THE ISOMORPHISM PROBLEM FOR RATIONAL GROUP ALGEBRAS OF FINITE METACYCLIC NILPOTENT GROUPS

ÀNGEL GARCÍA-BLÁZQUEZ AND ÁNGEL DEL RÍO

Departamento de Matemáticas, Universidad de Murcia, 30100, Murcia, Spain

Abstract. We prove that if G and H are finite metacyclic groups with isomorphic rational group algebras and one of them is nilpotent, then G and H are isomorphic.

1. Introduction

The following general problem has been largely studied since the seminal work of Graham Higman [Hig40a, Hig40b] and the influential paper of Richard Brauer [Bra51]:

> **The Isomorphism Problem for Group Rings**: Given R a commutative ring and G and H groups, does RG and RH being isomorphic as R-algebras implies that G and H are isomorphic as groups?

Suppose that G and H are finite abelian groups. Higman proved that if $\mathbb{Z}G \cong \mathbb{Z}H$, then $G \cong H$. This fails if $R = \mathbb{C}$ because if G and H are finite abelian group with the same order, then $\mathbb{C}G \cong \mathbb{C}H$. However, by a theorem of Perlis and Walker $\mathbb{Q}G \cong \mathbb{Q}H$ implies $G \cong H$ [PW50]. If now G and H are finite metabelian groups, then still we have that $\mathbb{Z}G \cong \mathbb{Z}H$ implies $G \cong H$ [Whi68]. However, Dade showed two finite metabelian groups G and H such that kG and kH are isomorphic as algebras for every field k [Dad71].

Observe that if $\mathbb{Z}G \cong \mathbb{Z}H$, then $RG \cong RH$ for every ring R. This explain why the positive results for the case where $R = \mathbb{Z}$ are more likely than for any other ring. Likewise positive results are more likely in a prime field than in any other field with the same characteristic. For a while it was expected that the Isomorphism Problem for Integral Group Ring may have a general positive answer at least for finite groups. However Hertweck showed two non-isomorphic solvable groups G and H such that $\mathbb{Z}G \cong \mathbb{Z}H$ and hence RG and RH are isomorphic for every ring R [Her01].

The aim of this paper is to contribute to the Isomorphism Problem for Group Rings with rational coefficients. The contrast between Perlis-Walker Theorem and the example of Dade suggests considering the class of metacyclic groups. The main result of the paper is the following, where π_G denotes the set of primes p for which G has a normal Hall p'-subgroup:

Theorem A. *Let G and H be two 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 A we obtain the following:

Corollary B. *If G and H are finite metacyclic groups with $\mathbb{Q}G \cong \mathbb{Q}H$ and G is nilpotent, then $G \cong H$.*

In Section 2 we introduce the main notation of the paper and review some known results. In Section 3 we prove Theorem A for p-groups, and in Section 4 we prove the whole theorem.

Observe that in Theorem A and Corollary B it is not sufficient to assume that only one of the two groups G or H is metacyclic because the following groups

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

E-mail address: `angel.garcia11@um.es, adelrio@um.es`.

1991 *Mathematics Subject Classification.* 16S34, 20C05, 20C10.

Key words and phrases. Group rings, Isomorphism Problem.

Partially supported Grant PID2020-113206GB-I00 funded by MCIN/AEI/10.13039/501100011033 and by Fundación Séneca (22004/PI/22).

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

2. Notation and preliminaries

2.1. Number theory

We adopt the convention that $0 \notin \mathbb{N}$ and prime means prime in $\mathbb{N}$. Let $n \in \mathbb{N}$. Then ζ_n denotes a complex primitive n-th root of unity and $\pi(n)$ denotes the set of prime divisors of n. If p is prime, then n_p denotes the greatest power of p dividing n and $v_p(n) = \log_p(n_p)$. Moreover $v_p(0) = \infty$. If π is a set of primes, then $n_\pi = \prod_{p\in\pi} n_p$. If $m \in \mathbb{Z}$ with $\gcd(m, n) = 1$, then $o_n(m)$ denotes the multiplicative order of m modulo n, i.e. the smallest positive integer k with $m^k \equiv 1 \mod n$.

If A is a finite set, then $|A|$ denotes the cardinality of A and $\pi(A) = \pi(|A|)$.

If $x \in \mathbb{Z} \setminus \{0\}$, then we denote:

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

The notation $\mathcal{S}(x \mid n)$ occurs in the following statement:

$$\text{If } g^{-1}hg = g^x \text{ with } g \text{ and } h \text{ elements of a group, then } (hg)^n = h^n g^{\mathcal{S}(x|n)}. \tag{2.1}$$

The following lemma collects some properties of the operator $\mathcal{S}(- \mid -)$.

Lemma 2.1. *Let p be a prime, $R \in \mathbb{Z}$, $m \in \mathbb{N}$ and $a = v_p(R-1) \geq 1$. Then*

(1) $$v_p(R^m - 1) = \begin{cases} v_p(R-1) + v_p(m), & \text{if } p \neq 2 \text{ or } a \geq 2; \\ v_p(R+1) + v_p(m), & \text{if } p = 2, a = 1 \text{ and } 2 \mid m; \\ 1, & \text{otherwise.} \end{cases}$$

(2) $$o_{p^m}(R) = \begin{cases} p^{\max(0, m - v_p(R-1))}, & \text{if } p \neq 2 \text{ or } a \geq 2; \\ 1, & \text{if } p = 2, a = 1 \text{ and } m \leq 1; \\ 2^{\max(1, m - v_2(R+1))}, & \text{otherwise.} \end{cases}$$

(3) *Suppose that $a \leq m$ and if $p = 2$, then $a \geq 2$. Then the following hold:*
  (a) $\{R^x + p^m\mathbb{Z} : x \geq 0\} = \{1 + yp^a + p^m\mathbb{Z} : 0 \leq y < p^{m-a}\}$.
  (b) *If $n \in \mathbb{N}$ and $n \equiv kp^{m-a} \mod p^m$, then*

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

Proof. See [GBdR23, Lemma 2.1] and [BGLdR23, Lemma 8.2]. □

We will need the following formula:

$$\begin{aligned} \sum_{d=0}^{n} d2^d &= \sum_{d=0}^{n}\sum_{i=0}^{d-1} 2^d = \sum_{i=0}^{n-1} 2^{i+1} \sum_{d=i+1}^{n} 2^{d-i-1} = \sum_{i=0}^{n-1} 2^{i+1} \sum_{j=0}^{n-i-1} 2^j = \sum_{i=0}^{n-1} 2^{i+1}(2^{n-i}-1) \\ &= n2^{n+1} - 2\sum_{i=0}^{n-1} 2^i = n2^{n+1} - 2(2^n - 1) = (n-1)2^{n+1} + 2. \end{aligned} \tag{2.2}$$

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

$$C_{R,n} = \sum_{d|n} \frac{\varphi(d)}{o_d(R)}. \tag{2.3}$$

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 2.2. *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*

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

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 2.1.(2) and (2.3) 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 2.1.(2) and (2.3) 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 $m < v_2(R+1)$, then $C_{R,2^m} = 2 + \sum_{k=2}^{m} 2^{k-2} = 1 + 2^{m-1}$. Otherwise, i.e. if $m \ge v_2(R+1)$, then

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

□

2.2. Group theory

By default all the groups in this paper are finite. We use standard notation for a group G and $g, h \in G$: $Z(G)$ = center of G, G' = commutator subgroup of G, $\text{Aut}(G)$ = group of automorphisms of G, $|g|$ = order of g, $g^h = g^{-1}hg$, $[g,h] = g^{-1}g^h$. The notation $H \le G$ and $N \trianglelefteq G$ means that H is a subgroup of G and N is a normal subgroup of G. If H is a subgroup, then $[G : H]$ denotes index of H in G, $N_G(H)$ the normalizer of H in G and $\text{Core}_G(H)$ the core of H in G, i.e. the greatest subgroup of H that is normal in G.

If π is a set of primes, then g_π and $g_{\pi'}$ denote the π-part and π'-part of g, respectively. When p is a prime we rather write g_p and $g_{p'}$ than $g_{\{p\}}$ and $g_{\{p'\}}$.

Let m be a positive integer. We let C_m denote a generic cyclic group of order m. For an integer x coprime with m, let α_x denote the automorphism of C_m given by $\alpha_x(a) = a^x$ for every $a \in A$ and σ_x the automorphism of $\mathbb{Q}(\zeta_m)$ given by $\sigma_x(\zeta_m) = \zeta_m^x$. Then $x \mapsto \alpha_x$ and $x \mapsto \sigma_x$ define isomorphisms $\alpha : \mathbb{Z}_m^* \to \text{Aut}(C_m)$ and $\sigma : \mathbb{Z}_m^* \to \text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$, where $\mathbb{Z}_m^*$ denotes the group of units of $\mathbb{Z}/m\mathbb{Z}$. We are abusing the notation by treating elements of $\mathbb{Z}_m^*$ as integers. In particular, $\alpha_x \mapsto \sigma_x$ defines an isomorphism $\text{Aut}(C_m) \to \text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. We abuse the notations by considering the latter as an identification so that if Γ is a subgroup of $\text{Aut}(C_m)$, then

$$\mathbb{Q}(\zeta_m)^\Gamma = \{a \in \mathbb{Q}(\zeta_m) : \sigma_x(a) = a \text{ for all } \alpha_x \in \Gamma\},$$

the Galois correspondent of Γ considered as a subgroup of $\text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$.

2.3. Finite metacyclic p-groups

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 [GBdR23] for the special case of p-groups. More precisely when [GBdR23, Corollary 4.1] is specialized to finite metacyclic p-groups one obtains the following:

Theorem 2.3. *Let p be a prime integer. Then every finite metacyclic p-group is isomorphic to a group given by the following presentation*

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

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 $p = 2 \geq \mu$, 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 $\rho \leq \sigma$,*

2.4. Wedderburn decomposition of rational group algebras

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

Let F/K be a finite Galois field extension and let $G = \mathrm{Gal}(F/K)$. Let $\mathcal{U}(F)$ denotes 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

$$(F/K, f) = \sum_{\alpha \in G} t_\alpha F, \quad x t_\alpha = t_\alpha \alpha(x), \quad t_\alpha t_\beta = t_{\alpha\beta} f(\alpha, \beta), \quad (x \in F, \alpha, \beta \in G).$$

It is well known that $(F/K, f)$ is a central simple K-algebra and, if g is another 2-cocycle, then $(F/K, f)$ and $(F/K, g)$ are isomorphic as K-algebras if and only if gf^{-1} is a 2-coboundary. Therefore, if $\overline{f} \in H^2(G, F)$ is represented by the coboundary f, then we denote $(F/K, \overline{f}) = (F/K, f)$.

If G is cyclic of order n generated by α, and $a \in \mathcal{U}(K)$, then there is a cocycle $f : G \times G \to \mathcal{U}(K)$ given by

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

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

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

If A is a semisimple ring, then A is a direct sum of central simple algebras. This expression 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. Then $\mathbb{Q}G$ is semisimple and the center of each component A of $\mathbb{Q}G$ is isomorphic to the field of character values $\mathbb{Q}(\chi)$ of any irreducible character χ of G with $\chi(A) \neq 0$. 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 $\mathbb{Q}(\chi)$. We will abuse the notation and consider $Z(A)$ as equal to $\mathbb{Q}(\chi)$.

An important tool for us is a technique to describe the Wedderburn decomposition of $\mathbb{Q}G$ introduced in [OdRS04]. See also [JdR16, Section 3.5]. A closely related method to compute the primitive central idempotents of group algebras of finite solvable groups was introduced by S.D. Berman (see [Ber52, Ber55, Ber56] and [KP21]). We recall here its main ingredients.

If H is a subgroup of G, then $\widehat{H}$ denotes the element $|H|^{-1} \sum_{h \in H} h$ of the rational group algebra $\mathbb{Q}G$. 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.

Let N be a normal subgroup of G. Then the kernel of the natural homomorphism $\mathbb{Q}G \to \mathbb{Q}(G/N)$ is $\mathbb{Q}G(1 - \widehat{N}) = \sum_{n \in N \setminus 1} \mathbb{Q}G(n - 1)$. Therefore $\mathbb{Q}G = \mathbb{Q}G\widehat{N} \oplus \mathbb{Q}G(1 - \widehat{N})$ and $\mathbb{Q}(G/N) \cong \mathbb{Q}G\widehat{N}$. Thus $\mathbb{Q}(G/N)$ is isomorphic to the direct sum of the Wedderburn components of $\mathbb{Q}G$ of the form $\mathbb{Q}Ge$ with e a primitive central idempotent of $\mathbb{Q}G$ with $e\widehat{N} = e$.

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

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

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

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

A *strong Shoda pair* of G is a pair (H,K) of subgroups of G satisfying the following conditions:

(SS1) $K \subseteq H \trianglelefteq N_G(K)$,
(SS2) H/K is cyclic and maximal abelian in $N_G(K)/K$,
(SS3) $\varepsilon(H,K)^g\varepsilon(H,K)$ for every $g \in G \setminus C_G(\varepsilon(H,K))$.

Remark 2.4. *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

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

Proposition 2.5. [OdRS04, Proposition 3.4] [JdR16, Theorem 3.5.5] *Let (H,K) be a strong Shoda pair of G and let $m = [H : K]$, $n = [G : N_G(K)]$ and $e = e(G,H,K)$. Then e is a primitive central idempotent of $\mathbb{Q}G$ and $\mathbb{Q}Ge \cong M_n(A(G,H,K))$. Moreover,* $\mathrm{Deg}(\mathbb{Q}Ge) = [G : H]$*,* $Z(\mathbb{Q}Ge(G,H,K)) \cong F_{G,H,K}$ *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 $A(G,H,K)$ for some special kind of strong Shoda pairs of G. More precisely we have the following (see [OdRS04, Theorem 4.7] or [JdR16, Theorem 3.5.12]):

Theorem 2.6. *Let G be a finite 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 $\mathbb{Q}Ge(G,H,K)$ for subgroups H and K satisfying the following conditions:*

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

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

Suppose that G is a finite metacyclic group and let A be a cyclic normal subgroup of G with G/A cyclic. Then every Wedderburn component of $\mathbb{Q}G$ is of the form $\mathbb{Q}Ge(G,H,K)$ for (H,K) be subgroups of G satisfying the conditions of Theorem 2.6. Then, $N_G(K)/H$ is cyclic, say generated by uH, and of order k. Moreover, H/K is cyclic, say generated by aK, and normal in $N_G(K)/K$ so that $(aK)^{uK} = a^xK$ and $(uK)^k = a^y$ for some integers x and y. By Proposition 2.5 we have

$$A(G,H,K) \cong (\mathbb{Q}(\zeta_m)/F, \sigma_x, \zeta_m^y) = \mathbb{Q}(\zeta_m)[\overline{u} \mid \zeta_m\overline{u} = \overline{u}\zeta_m^x, \overline{u}^k = \zeta_m^y]. \tag{2.4}$$

2.5. Tools for the Isomorphism Problem for group rings

In this subsection 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 2.7 (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.

Theorem 2.8. *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]. ☐

3. The Isomorphism Problem 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 2.3, $G \cong \mathcal{P}_{p,\mu,\nu,\sigma,\rho,\epsilon}$ for unique non-negative integers μ, ν, σ and ρ and unique $\epsilon \in \{1, -1\}$ satisfying conditions (A)-(C).

The proof of the main result of this section relies in five technical lemmas.

Lemma 3.1. *Suppose that $\epsilon = 1$ and $\mu > 0$. Let $0 \le d < \nu$ and for every $1 \le i \le p^\mu$ 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 2.1.(1) we have $v_p(R^{p^d} - 1) = d + \rho$ and by condition (B) we have $\mu - (d + \rho) \le \nu - d$. Hence, applying Lemma 2.1.(3b) with $a = d + \rho$ and $m = \nu + \rho > a$ we obtain the following for every $k \in \mathbb{N}$:

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

Then

$$\mathcal{S}\left(R^{p^d} \mid kp^{\nu-d}\right) \equiv \begin{cases} k2^{\nu-d} + k2^{\mu-1} \mod 2^\mu, & \text{if } p = 2, \text{ and } \mu = \nu + \rho; \\ kp^{\nu-d} \mod p^\mu, & \text{otherwise}. \end{cases} \tag{3.1}$$

Moreover $a^{b^{p^d}} = a^{R^{p^d}}$ and hence, by (2.1) we have

$$(b^{p^d} a^i)^{p^{\nu-d}} = b^{p^\nu} a^{i\mathcal{S}\left(R^{p^d} | p^{\nu-d}\right)} = a^{p^\sigma + i\mathcal{S}\left(R^{p^d} | p^{\nu-d}\right)} = a^{l_i}. \tag{3.2}$$

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

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

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 2.1.(1). 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 (3.2), 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 2.1.(3a), 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 (3.2) 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. ☐

Lemma 3.2. *If $\epsilon = 1$, then the number of conjugacy classes of cyclic subgroups of G is $N = A_\sigma + A$ where*

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

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. 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 cyclic 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 3.1.

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 3.1 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 2.3 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 3.1 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 3.1 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 3.1 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

$$N_d = 1 + \sum_{h=0}^{\min(\sigma,\rho+d)-1} N_{d,h}. \tag{3.3}$$

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 $\rho \le \sigma$, 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 $\rho + h = \rho + d - \nu + \sigma \le \sigma$. 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 $h + \rho \le h + \nu - d = v_p(l_i) < \sigma \le \mu$ 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 $\mu \ge \sigma > v_2(l_i) = v_2(2^{\nu-d} + 2^{\mu-1}) \ge \nu - d \ge \rho = \rho + h$, because $\nu - d = \mu - \rho - d \le \mu - \rho \le \mu - 1$. 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 3.1 with the claim in the previous paragraph we deduce that for $d \le \nu - \rho$ 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 $d \le \nu - \rho$ and $0 \le h < \min(\sigma, \rho + d)$, 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 $v_p(i) \ge \min(\sigma, \rho + d)$ are conjugate we have

$$\begin{aligned}
&\sum_{d=0}^{\nu-\rho} N_d = \sum_{d=0}^{\nu-\rho} \left(1 + \sum_{h=0}^{\min(\sigma,\rho+d)-1} N_{d,h} \right) = \sum_{d=0}^{\sigma-\rho} \left(1 + \sum_{h=0}^{d-1} (p-1)p^{\rho-1} + \sum_{h=d}^{d+\rho-1} (p-1)p^{\rho+d-h-1} \right) \\
&+ \sum_{d=\sigma-\rho+1}^{\nu-\rho} \left(1 + \sum_{h=0}^{\sigma-\rho-1} (p-1)p^{\rho-1} + \sum_{h=\sigma-\rho}^{\sigma-1} (p-1)p^{\sigma-h-1} \right) = (\nu-\rho+1) + \\
&\sum_{d=0}^{\sigma-\rho} \left(d(p-1)p^{\rho-1} + (p-1)\sum_{x=0}^{\rho-1} p^x \right) + \sum_{d=\sigma-\rho+1}^{\nu-\rho} \left((\sigma-\rho)(p-1)p^{\rho-1} + (p-1)\sum_{x=0}^{\rho-1} p^x \right) \\
&= (\nu-\rho+1) + \frac{(\sigma-\rho)(\sigma-\rho+1)}{2}(p-1)p^{\rho-1} + (\nu-\sigma)(\sigma-\rho)(p-1)p^{\rho-1} + (\nu-\rho+1)(p^\rho - 1) \\
&= p^{\rho-1}\left((\sigma-\rho)(p-1)\frac{1+2\nu-\rho-\sigma}{2} + (\nu-\rho+1)p \right).
\end{aligned} \tag{3.4}$$

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

Let $i \in X_h$. Then $v_p(p^\sigma + ip^{\nu-d}) = \min(\sigma, h + \nu - d)$. If $v_p(l_i) \ne \min(\sigma, h + \nu - d)$, then $p = 2 \ne i$, $\mu = \nu + \rho$ and $l_i = 2^\sigma + i(2^{\nu-d} + 2^{\mu-1})$. Then, from $\rho \ge 1$ and $d > \nu - \rho \ge 0$ we deduce $\mu - 1 = v_2(l_i - (2^\sigma + i2^{\nu-d})) = \min(v_2(l_i), v_2(2^\sigma + i2^{\nu-d})) = \min(v_2(l_i), \sigma, \nu - d) \le \nu - d = \mu - \rho - d < \mu - 1$, a contradiction. This proves that $v_p(l_i) = \min(\sigma, h + \nu - d)$. Therefore, $h_i = \min(\mu, v_p(l_i), \rho + d, \rho + h) = \min(\sigma, h + \nu - d, \rho + d, \rho + h) = \min(\sigma, h + \nu - d, \rho + h) = \min(\sigma, h + \nu - d) \le \mu$, because $\sigma \le \nu < \rho + d$ and $h + \nu - d < h + \rho$, by condition (B) in Theorem 2.3 and the assumption. Hence, by Lemma 3.1, each class inside X_h with $\sigma > h \ne \sigma + d - \nu$ contains $p^{\mu - \min(\sigma, h+\nu-d)}$ elements. This proves the following

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

Then

$$\begin{aligned}
&\sum_{d=\nu-\rho+1}^{\nu-1}\left(1+\sum_{h=0,h\neq\sigma+d-\nu}^{\sigma-1} N_{d,h}\right)\\
&=\sum_{d=\nu-\rho+1}^{\nu-1}\left(1+(p-1)\left(\sum_{h=0}^{\sigma+d-\nu-1} p^{\nu-d-1}+\sum_{h=\sigma+d-\nu+1}^{\sigma-1} p^{\sigma-h-1}\right)\right)\\
&=\sum_{x=1}^{\rho-1}\left(1+(p-1)\sum_{h=0}^{\sigma-x-1} p^{x-1}+(p-1)\sum_{h=\sigma-x+1}^{\sigma-1} p^{\sigma-h-1}\right)\\
&=\sum_{x=1}^{\rho-1}\left(1+(\sigma-x)(p-1)p^{x-1}+(p-1)\sum_{y=0}^{x-2} p^{y}\right)=\sum_{x=1}^{\rho-1}\left((\sigma-x)p^x-(\sigma-x)p^{x-1}+p^{x-1}\right)\\
&=\sum_{x=1}^{\rho-1}(\sigma-x)p^x-\sum_{x=0}^{\rho-2}(\sigma-x-1)p^x+\sum_{x=0}^{\rho-2}p^x=(\sigma-\rho+1)p^{\rho-1}+2\sum_{x=1}^{\rho-2}p^x-(\sigma-1)+1\\
&=(1-\rho)p^{\rho-1}+\sigma(p^{\rho-1}-1)+2\frac{p^{\rho-1}-1}{p-1}.
\end{aligned} \tag{3.5}$$

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 3.1, 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

$$\begin{aligned}
N_{d,\sigma+d-\nu}&=\frac{|Z_{\min(\mu-\sigma,\rho+d-\nu)+1}|}{p^{\mu-\min(\mu,\rho+\sigma+d-\nu)}}+\sum_{l=0}^{\min(\mu-\sigma,\rho+d-\nu)}\frac{|Y_l|}{p^{\mu-(\sigma+l)}}\\
&=p^{\nu-d-1}+(p-2)p^{\nu-d-1}+\sum_{l=1}^{\min(\mu-\sigma,\rho+d-\nu)}\frac{\varphi(p^{\mu-\sigma+\nu-d-l})}{p^{\mu-\sigma-l}}\\
&=(p-1)p^{\nu-d-1}+\min(\mu-\sigma,\rho+d-\nu)(p-1)p^{\nu-d-1}=(1+\min(\mu-\sigma,\rho+d-\nu))(p-1)p^{\nu-d-1}.
\end{aligned}$$

Thus

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

Combining (3.3), (3.4), (3.5). and (3.6), and recalling that $N_\nu = \mu+1$, we finally obtain that the number of conjugacy classes of cyclic subgroups of G

$$
\begin{aligned}
\sum_{d=0}^{\nu} N_d =& \mu+1+\sum_{d=0}^{\nu-\rho}N_d + \sum_{d=\nu-\rho+1}^{\nu-1}\left(1+\sum_{h=0,h\neq\sigma+d-\nu}^{\min(\sigma,\rho+d)}N_{d,h}+N_{d,\sigma+d-\nu}\right) \\
=&\mu+1+p^{\rho-1}\left((\sigma-\rho)(p-1)\frac{1+2\nu-\rho-\sigma}{2}+(\nu-\rho+1)p\right) \\
&+(1-\rho)p^{\rho-1}+\sigma(p^{\rho-1}-1)+2\frac{p^{\rho-1}-1}{p-1}+(\sigma-1-\mu)+2p^{\rho-1}+\frac{p^{\rho-1}-p^{\rho+\sigma-\mu}}{p-1} \\
=&p^{\rho-1}\sigma\left[1+(p-1)\frac{1+2\nu-\rho-\sigma}{2}\right]+p^{\rho-1}\left(-\rho(p-1)\frac{1+2\nu-\rho-\sigma}{2}+(\nu-\rho+1)p\right) \\
&+(1-\rho)p^{\rho-1}+2\frac{p^{\rho-1}-1}{p-1}+2p^{\rho-1}+\frac{p^{\rho-1}-p^{\rho+\sigma-\mu}}{p-1} \\
=&p^{\rho-1}\sigma\left[1+(p-1)\frac{1+2\nu-\sigma}{2}\right]-\frac{p^{\rho+\sigma-\mu}}{p-1} \\
&+\frac{3p^{\rho-1}-2}{p-1}+p^{\rho-1}\frac{6-2\rho-\rho(p-1)(1+2\nu-\rho)+2(\nu-\rho+1)p}{2} \\
=&p^{\rho-1}\sigma\left[1+(p-1)\frac{1+2\nu-\sigma}{2}\right]-\frac{p^{\rho+\sigma-\mu}}{p-1} \\
&+\frac{3p^{\rho-1}-2}{p-1}+p^{\rho-1}\frac{6-\rho+2\nu\rho-\rho^2+p(\rho^2+2\nu-3\rho-2\nu\rho+2)}{2} = A_\sigma + A.
\end{aligned} \tag{3.7}
$$

□

Lemma 3.3. *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. 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 these 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 2.1.(2),

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

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

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

as desired. □

Lemma 3.4. *Suppose that $\epsilon=-1$, $\rho\ge\mu-1$ and $\mu\ge 3$. 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 $K_0=\left\langle b^2\right\rangle$. The assumption $\rho\ge\mu-1$ implies that $H=\left\langle a,b^2\right\rangle$ is a maximal abelian subgroup of G. Then (H,K_0) satisfy the conditions in Theorem 2.6 and hence $\mathbb{Q}Ge(G,H,K_0)$ is a simple component of $\mathbb{Q}G$. Moreover, by Proposition 2.5 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 $\mu\ge 3$, 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 2.6 and $H_1\in\{H,G\}$. However, $H_1\ne G$ 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 2.5, $\varphi([H:K])=2\dim Z(A)=2^{\mu-1}$ and hence $[H:K]=2^\mu$. Another consequence of Proposition 2.5 and the fact that A is not commutative is that $H\ne\left\langle K,b^2\right\rangle$ and as $H/K=\left\langle aK,b^2K\right\rangle$ 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 $Z(G)=\left\langle b^2\right\rangle$ and its order is 2^ν. Then $K=\left\langle b^4\right\rangle$, which is not possible because $H/\left\langle b^4\right\rangle$ is not cyclic. Thus $\sigma=\mu$ and $Z(G)=\left\langle a^{2^{\mu-1}}\right\rangle\times\left\langle b^2\right\rangle$. Then $K=\left\langle b^2\right\rangle$ 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 3.5. *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 2.6, and by Proposition 2.5, 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 2.3 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 2.6, we have $A = \mathbb{Q}Ge(G, H_1, K)$ for subgroups H_1 and K satisfying the conditions of Theorem 2.6 and $H_1 \supseteq H$. However, by Proposition 2.5, $[G : H] = 2^{\mu-\rho} = \mathrm{Deg}(A) = [G : H_1]$ 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 2.5, 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 2.6. Therefore $K \cap \langle a\rangle = 1$, and hence $[H : K] \ge |a| = 2^\mu$. So $[H : K] = 2^\mu$. As $N_G(K)/H \cong \mathrm{Gal}(\mathbb{Q}(\zeta_{[H:K]})/F)$, 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 3.6. *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 2.3, 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 2.8 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 $C_{2^{\rho_1}} \times C_{2^{\nu_1}} \cong C_2 \times C_{2^{\nu_2}}$, by Theorem 2.8, and by conditions (B) and (C) we have $p = 2$, $\rho_1 \le \nu_1$, $2 \le \rho_2$ and $1 \le \nu_2$. 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 $\rho_i \le \nu_i$, and if $\epsilon = -1$, then $C_2 \times C_{2^{\nu_1}} \cong C_2 \times C_{2^{\nu_2}}$ and $1 \le \nu_1, \nu_2$. 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 2.7), the number of Wedderburn components of $\mathbb{Q}G_i$ is the number of conjugacy classes of cyclic subgroups of G_i. Therefore, if A_{σ_1} and A_{σ_2} are as defined in Lemma 3.2, 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 $\sigma_1 < \sigma_2 \le \mu \le \nu + \rho$. If $\sigma_1 < \mu - 1$, then $\min(\sigma_2, \mu - 1) \le v_p(B_{\sigma_2}) = v_p(B_{\sigma_1}) = \sigma_1 < \mu - 1$, 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

$\sigma_2 = \mu \leq \nu$. 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 3.3 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 $\rho_2 \geq \mu - 1$. If $\rho_1 < \mu - 1$, then using that $\mu \geq 2$, by condition (C), we have

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

again in contradiction with the assumption $\rho_1 < \rho_2$. Therefore $\rho_1 = \mu - 1$ and $\rho_2 = \mu$, and hence $\mu \geq 3$, by condition (A). If $\sigma_2 = \mu$, then, by Lemma 3.4, $\mathbb{Q}G_2$ 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 3.5. Thus $\rho = \mu$. If $\mu \geq 3$, then the contradiction follows from Lemma 3.4. 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. □

4. The Isomorphism Problem for finite metacyclic nilpotent groups

Given a finite group G 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.

Lemma 4.1. *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 2.5. 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, it is a power of p. Moreover the center of A is isomorphic to the Galois correspondent $F_{G,L,K} = \mathbb{Q}(\zeta_c)^{\mathrm{Im}\,(\alpha)}$ of a subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta_c)/\mathbb{Q})$ isomorphic to $N_G(K)/L$ (Remark 2.4). The assumption implies that $F \subseteq \mathbb{Q}(\zeta_{c_p})$. As $[N_G(K) : L]$ is a power of p, 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. □

If G is a finite group, then we use the notation

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

Remark 4.2. *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 [GBdR23, Lemma 3.1], 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 $\operatorname{Aut}(\langle h \rangle)$ has an element of order q. As $\operatorname{Aut}(\langle h \rangle)$ 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 4.3. *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 [GBdR23, Lemma 3.1], $\langle a_p, b_p \rangle$ 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 2.8, 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 $\pi_G = \pi(|G|) \setminus \pi'_G = \pi(|H|) \setminus \pi'_H = \pi_H$. □

In the remainder of the paper if G is a group and p is a prime, then G_p denotes a Sylow subgroup of G and $G_{p'}$ a Hall p'-subgroup of G.

Lemma 4.4. *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 4.2, $2 \notin \pi'$ 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 4.1 $[G : K]$ 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 4.1, 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 4.5. *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 4.4. As $2 \notin \pi'$, by Remark 4.2, 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 $\mathbb{Q}G \cong \mathbb{Q}H$, $A_G \cong A_H$. By Lemma 4.4, $(\mathbb{Q}G_p)^k \cong A_G \cong A_H \cong (\mathbb{Q}H_p)^k$ an therefore $\mathbb{Q}G_p \cong \mathbb{Q}H_p$. □

We are ready to prove our main results. We first state and prove Theorem A.

Theorem 4.6. *Let G and H be two 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.*

Proof. By Lemma 4.3 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 4.5, and hence $G_p \cong H_p$, by Theorem 3.6. □

If G is nilpotent, then $\pi'_G = \emptyset$ and hence Corollary B follows directly from Theorem 4.6.

References

[Ber52] S. D. Berman, *On the theory of representations of finite groups*, Dokl. Akad. Nauk SSSR (N.S.) **86** (1952), 885–888.

[Ber55] ———, *Group algebras of abelian extensions of finite groups*, Dokl. Akad. Nauk SSSR (N.S.) **102** (1955), 431–434.

[Ber56] ———, *p-adic ring of characters*, Dokl. Akad. Nauk SSSR (N.S.) **106** (1956), 583–586. MR 0077539 (17,1052g)

[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

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

[Bra51] R. Brauer, *On the algebraic structure of group rings*, J. Math. Soc. Japan **3** (1951), 237–251. MR 0044577 (13,442b)

[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.

[GBdR23] À. García-Blázquez and Á. del Río, *A classification of metacyclic groups by group invariants*, Bull. Math. Soc. Sci. Math. Roumanie (N.S.) **66(114)** (2023), no. 2, 209–233.

[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*, Thesis (Ph.D.)–Univ. Oxford, 1940.

[Hig40b] ———, *The units of group-rings*, Proc. London Math. Soc. (2) **46** (1940), 231–248. MR 0002137 (2,5b)

[JdR16] E. Jespers and Á. del Río, *Group Ring Groups. Volume 1: Orders and generic constructions of units*, Berlin: De Gruyter, 2016.

[Kin73] B. W. King, *Presentations of metacyclic groups*, Bull. Austral. Math. Soc. **8** (1973), 103–131. MR 323893

[KP21] R. S. Kulkarni and S. S. Pradhan, *Schur index and extensions of witt-berman's theorems*, arxiv.2012.10892 (2021).

[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

[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)

[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

[Sim94] Hyo-Seob Sim, *Metacyclic groups of odd order*, Proc. London Math. Soc. (3) **69** (1994), no. 1, 47–71. MR 1272420

[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