte Mathematik (Crelles Journal) **2022** (2022), no. 783, 269–274.

[Hal59] M. Hall, Jr., *The theory of groups*, The Macmillan Company, New York, N.Y., 1959. MR 0103215

[Hem00] C. E. Hempel, *Metacyclic groups*, Communications in Algebra **28** (2000), no. 8, 3865–3897.

[Her01] M. Hertweck, *A counterexample to the isomorphism problem for integral group rings*, Ann. of Math. **154** (2001), 115–138.

[Hig40a] G. Higman, *Units in group rings*, Oxford, 1940, Thesis (Ph.D.)–Univ. Oxford.

[Hig40b] ———, *The units of group-rings*, Proc. London Math. Soc. (2) **46** (1940), 231–248. MR 0002137 (2,5b)

[HOdR09] A. Herman, G. Olteanu, and Á. del Río, *Ring isomorphism of cyclic cyclotomic algebras*, Algebras and Representation Theory **12** (2009), no. 2, 365–370.

[JdR16] E. Jespers and Á. del Río, *Group Ring Groups. Volume 1: Orders and generic constructions of units*, Berlin: De Gruyter, 2016.

[Kap57] I. Kaplansky, *Problems in the theory of rings*, 1957.

[Kap70] ———, *Problems in the theory of rings* revisited, The American Mathematical Monthly **77** (1970), no. 5, 445–454.

[Kim91] W. Kimmerle, *Beitrage zur ganzzabligen darstellungstheorie endlicher gruppen*, Bayreuther Math. Schriften (1991), 139.

[Kin73] B. W. King, *Presentations of metacyclic groups*, Bull. Austral. Math. Soc. **8** (1973), 103–131. MR 323893

[KLST90] W. Kimmerle, R. Lyons, R. Sandling, and D. N. Teague, *Composition factors from the group ring and artin's theorem on orders of simple groups*, Proceedings of the London Mathematical Society **3** (1990), no. 1, 89–122.

[Lie94] S. Liedahl, *Presentations of metacyclic p-groups with applications to K-admissibility questions*, J. Algebra **169** (1994), no. 3, 965–983. MR 1302129

[Lie96] ———, *Enumeration of metacyclic p-groups*, J. Algebra **186** (1996), no. 2, 436–446. MR 1423270

[Lin71] W. Lindenberg, *Struktur und Klassifizierung bizyklischer p-Gruppen*, Gesellschaft für Mathematik und Datenverarbeitung, Bonn, 1971, BMBW-GMD-40. MR 0285609

[Mar22] L. Margolis, *The Modular Isomorphism Problem: A survey*, Jahresber. Dtsch. Math. Ver. **124** (2022), 157–196.

[Mol92] T. Molien, *Ueber systeme höherer complexer zahlen*, Mathematische Annalen **41** (1892), no. 1, 83–156.

[Mol97] ______, *Über die invarianten der linearen substitutionsgruppen*, 1897, pp. 1152–1156.

[Noe29] E. Noether, *Hyperkomplexe grössen und darstellungstheorie*, Mathematische Zeitschrift **30** (1929), no. 1, 641–692.

[NX88] M. F. Newman and M. Xu, *Metacyclic groups of prime-power order*, Adv. in Math. (Beijing) **17** (1988), 106–107. MR 0404441

[OdRS04] A. Olivieri, Á. del Río, and J. J. Simón, *On monomial characters and central idempotents of rational group algebras*, Comm. Algebra **32** (2004), no. 4, 1531–1550. MR 2100373 (2005i:16054)

[OdRS06] ______, *The group of automorphisms of the rational group algebra of a finite metacyclic group*, Comm. Algebra **34** (2006), no. 10, 3543–3567. MR 2262368 (2007g:20037)

[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, 1977. MR 470211 (81d:16001)

[Pie82] R. S. Pierce, *Associative algebras*, Graduate Texts in Mathematics, vol. 88, Springer-Verlag, New York, 1982, Studies in the History of Modern Science, 9. MR 674652 (84c:16001)

[PW50] S. Perlis and G. L. Walker, *Abelian group algebras of finite order*, Trans. Amer. Math. Soc. **68** (1950), 420–426. MR 0034758 (11,638k)

[Réd89] L. Rédei, *Endliche p-Gruppen*, Akadémiai Kiadó, Budapest, 1989. MR 992619

[Rob82] D. J. S. Robinson, *A course in the theory of groups*, Graduate Texts in Mathematics, vol. 80, Springer-Verlag, New York, 1982. MR 648604 (84k:20001)

[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*, DMV Seminar, vol. 18, Birkhäuser Verlag, Basel, 1992.

[San96] Robert Sandling, *The modular group algebra problem for metacyclic p-groups*, Proc. Amer. Math. Soc. **124** (1996), no. 5, 1347–1350. MR 1343723

[Seh78] S. K. Sehgal, *Topics in group rings*, Monographs and Textbooks in Pure and Applied Math., vol. 50, Marcel Dekker Inc., New York, 1978. MR 508515 (80j:16001)

[Sim94] Hyo-Seob Sim, *Metacyclic groups of odd order*, Proc. London Math. Soc. (3) **69** (1994), no. 1, 47–71. MR 1272420

[Wei88] A. Weiss, *Rigidity of p-adic p-torsion*, Ann. of Math. (2) **127** (1988), no. 2, 317–332. MR 932300 (89g:20010)

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

[Zas99] H. J. Zassenhaus, *The theory of groups*, Dover Publications, Inc., Mineola, NY, 1999, Reprint of the second (1958) edition. MR 1644892