

# The group of automorphisms of the rational group algebra of a finite metacyclic group

Aurora Olivieri	Á. del Río and J.J. Simón*
Departamento de Matemáticas	Departamento de Matemáticas
Universidad Simón Bolívar	Universidad de Murcia
Ap. Postal 89000	30100 Murcia, Spain
Caracas 1080-A, Venezuela	
olivieri@usb.ve	adelrio@um.es, jsimon@um.es

June 16, 2006

## Abstract

We investigate the group of automorphism  $\text{Aut}(\mathbb{Q}G)$  of a rational group algebra  $\mathbb{Q}G$  of a finite metacyclic group  $G$  by first describing the simple components of the Wedderburn decomposition of  $\mathbb{Q}G$  and then investigating when two of these simple components are isomorphic.

The aim of this paper is to compute the group of automorphism  $\text{Aut}(\mathbb{Q}G)$  of a rational group algebra  $\mathbb{Q}G$  of a finite metacyclic group  $G$ . Aside of the interest of understanding  $\text{Aut}(\mathbb{Q}G)$  as an important invariant of the  $\mathbb{Q}G$ , another motivation is the connection of the group  $\text{Aut}(\mathbb{Q}G)$  with Zassenhaus conjectures [3, 15].

To describe the group of automorphism of a finite dimensional semisimple algebra  $A$  one can proceed as follows. Assume that  $A = \prod_{i=1}^n A_i^{k_i}$ , where  $A_1, \dots, A_n$  are non-isomorphic simple algebras. For every  $i = 1, \dots, n$  consider the symmetric group on  $k_i$  letters acting on  $A_i^{k_i}$  by permutation of the components and let  $A_i^{k_i} \rtimes S_{k_i}$  be the corresponding semidirect product. Then  $\text{Aut}(A) \simeq \prod_{i=1}^n \text{Aut}(A_i)^{k_i} \rtimes S_{k_i}$ . Moreover if  $A$  is simple then  $\text{Aut}(A)$  fits into an exact sequence

$$1 \rightarrow \text{Inn}(A) \xrightarrow{i} \text{Aut}(A) \xrightarrow{r} (\text{Aut}(Z(A)); A) \rightarrow 1$$

where  $\text{Inn}(A)$  denotes the group of inner automorphisms of  $A$ ;  $\text{Aut}(Z(A); A)$  is the group of automorphisms of the centre  $Z(A)$  of  $A$  that fix the class of  $A$  in the Brauer group of  $Z(A)$  and  $i$  and  $r$  are the inclusion and restriction maps respectively [8]. Moreover, if  $A = \mathbb{Q}G$  is a rational group algebra of a finite group  $G$  then  $\text{Aut}(Z(A_i) : A_i) \simeq \text{Gal}(Z(A_i)/\mathbb{Q}(\xi_{m_i}))$  where  $m_i$  is the Schur index of  $A_i$  and  $\xi_{m_i}$  is an  $m_i$ -th primitive root of 1 (see [8] for the last isomorphism and [2] for the existence of a primitive  $m_i$ -th root of unity in  $Z(A_i)$ ). Therefore computing  $\text{Aut}(\mathbb{Q}G)$  for  $G$  a finite group reduces to the following two problems:

**Problem 1:** Compute the Wedderburn decomposition of  $\mathbb{Q}G$ .

**Problem 2:** Recognize the components of the Wedderburn decomposition of  $\mathbb{Q}G$  that are isomorphic.

---

\*The second and third author have been partially supported by the D.G.I. of Spain and Fundación Séneca of Murcia

Although this method is present in previous works [3, 4, 6], the only non abelian groups for which precise information on  $\text{Aut}(\mathbb{Q}G)$  is known are metacyclic groups of type  $C_m : C_p$  with  $p$  prime [6]. The obstacle relies in the difficulty of solving Problems 1 and 2. We quote the following from [6]: “In order to generalize the results of the above metacyclic groups (that is for  $n$  prime) to the class of general metacyclic groups, we need an algorithm means to determining the entire collection of non-abelian simple components that would appear. This appears to be a complicated process to work out for a general  $m$  and  $n$ .” In this paper we solve completely Problem 1 for arbitrary metacyclic groups and provide information on Problem 2 for metacyclic groups of type  $C_m : C_{pq}$ , where  $p$  and  $q$  are two, non necessarily different, primes. In the way we also solve an error in [6]. This paper of Herman has been the main source of ideas.

## 1 Notation and Preliminaries

In this section we establish the basic notation of the paper and show the main tools to be used. We start with the following notation where  $r$  and  $m$  are coprime integers,  $p$  is a prime integer,  $G$  is a group,  $H$  is a subgroup of  $G$ ,  $R$  is a ring and  $E/F$  is a cyclic field extension of degree  $n$  with  $\text{Gal}(E/F) = \langle \sigma \rangle$ .

$o_m(r)$	=	multiplicative order of $r$ module $m$ .
$v_p$	=	$p$ -adic valuation.
$\langle X \rangle$	=	group generated by $X \subseteq G$ .
$G'$	=	commutator of $G$ .
$N_G(H)$	=	normalizer of $H$ in $G$ .
$Z(R)$	=	centre of $R$ .
$R^*$	=	group of units of $R$ .
$\text{Aut}(R)$	=	group of automorphisms of $R$ .
$R *_{\alpha}^{\tau} G$	=	$R * G =$ crossed product over $G$ with coefficients in $R$ , action $\alpha$ and twisting $\tau$ [12].
$(E, \sigma, a)$	=	$E * \langle \sigma \rangle = E[u : u^n = a, u^{-1}xu = \sigma(x), (x \in E)] =$ cyclic algebra over $F$ [13, 14].
$N_{E/F}$	=	norm map of the extension $E/F$ .
$N_{E/F}^*$	=	$N_{E/F}(E^*)$ .
$\xi_m$	=	complex $m$ -th primitive root of unity.
$\mathbb{Q}_m$	=	$\mathbb{Q}(\xi_m)$ .
$\sigma_r$	=	automorphism of $\mathbb{Q}_m$ given by $\sigma_r(\xi_m) = \xi_m^r \pmod{\text{gcd}(m, r)}$ .
$\mathcal{U}(m, r, s)$	=	$(\mathbb{Q}_m, \sigma_r, \xi_m^s)$ , with $m s(r-1)$ .

We write  $H \leq G$  (resp.  $H \trianglelefteq G$ ) to mean that  $H$  is a subgroup (resp. normal subgroup) of a group  $G$ .

It is well know that two cyclic  $F$ -algebras  $(E, \sigma, a)$  and  $(E, \sigma, b)$  are isomorphic as  $F$ -algebras if and only if  $b/a \in N_{E/F}^*$  [13, 14] and that  $(E, \sigma, a)$  is split if and only if  $a \in N_{E/F}^*$ . Rather than comparing cyclic algebras as  $F$ -algebras we need to compare them as rings. That is the use of the following Lemma. The notation  $R \simeq S$  for  $R$  and  $S$  rings (or algebras) means that  $R$  and  $S$  are isomorphic as rings (not necessarily as algebras).

**Lemma 1.1** *Let  $E/F$  be a finite cyclic field extension of degree  $n$ ,  $\text{Gal}(E/F) = \langle \sigma \rangle$  and  $a, b \in F^*$ .*

1. *If  $\text{gcd}(k, n) = 1$  then  $(E, \sigma, a)$  and  $(E, \sigma^k, a^k)$  are isomorphic as  $F$ -algebras. In particular, if  $(k, o_m(r)) = 1$  then  $\mathcal{U}(m, r, s) \simeq \mathcal{U}(m, r^k, ks)$  as central simple algebras.*

2. Every automorphism  $\tau$  of  $E$  extends to a ring isomorphism  $(E, \sigma, a) \simeq (E, \tau^{-1}\sigma\tau, \tau(a))$  (not necessarily of  $F$ -algebras). In particular, if  $\gcd(m, k) = 1$  then  $\mathcal{U}(m, r, s) \simeq \mathcal{U}(m, r, ks)$ .
3. If there is a ring isomorphism  $f : (E, \sigma, a) \rightarrow (E, \sigma, b)$  and a ring automorphism  $g$  of  $(E, \sigma, a)$  such that  $f(x) = g(x)$  for every  $x \in F$  then  $b/a \in N_{E/F}^*$ .
4.  $(E, \sigma, a) \simeq M_n(F)$  if and only if  $a \in N_{E/F}^*$  if and only if  $(E, \sigma, a)$  and  $M_n(F)$  are isomorphic as  $F$ -algebras.
5. If  $E/\mathbb{Q}$  is an abelian extension then  $(E, \sigma, a) \simeq (E, \sigma, b)$  if and only if there is an automorphism  $f$  of  $F$  such that  $b/f(a) \in N(E/F)$ .
6. Assume now that  $(E, \sigma, a)$  has index  $m$  and it is a simple quotient of a rational group algebra of a finite group. Then  $\xi_m \in F$ . If there is a ring isomorphism  $f : (E, \sigma, a) \rightarrow (E, \sigma, b)$  such that  $f(\xi_m) = \xi_m$ , then  $b/a \in N_{E/F}^*$ .

**Proof.** 1 is well known. To prove 2, notice that there is a unique ring homomorphism  $f : E[u_1 | u_1^n = a, u_1^{-1}xu_1 = \sigma(x)(x \in E)] \rightarrow E[u_2 | u_2^n = \tau(a), u_2^{-1}xu_2 = \tau^{-1}\sigma\tau(x)(x \in E)]$  that extends  $\tau$  and  $f(u_1) = u_2$  and  $f$  is obviously a ring isomorphism.

3. Just use that  $fg^{-1}$  is an isomorphism of  $F$ -algebras.

4. Is a consequence of 3 and the obvious fact that every automorphism of  $F$  extends to an automorphism of  $M_n(F)$ .

5. Assume that  $E/\mathbb{Q}$  is an abelian extension and let  $f : (E, \sigma, a) \rightarrow (E, \sigma, b)$  be a ring isomorphism. Then the restriction of  $f$  to  $F$  extends to an automorphism  $g$  of  $E$ . By 2,  $g$  extends to an isomorphism  $g : (E, \sigma, a) \rightarrow (E, \sigma, f(a))$ , since  $\text{Aut}(E)$  is abelian. Then  $h = gf^{-1} : (E, \sigma, f(a)) \rightarrow (E, \sigma, b)$  is an isomorphism of  $F$ -algebras and so  $b/f(a) \in N_{E/F}^*$ , by 3. Conversely, assume that there is an automorphism  $f$  of  $E$  such that  $b/f(a) \in N_{E/F}^*$ . Then  $(E, \sigma, b) \simeq (E, \sigma, f(a)) \simeq (E, \sigma, a)$ , by 2.

6. The existence of a  $m$ -th primitive root of unit in  $F$  is proved in [2]. Let  $f : (E, \sigma, a) \rightarrow (E, \sigma, b)$  be an isomorphism. If  $f(\xi_m) = \xi_m$ , then the restriction of  $f$  to  $F$  extends to an automorphism of  $(E, \sigma, a)$  [8] and 3 applies. ■

We recall the following lemma for future use.

**Lemma 1.2** *Let  $m, r, n, s, t, x, y$  and  $z$  integers such that  $\gcd(r, m) = 1$ .*

1. *If  $m|n$  then there exists an integer  $j$  relatively prime with  $n$  such that  $r \equiv j \pmod{n}$ .*
2. *If  $f$  is the smallest positive divisor  $h$  of  $x$  such that  $\gcd(x/h, y)$  divides  $z$  then every prime divisor of  $f$  is also a prime divisor of  $\frac{y}{\gcd(\frac{x}{f}, y)}$ .*
3. *If  $n = o_m(r)$ ,  $t|\gcd(s, n)$  and  $m|\frac{s}{t}(r-1)$  then the Schur index  $\mathcal{U}(m, r, s)$  divides  $n/t$ .*

**Proof.** 1 is very easy to proof.

2. Let  $p$  be a prime divisor of  $f$  and  $d = \gcd(\frac{x}{f}, y)$ . Then  $v_p(z) < \min\{v_p(x), v_p(y)\}$  and  $v_p(f) = v_p(x) - v_p(z)$ . Thus  $v_p(\frac{x}{f}) = v_p(z) < v_p(y)$  and hence  $v_p(d) = v_p(z) < v_p(y)$ . We conclude that  $p$  divides  $\frac{y}{d}$ .

3. The degree of  $A = \mathcal{U}(m, r, s)$  is  $n$  and the assumption  $m|\frac{s}{t}(r-1)$  implies that  $\xi_m^{s/t} \in Z(A)$ . Then  $\xi_m^{sn/t} = N_{\mathbb{Q}_m/K}(\xi_m^{s/t})$  and hence  $\mathcal{U}(m, r, sn/t)$  is a split algebra. Thus the index of  $A$  is a divisor of  $n/t$  (see e.g. [14, Theorem 32.19]). ■

## 1.1 Primitive central idempotents

In this subsection we recall some results from [11]. Throughout  $G$  denotes a finite group. If  $H \trianglelefteq K \leq G$  then let  $\widehat{K} = \frac{1}{|K|} \sum_{k \in K} k \in \mathbb{Q}K$  and

$$\varepsilon(K, H) = \begin{cases} \widehat{K} & \text{if } K = H \\ \prod_{M/H} (\widehat{H} - \widehat{M}) & \text{otherwise} \end{cases}$$

where, in the last product,  $M/H$  runs through the minimal non trivial normal subgroups of  $K/H$ . Finally let  $e(G, K, H)$  denote the sum of the different  $G$ -conjugates of  $\varepsilon(K, H)$  in  $\mathbb{Q}G$ .

**Theorem 1.3** [11] *If  $G$  is a metabelian finite group and  $A$  is a maximal element of  $\{B \leq G : B \text{ is abelian and } G' \leq B\}$  then the primitive central idempotents of  $\mathbb{Q}G$  are the elements of the form  $e(G, K, H)$  for  $(K, H)$  pairs of subgroups of  $G$  satisfying the following conditions:*

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

*If  $(K, H)$  is a pair of subgroups of  $G$  satisfying conditions (1) and (2) and  $e = e(G, K, H)$  then  $\mathbb{Q}Ge \simeq M_n(\mathbb{Q}_k *_{\sigma}^{\tau} N/K)$  where  $N = N_G(H)$ ,  $n = [G : N]$ ,  $k = [K : H]$  and if  $aH$  is a generator of  $K/H$  and  $g, h \in N$ , then  $\sigma(gK) = \xi_k^i$  if  $g^{-1}agH = a^iH$  and  $\tau(gK, hK) = \xi_k^j$  if  $[g, h]H = a^jH$  (Remark:  $N/K$  is abelian [10].)*

In Section 2 we are going to use Theorem 1.3 to give a precise description of the primitive central idempotents of  $\mathbb{Q}G$  for  $G$  a finite metacyclic group. We will need to decide when two pairs  $(H_1, K_1)$  and  $(H_2, K_2)$  of subgroups of  $G$  satisfying conditions (1) and (2) of Theorem 1.3 give rise to the same primitive central idempotent, i.e.  $e(G, K_1, H_1) = e(G, K_2, H_2)$ . In order to deal with this problem it is better to consider a more general class of pairs of subgroups.

A *Shoda pair* of  $G$  is a pair  $(K, H)$  of subgroups of  $G$  such that  $H \trianglelefteq K$ ,  $K/H$  is cyclic and if  $g \in G$  and  $[K, g] \cap K \subseteq H$  then  $g \in K$ . If  $(K, H)$  is a pair of subgroups of  $G$  satisfying conditions (1) and (2) of Theorem 1.3 then  $(K, H)$  is a Shoda pair of  $G$ . If  $H \trianglelefteq K \leq G$  then  $(K, H)$  is a Shoda pair of  $G$  if and only if the induced character  $\chi^G$  in  $G$  of one (resp. any) linear character  $\chi$  of  $K$  with kernel  $H$  is irreducible. In that case there is a (necessarily unique) rational number  $\alpha$  such that  $\alpha e(G, K, H)$  is a primitive central idempotent of  $\mathbb{Q}G$  and if  $\lambda$  is an irreducible character of  $G$  then  $\lambda(e) \neq 0$  if and only if  $\lambda$  is the character of  $G$  induced by a linear character of  $K$  with kernel  $H$  [11]. Using this and [5, Theorem 45.6] it is easy to prove the following proposition.

**Proposition 1.4** *Let  $(K_1, H_1)$  and  $(K_2, H_2)$  be two Shoda pairs of a finite group  $G$  and let  $\alpha_1, \alpha_2 \in \mathbb{Q}$  be such that  $e_i = \alpha_i e(G, K_i, H_i)$  is a primitive central idempotent of  $\mathbb{Q}G$  for  $i = 1, 2$ . Then  $e_1 = e_2$  if and only if there is  $g \in G$  such that  $K_1^g \cap H_2 = H_1^g \cap K_2$ .*

## 1.2 Finite subgroups of division rings

A finite metacyclic group of type  $C_m : C_n$  is a group having an normal cyclic group of order  $m$  and index  $n$  or equivalent a group given by the following presentation

$$G_{m,r,n,s} = \langle a, b \mid a^m = 1, b^n = a^s, b^{-1}ab = a^r \rangle \quad (1.1)$$

for  $m, r, n$  and  $s$  satisfying the following conditions:

$$m \mid r^n - 1, \quad m \mid s(r - 1). \quad (1.2)$$

Our second tool is Amitsur's classification of the finite subgroups of division rings. In this section we collect the ingredients of this classification which are useful for us.

**Theorem 1.5** [1] *A finite metacyclic group  $G$  is isomorphic to a subgroup of a division ring if and only if there are relatively prime integers  $m$  and  $r$  such that  $G \simeq G_{m,r,n,s}$  and  $\mathcal{U}(m, r, s)$  is a division ring, where  $n = o_m(r)$  and  $s = m/\gcd(m, r - 1)$ . Moreover if  $m, r, n$  and  $s$  are as above then  $\mathcal{U}(m, r, s)$  is a division ring if and only if one of the following conditions holds:*

(A)  $\gcd(n, s) = 1$ , and hence  $\gcd(m, r - 1, s) = 1$ ,

(B)  $v_2(n) = v_2(\frac{m}{s}) = 1$ ,  $2 \leq v_2(m) \leq v_2(r + 1)$  and  $\gcd(n, s) = \gcd(m, r - 1, s) = 2$  and  $2^\alpha | r + 1$ ;

and one of the following conditions holds,

1.  $n = \gcd(m, r - 1) = 2$  and  $m | r + 1$ ,

2. for every prime divisor  $q$  of  $n$  there is a prime divisor  $p$  of  $m$  such that  $q \nmid o_{m_p}(r)$  and either

- $p \neq 2$  and  $\gcd(q, \frac{p^\delta - 1}{\gcd(m, r - 1)}) = 1$  or

- $p = q = 2$ , (B) holds and  $m/4 \equiv \delta \equiv 1 \pmod{2}$ ,

where  $\delta = o_{m_p}(p)a/o_{m_p}(r)$  being  $m_p = m/p^{v_p(m)}$  and  $a$  is the minimum positive integers such that  $r^a \equiv p^x \pmod{m_p}$ , for some  $x$ :

**Corollary 1.6** *Let  $m$  be an odd positive integer and  $r$  and  $s$  positive integers such that  $m | s(r - 1)$ .*

1. *If  $o_m(r)$  is odd, then  $\mathcal{U}(m, r, s) \simeq \mathcal{U}(2m, r, s)$ .*

2. *If  $\mathcal{U}(m, r, s)$  is a division ring then  $o_m(r)$  is odd.*

**Proof.** 1. The degree of  $\mathcal{U}(m, r, s)$  is  $n = o_m(r)$ . Thus if  $n$  is odd then  $\mathcal{U}(m, r, s) \simeq \mathcal{U}(2m, r, 2s) \simeq \mathcal{U}(2m, r, s)$ , by Lemma 1.1.

2. Assume that  $D = \mathcal{U}(m, r, s)$  is a division ring and let  $n = o_m(r)$ . The group  $G = G_{m,r,n,s}$  is a metacyclic subgroup of the group of units of  $D$  and hence  $G$  has an irreducible character whose degree coincides with the degree of  $D$  as a  $Z(D)$ -algebra which is precisely  $n$ . By Theorem 1.5,  $G \simeq G_{m_1, r_1, n_1, s_1}$  for  $m_1, r_1, n_1$  and  $s_1$  satisfying the conditions of Theorem 1.5. In particular  $mn = |G| = m_1 n_1$  and  $G$  has an abelian normal subgroup of index  $n_1$ . By Ito's Theorem [7, Theorem 6.15] the degree of every irreducible character of  $G$  divides  $n_1$ . In particular  $n | n_1$  and hence  $m_1 | m$ . If  $n$  is even then  $m_1$  and  $r_1$  do not satisfy the conditions of Theorem 1.5. Indeed, since  $m_1$  is odd condition 1 does not hold. Furthermore if we take  $q = 2$  and  $p$  is a prime divisor of  $m_1$ , then  $t = \gcd(m_1, r_1 - 1)$  is odd and hence  $\frac{p^\delta - 1}{t}$  is even so that condition 2 does not hold too. ■

## 2 The Wedderburn decomposition

In this section  $G = G_{m,r,n,s}$ , a metacyclic group as in (1.1). Since  $G$  is metabelian, Theorem 1.3 applies to describe the simple components of the Wedderburn decomposition of  $\mathbb{Q}G$ . In this section we are going to give a more precise description in terms of some lists of integers. In order to state the main theorem of this section we need to introduce the following notation:

Given a divisor  $d$  of  $n$ , a divisor  $v$  of  $m$  and an integer  $i$  we set

$$\begin{aligned}
G_d &= \langle a, b^d \rangle, \\
m_d &= \gcd(r^d - 1, m), \\
\mathcal{B}_d &= \{(v, i, c) \in \mathbb{Z}^3 : 0 < v|m_d, 0 < dc|n, \text{ and } v|s + i\frac{n}{dc}\}, \\
o_v &= o_v(r), \\
c_v &= \text{smallest positive divisor } h \text{ of } \frac{n}{o_v} \text{ such that } \gcd(v, \frac{n/o_v}{h}) \text{ divides } s, \\
n_v &= \frac{n}{o_v c_v}, \\
D_v &= \gcd(n_v, v), \\
n'_v &= \frac{n_v}{D_v}, \\
v'_v &= \frac{v}{D_v}, \\
i_v &= \text{an arbitrary integer satisfying } v|s + i_v n_v \\
o_{v,i} &= o_v / \gcd(v, i) \quad \text{and} \\
H_{v,i,d} &= \langle a^v, a^i b^d \rangle.
\end{aligned}$$

By (1.2) for every  $v|m$  and  $k \in \mathbb{Z}$  one has  $s + i_v r^k n_v \equiv (s + i_v n_v) r^k \equiv 0 \pmod{v}$  and therefore  $v'_v | i_v (r^k - 1)$ . Let

$$\alpha_{k,v} = \frac{i_v (r^k - 1)}{v'_v}.$$

For every  $a = (v, j, t) \in \mathbb{Z}^3$  such that  $0 < v|m$ ,  $0 < t|n'_v$  and  $j \in \mathbb{Z}$  let

$$i(a) = i_v t + v'_v j, \quad e_a = e_{v,j,t} = e(G, G_{o_v}, H_{v,i(a), o_v c_v t}) \quad \text{and} \quad S_a = S_{v,j,t} = \mathbb{Q}G e_a.$$

Finally set

$$\mathcal{A}_{m,r,n,s} = \{ (v, j, t) \in \mathbb{Z}^3 : 0 < v|m, 0 < t|n'_v, 0 \leq j < D_v \text{ and } \gcd(v, j, t) = 1 \}.$$

Now we can state the main result of this section that will be proof at the end of the section.

**Theorem 2.1** *Let  $G = G_{m,r,n,s}$  be the group given by the presentation (1.1), with  $m, r, n$  and  $s$  satisfying conditions (1.2) and  $\mathcal{A} = \mathcal{A}_{m,r,n,s}$ .*

1. *The primitive central idempotents of  $\mathbb{Q}G$  are the elements of the form  $e_a$  with  $a \in \mathcal{A}$ .*
2. *If  $a_1 = (v_1, j_1, t_1), a_2 = (v_2, j_2, t_2) \in \mathcal{A}$  then*

$$e_{a_1} = e_{a_2} \Leftrightarrow v_1 = v_2, t_1 = t_2 \quad \text{and} \quad j_2 \equiv j_1 r^k + \alpha_{k,v} t_1 \pmod{D_{v_1}}, \text{ for some } k \in \mathbb{Z}.$$

3. *If  $a = (v, j, t) \in \mathcal{A}$  and  $i = i(a)$  then there are exactly  $o_{v,i}$  elements  $a' \in \mathcal{A}$  such that  $e_a = e_{a'}$ , namely the elements of the form  $a' = (v, j_k, t)$ , with  $0 \leq k < o_{v,i}$ , where  $j_k$  is the remainder module  $D_v$  of  $j r^k + \alpha_{k,v} t$ .*
4. *If  $a = (v, j, t) \in \mathcal{A}$  and  $i = i(a)$  then there exist integers  $v_1, c_1, i_1$  and  $i'$  satisfying the following conditions*

$$v_1 v + c_1 c_v t = 1 + i_1 i \quad \text{and} \quad i' i_1 \equiv 1 \pmod{c_v t}. \quad (2.3)$$

Moreover,

$$S_a = \mathbb{Q}G e_a \simeq M_{o_{v,i}}(\mathcal{U}(v c_v t, 1 + c_1 c_v t (r^{o_{v,i}} - 1), i' v_1 v - i)),$$

for every list of integers  $v_1, c_1, i_1$  and  $i'$  satisfying (2.3).

The next lemma provides information on the groups of the form  $G_d$  and  $H_{v,i,d}$ .

**Lemma 2.2** 1. The subgroups of  $G$  containing  $\langle a \rangle$  are the groups of the form  $G_d$  with  $d|n$ .

2. If  $d|n$  then  $G'_d = \langle a^{r^d-1} \rangle = \langle a^{m_d} \rangle$ .

3.  $G_{o_m}$  is a maximal element of  $\{A \leq G : A \text{ is abelian and } G' \leq A \leq G\}$ .

4. If  $d|n$ ,  $v|m_d$  and  $i \in \mathbb{Z}$  then  $H_{v,i,d} = \{a^j b^k : d|k \text{ and } j \equiv i \frac{k}{d} \pmod{v}\}$ . Moreover if  $v|s + i \frac{n}{d}$  then  $H_{v,i,d} \cap \langle a \rangle = \langle a^v \rangle$  and  $N_G(H_{v,i,d}) = G_{o_{v,i}}$ .

5. Two subgroups of the form  $H_{v,i,d}$  with  $0 < d|n$ ,  $0 < v|m_d$  and  $v|s + i \frac{n}{d}$  are equal if and only if the  $v$  and  $d$  parameters are equal and the  $i$  parameters are congruent module  $v$ ; that is if  $0 < d_j|n$ ,  $0 < v_j|m_{d_j}$  and  $i_j \in \mathbb{Z}$  ( $j = 1, 2$ ) then

$$H_{v_1, i_1, d_1} = H_{v_2, i_2, d_2} \iff v_1 = v_2, \quad d_1 = d_2 \quad \text{and} \quad i_1 \equiv i_2 \pmod{v_1}.$$

6. If  $d|n$  then the subgroups of  $G_d$  containing  $G'_d$  are the groups of the form  $H_{v,i,d,c}$  with  $(v, i, c) \in \mathcal{B}_d$ .

7. Let  $(v, i, c) \in \mathcal{B}_d$  and  $H = H_{v,i,d,c}$ . Then  $G_d/H$  is cyclic if and only if  $\gcd(v, i, c) = 1$ . In that case there are integers  $v_1, c_1, i_1$  and  $i'$  satisfying the following conditions:

$$v_1 v + c_1 c = 1 + i_1 i \quad \text{and} \quad i' i_1 \equiv 1 \pmod{c} \quad (2.4)$$

If  $v_1, c_1, i_1$  and  $i'$  is a list of integers satisfying (2.4) then  $x = a^{c_1} b^{d i_1} H$  is a generator of  $G_d/H$ , (namely  $aH = x^c$  and  $b^d H = x^{i' v_1 v - i}$ ).

8. Let  $d|n$  and assume that  $(v, i, c) \in \mathcal{B}_d$  and  $\gcd(v, i, c) = 1$ . Then  $G_{o_v}$  is the unique maximal element of  $\{B \leq G : G_{o_m} \leq B, B' \leq H_{v,i,d,c} \leq B\}$ . Assume that  $d = o_v$  and let  $v_1, c_1, i_1$  and  $i'$  be integers satisfying conditions (2.4). Then

$$\mathbb{Q}Ge(G, G_{o_v}, H_{v,i,o_v,c}) \simeq M_{o_v,i}(\mathcal{U}(vc, 1 + c_1 c(r^{o_v,i} - 1), i' v_1 v - i)).$$

**Proof.** 1, 2 and 3 are obvious.

4. Set  $H = H_{v,i,d}$  and  $K = \{a^j b^k : d|k \text{ and } j \equiv i \frac{k}{d} \pmod{v}\}$ . By using that  $v|m_d|r^d - 1$  one deduces  $G'_d = \langle a^{m_d} \rangle \leq \langle a^v \rangle \leq H$  and one can easily prove that  $K$  is a subgroup of  $G$ . Then  $H \leq K$  because  $a^v, a^i b^d \in K$ . Thus to prove that  $H = K$  one can assume that  $K$  is abelian by factoring out by  $G'_d$ . If  $d|k$  and  $j \equiv i \frac{k}{d} \pmod{v}$ , then  $a^j b^k = a^{j - i \frac{k}{d}} (a^i b^d)^{k/d} \in H$ . This proves that  $H = K$ .

Assume now that  $v|s + i \frac{n}{d}$ . If  $x \in H \cap \langle a \rangle$  then  $x = a^j b^k$  for  $j$  and  $k$  integers such that  $n|k$  and  $j \equiv i \frac{k}{d} \pmod{v}$ . Then  $x = a^{j + s \frac{k}{n}}$  and  $j + s \frac{k}{n} \equiv (i \frac{n}{d} + s) \frac{k}{n} \equiv 0 \pmod{v}$ . Thus  $x \in \langle a^v \rangle$  and this proves that  $H \cap \langle a \rangle = \langle a^v \rangle$ .

Since  $G'_d \leq H \leq G_d$ ,  $N_G(H) \geq G_d$  and hence  $N_G(H) = G_t$  for some divisor  $t$  of  $d$ . In particular  $a$  normalizes  $H$  and, since  $\langle a^v \rangle$  is normal in  $G$ , if  $x$  is a divisor of  $d$  then  $H \leq G_x$  if and only if  $a^{i r^x} b^d = b^{-x} a^i b^d b^x \in H$  if and only if  $a^{i(r^x - 1)} = a^{i r^x} b^d (a^i b^d)^{-1} \in H$  if and only if  $v|i(r^x - 1)$  if and only if  $r^x \equiv 1 \pmod{v/\gcd(v, i)}$  if and only if  $o_{v,i}|x$ . Therefore  $t = o_{v,i}$ .

5. It follows from 4, by noticing that  $H_{v,i,d} \cap \langle a \rangle = \langle a^v \rangle$  and  $H_{v,i,d}/\langle a^v \rangle$  is cyclic of order  $n/d$ .

Notice that if  $d$  is a divisor of  $n$  then  $G_d$  is a metacyclic group and therefore to prove 6 and 7 one may assume without loss of generality that  $G = G_d$ , that is  $d = 1$ .

6. From 4 one deduces that if  $(v, i, c) \in \mathcal{B}_1 (= \mathcal{B}_d)$  then  $G' = \langle a^{m_1} \rangle \subseteq \langle a^v \rangle \leq H_{v,i,c}$ . Conversely, let  $H$  be a subgroup of  $G$  containing  $G'$ . We want to show that  $H = H_{v,i,c}$  for some  $(v, i, c) \in \mathcal{B}_1$ .

Factoring out by  $G'$  one may assume that  $G$  is abelian. Let  $H \cap \langle a \rangle = \langle a^v \rangle$ , with  $v$  a divisor of  $m$ . Then  $H/\langle a^v \rangle \simeq H\langle a \rangle/\langle a \rangle \leq G/\langle a \rangle$ . Since  $G/\langle a \rangle$  is cyclic of order  $n$  and it is generated by  $b\langle a \rangle$ ,  $H\langle a \rangle/\langle a \rangle$  is cyclic generated by  $b^c\langle a \rangle$  for some divisor  $c$  of  $n$ . Then there is  $i \in \mathbb{Z}$  such that  $H/\langle a^v \rangle$  is generated by  $a^i b^c \langle a^v \rangle$  and hence  $H = \langle a^v, a^i b^c \rangle = H_{v,i,c}$ . Finally,  $(a^i b^c)^{\frac{n}{c}} = a^{s+i\frac{n}{c}} \in H \cap \langle a \rangle = \langle a^v \rangle$  and therefore  $v|s+i\frac{n}{c}$ .

7. Let  $(v, i, c) \in \mathcal{B}_1 (= \mathcal{B}_d)$  and set  $H = H_{v,i,c}$ . Then  $G/H$  has the following presentation:  $\langle a, b | a^v = 1, b^c = a^i, ba = ab \rangle$ . The order of  $G$  is  $vc$  and, by the classification of the finite abelian groups, its period is  $vc/\gcd(v, i, c)$ . Thus  $G/H$  is cyclic if and only if  $\gcd(v, i, c) = 1$ .

Assume that  $\gcd(v, i, c) = 1$ . By Lemma 1.2, there is  $i_1 \in \mathbb{Z}$  such that  $\gcd(i_1, c) = 1$  and  $i_1 i \equiv -1 \pmod{\gcd(v, c)}$ . From this the existence of  $v_1, c_1, i' \in \mathbb{Z}$  satisfying (2.4) follows.

Now assume that  $v_1, c_1, i_1$  and  $i'$  are integers satisfying (2.4) and let  $x = a^{c_1} b^{i_1} H$ ,  $a_1 = aH$  and  $b_1 = bH$  (remember that we are assuming that  $d = 1$ ). Thus  $a_1^v = a_1^{c_1} b_1^{i_1} = 1$  and  $x = a_1^{c_1} b_1^{i_1}$ . Having in mind that  $G/H$  is cyclic one has

$$x^c = a_1^{cc_1} b_1^{ci_1} = a_1^{cc_1 - ii_1} = a_1^{1-v_1v} = a_1$$

and, if  $c'c + i'i_1 = 1$ , then

$$x^{i'v_1v-i} = x^{i'(1-c_1c)-i(1-i'i_1)} = x^{i'-c(i'c_1+ic')} = a_1^{c_1 i'} b_1^{i' i_1} a_1^{-(i'c_1+ic')} = b_1^{i'i_1+c'c} = b_1.$$

This proves that  $x$  is a generator of  $G/H$ .

8. Let  $d|n$  and  $(v, i, c) \in \mathcal{B}_d$ . Set  $H = H_{v,i,dc}$  and

$$X = \{B \leq G \quad : \quad G_{o_m} \leq B, \quad B' \leq H \leq B\}$$

Since  $o_v|o_m$ ,  $G_{o_m} \leq G_{o_v}$ . Moreover, since  $v|m_d$ , one has  $o_v|d$  and therefore

$$G'_{o_v} = \langle a^{r^{o_v}-1} \rangle \leq \langle a^v \rangle \leq H \leq G_d \leq G_{o_v}.$$

This proves that  $G_{o_v} \in X$ . Let  $B \in X$ . Since  $G_{o_m} \leq B$  then  $B = G_t$  for some divisor  $t$  of  $o_m$ . Thus  $B' = \langle a^{r^t-1} \rangle \subseteq H \cap \langle a \rangle = \langle a^v \rangle$ . This implies that  $v|r^t-1$  and then  $o_v|t$  which implies that  $B = G_t \subseteq G_{o_v}$ . We conclude that  $G_{o_v}$  is the unique maximal element of  $X$ .

In the remainder of the proof we assume that  $d = o_v$  and set  $x = a^{c_1} b^{d i_1} H$ . By 4,  $N = N_G(H) = G_o$ , where  $o = o_{v,i}$ . Thus  $[G : N] = o$ ,  $[G_d : H] = vc$  and  $N/G_d$  is cyclic of order  $d/o$ , generated by  $b^o H$ . By Theorem 1.3,  $\mathbb{Q}G\mathbb{e}(G, G_d, H) \simeq M_o(\mathbb{Q}_{vc} *_{\sigma}^{\tau} N/K)$  where  $\sigma$  and  $\tau$  are given as in Theorem 1.3. Since  $N/G_d$  is cyclic,  $\mathbb{Q}_{vc} *_{\sigma}^{\tau} N/K$  is a cyclic algebra  $\mathcal{U}(vc, u, t)$ , where  $u$  and  $t$  are integers satisfying  $(bH)^{-o} x (bH)^o = x^u$  and  $(b^o)^{d/o} H = x^t$ .

Using 7 one obtains  $(b^o)^{d/o} H = b^d H = x^{i'v_1v-i}$  and

$$\begin{aligned} (bH)^{-o} x (bH)^o &= b^{-o} a^{c_1} b^{d i_1} b^o H = a^{c_1 r^o} b^{d i_1} H = x^{cc_1 r^o + i_1(i'v_1v-i)} \\ &= x^{cc_1(r^o-1) + cc_1 - i_1 i + i_1 i' v_1 v} = x^{1 + cc_1(r^o-1) + v_1 v(i_1 i' - 1)} = x^{1 + cc_1(r^o-1)}, \end{aligned}$$

where the last equality is a consequence of the fact that  $i_1 i' \equiv 1 \pmod{c}$  and  $x$  has order  $vc$ . Thus one can take  $u = 1 + cc_1(r^o - 1)$  and  $t = i'v_1v - i$  as wanted. ■

Now we show some relations on the numerical information attached to the group  $G$ .

**Lemma 2.3** *Let  $v$  be a divisor of  $m$ ,  $t$  a divisor of  $n'_v$  and  $i$  an arbitrary integer.*

1.  $\gcd(\frac{n_v}{t}, v) = D_v$  and therefore  $v|s + i\frac{n_v}{t}$  if and only if  $i = i_v t + v'_v j$  for some  $j \in \mathbb{Z}$ .

2. If  $v|s + in_v$  then  $\gcd(i, c_v) = 1$ , or equivalently  $\gcd(i_v + v'_v j, c_v) = 1$ , for every  $j \in \mathbb{Z}$ .
3. Every prime divisor of  $c_v$  is also a prime divisor of  $v'_v$ .
4. If  $j \in \mathbb{Z}$  and  $i = i_v t + v'_v j$  then

$$\gcd(v, i, c_v t) = 1 \iff \gcd(v, i, t) = 1 \iff \gcd(v, j, t) = 1.$$

**Proof.** 1 is obvious.

2. Let  $h = \gcd(i, c_v)$ . Then  $v|s + \frac{i}{h} \frac{n/o_v}{c_v/h}$  and hence  $\gcd(v, \frac{n/o_v}{c_v/h})|s$ . By the definition of  $c_v$ ,  $\frac{c_v}{h} \geq c_v$  and hence  $h = 1$ .

3. Is a particular case of Lemma 1.2 for  $x = \frac{n}{o_v}$ ,  $y = v$  and  $z = s$ .

4. Since  $\gcd(v, j, t) | \gcd(v, i, t) | \gcd(v, i, c_v t)$ , we only have to prove that  $\gcd(v, j, t) = 1$  implies  $\gcd(v, i, c_v t) = 1$ . By means of contradiction assume that  $\gcd(v, j, t) = 1$  and  $\gcd(v, i, c_v t)$  has a prime divisor  $p$ . We claim that  $p$  divides  $t$ . Indeed, otherwise  $p$  divides  $c_v$  and hence  $p$  divides  $v'_v$ , by 3. This implies that  $p$  divides  $i_v t$  and hence  $p | \gcd(i_v t, c_v)$  contradicting 2. So  $p|t$  and hence  $p$  divides  $v'_v j$  and using that  $p$  divides  $v$  and  $\gcd(v, t, j) = 1$  one deduces that  $p$  divides  $v'_v$ . Therefore  $v_p(v) > v_p(D_v) = v_p(\frac{n_v}{t})$ , by 1. Thus  $v_p(t) > v_p(n_v) - v_p(v)$ . Since  $t$  is a divisor of  $n'_v$ ,  $v_p(n'_v) \geq v_p(t) > 0$ , and hence  $v_p(n_v) > v_p(D_v)$ . Thus  $v_p(D_v) = v_p(v) < v_p(n_v)$  and  $v_p(t) \leq v_p(n'_v) = v_p(n_v) - v_p(D_v) = v_p(n_v) - v_p(v) < v_p(t)$ , a contradiction. ■

We have collected enough tools to prove Theorem 2.1.

**Proof of Theorem 2.1.** We start proving that for  $a_1 = (v_1, j_1, t_1), a_2 = (v_2, j_2, t_2) \in \mathbb{Z}^3$  with  $v_l|m$  and  $t_l|n'_v$  ( $l = 1, 2$ ) then  $e_{a_1} = e_{a_2}$  if and only if  $v_1 = v_2$ ,  $t_1 = t_2$  and  $j_2 \equiv j_1 r^k + \alpha_{v,k} \pmod{D_{v_1}}$  for some  $k$ . Statement 2 is an obvious consequence of this.

Set  $i_l = i(a_l)$ ,  $d_l = o_{v_l}$  and  $c_l = c_{v_l} t_l$  ( $l = 1, 2$ ). By Proposition 1.4,  $e_{a_1} = e_{a_2}$  if and only if there is  $g \in G$  such that  $G_{d_2} \cap H_{v_1, i_1, d_1 c_1}^g = G_{d_1}^g \cap H_{v_2, i_2, d_2 c_2} = G_d \cap H_{v_2, i_2, d_2 c_2}$ . In such case  $\langle a^{v_1} \rangle = G_{d_2} \cap H_{v_1, i_1, d_1 c_1}^g \cap \langle a \rangle = G_{d_1} \cap H_{v_2, i_2, d_2 c_2} \cap \langle a \rangle = \langle a^{v_2} \rangle$ . Thus  $v_1 = v_2$  and as a consequence  $d_1 = d_2$  and  $H_{v_1, i_1, d_1 c_1}^g = G_{d_2} \cap H_{v_1, i_1, d_1 c_1}^g = G_{d_1} \cap H_{v_1, i_2, d_1 c_2} = H_{v_1, i_2, d_1 c_2}$ . By Lemma 2.2,  $N_G(H_{v_1, i_1, d_1 c_1}) = G_{o_{v_1, i_1}}$  and therefore  $g$  can be taken of the form  $g = b^k$  for some  $0 \leq k < o_{v_1, i_1}$ . Then  $H_{v_1, i_1 r^k, d_1 c_1} = H_{v_1, i_1, d_1 c_1}^{b^k} = H_{v_1, i_2, d_1 c_2}$ . Applying Lemma 2.2 once more one deduces that  $c_1 = c_2$ , or equivalently  $t_1 = t_2$ , and  $i_1 r^k \equiv i_2 \pmod{v_1}$ . Set  $v = v_1$  and  $t = t_1$ . Then  $v|i_1 r^k - i_2 = i_v t(r^k - 1) + v'_v(j_1 r^k - j_2) = v'_v(\alpha_{k,v} t + j_1 r^k - j_2)$  and therefore  $j_2 \equiv j_1 r^k + \alpha_{k,v} \pmod{D_v}$ . The converse follows by reversing the arguments.

1. By Lemma 2.2,  $A = G_{o_m}$  is a maximal abelian subgroup of  $G$  containing  $G'$  and the subgroups of  $G$  containing  $A$  are the groups of the form  $G_d$  with  $d|o_m$ . Since  $G$  is metabelian, by Theorem 1.3 the primitive central idempotents of  $\mathbb{Q}G$  are the elements of the form  $e(G, G_d, H)$  with  $d$  a divisor of  $o_m$  and  $H$  a subgroup of  $G$  such that  $G_d$  is maximal element in the set  $X_H = \{B \leq G : A \leq B \text{ and } B' \leq H \leq B\}$  and  $G_d/H$  is cyclic. We are going to use this in the remainder of the proof without specific mention.

First we prove that if  $a = (v, j, t) \in \mathcal{A}$  then  $e_a$  is a primitive central idempotent of  $\mathbb{Q}G$ . Set  $i = i(a)$  and  $H = H_{v, i, o_v c_v t}$ . Notice that  $(v, i, c_v t) \in \mathcal{B}_{o_v}$  because  $v|m_{o_v}$ ,  $t|n'_v$  and  $v|s + i \frac{n_v}{t}$ . Therefore  $v|m_{o_v}$ ,  $o_v c_v t|n$  and  $v|s + \frac{n}{o_v c_v t}$ . Moreover  $\gcd(v, i, c_v t) = 1$ , by Lemma 2.3, and hence  $G_{o_v}/H$  is cyclic, by statement 7 of Lemma 2.2. By statement 8 of Lemma 2.2,  $G_{o_v}$  is the unique maximal element element of  $X_H$  and we conclude that  $e_a = e(G, G_{o_d}, H)$  is a primitive central idempotent of  $\mathbb{Q}G$ .

Conversely, let  $e$  be a primitive central idempotent of  $\mathbb{Q}G$ . Thus  $e = e(G, G_d, H)$  with  $d$  a divisor of  $o_m$ ,  $H$  a subgroup of  $G$ ,  $G_d$  a maximal element of  $X_H$  and  $G_d/H$  cyclic. By statement 6 of Lemma 2.2,  $H = H_{v,i,dc}$  with  $(v, i, c) \in \mathcal{B}_d$  and  $\gcd(v, i, c) = 1$ . Moreover  $d = o_v$ , by statement 8 of Lemma 2.2. Thus  $(v, i, c) \in \mathcal{B}_{o_v}$ , hence  $v|s + i\frac{n}{o_v c}$  and so  $\gcd(v, \frac{n}{o_v c})$  divides  $s$  or equivalently  $c_v|c$ , that is  $c = c_v t$  for some  $t|n_v$ . Thus  $t|n'_v$  and  $v|s + i\frac{n_v}{t}$ . By Lemma 2.3,  $i = i_v t + v'_v j$  for some  $j \in \mathbb{Z}$  and  $\gcd(v, j, t) = 1$ . Thus  $e = e(G, G_{o_v}, H_{v,i,o_v c_v t}) = e_{v,j,t}$ . If  $j \equiv j_1 \pmod{D_v}$  then  $e = e_{v,j_1,t}$ , by the first paragraph of the proof, and  $\gcd(v, j_1, t) = \gcd(D_v, j_1, t) = \gcd(D_v, j, t) = \gcd(v, j, t) = 1$ . Thus by replacing  $j$  by its remainder module  $D_v$ , we may assume that  $(v, j, t) \in \mathcal{A}$  and the proof of 1 is finished.

3. By 2, the elements of  $\mathcal{A}$  that give rise to the same idempotent than  $(v, j, t)$  are the elements of the form  $(v, j_1, t) \in \mathcal{A}$  with  $j_1 \equiv jr^k + \alpha_{k,v} t \pmod{D_v}$  for some  $k \in \mathbb{Z}$ . If  $i = i_v t + v'_v j$  and  $i_1 = i_v t + v'_v j_1$ , then  $j_1 \equiv jr^k + \alpha_{k,v} t \pmod{D_v}$  if and only if  $i_1 \equiv ir^k \pmod{v}$ . Therefore there are as many integers  $0 \leq j_1 < D_v$  satisfying  $j_1 \equiv jr^k + \alpha_{k,v} t \pmod{D_v}$  as classes module  $v$  of elements of the form  $ir^k$ , and this number coincides with the number of classes module  $\gcd(i, v)$  of powers of  $r$  which is equal to  $o_{v,i}$ . Moreover this  $o_{v,i}$  classes module  $\gcd(i, v)$  are realized with the exponents  $0 \leq k < o_{v,i}$  and therefore the  $o_{v,i}$  different elements of  $\mathcal{A}$  that give rise to  $e_{v,j,t}$  are the elements of the form  $(v, j_1, t)$  with  $j_1$  running on the reminders module  $D_v$  of the elements of the form  $jr^k + \alpha_{k,v} t$ , with  $0 \leq k < o_{v,i}$ .

4. If  $a = (v, j, t) \in \mathcal{A}$  and  $i = i(a)$  then  $(v, i, c_v t) \in \mathcal{B}_{o_v}$  and  $\gcd(v, i, t) = 1$ , by Lemma 2.3. Now statements 7 of 8 of Lemma 2.2 apply. ■

### 3 $\text{Aut}(\mathbb{Q}G)$ for $n = pq$

The aim of this section is to provide enough information to compute  $\text{Aut}(\mathbb{Q}G)$  for  $G = G_{m,r,n,s}$  where  $n$  is the product of two primes. The case of  $n$  being prime was considered in [6]. Unfortunately there is an error in the main theorem of [6]. Our results will also correct this error along the way. Following the program explained in the introduction we first have to compute simple components of the Wedderburn decomposition of  $\mathbb{Q}G$  and then classify these simple components in isomorphism classes. The first can be done as explained in Section 2. We are going to present a more precise description in Proposition 3.1. Theoretically one could attack the second problem by using classical methods including the Brauer-Witt Theorem, and methods to compute local Schur indices of cyclic algebras and Hasse invariants. Unfortunately these methods are usually difficult to apply in concrete examples.

Throughout this section  $p$  and  $q$  denote prime integers, not necessarily different,  $G = G_{m,r,n,s}$  is a metacyclic group as in (1.1) with  $n = pq$  and  $\mathcal{A} = \mathcal{A}_{m,r,n,s}$ . By Theorem 2.1 the primitive central idempotents of  $\mathbb{Q}G$  are parametrized by the elements of  $\mathcal{A}$ . We define the following two equivalent relations in  $\mathcal{A}$ :

$$a_1 \equiv a_2 \Leftrightarrow S_{a_1} = S_{a_2} \quad \text{and} \quad a_1 \sim a_2 \Leftrightarrow S_{a_1} \simeq S_{a_2}.$$

Solving Problem 1 of the introduction for  $G$  is equivalent to describing the partition  $\mathcal{A}/\equiv$  and solving Problem 2 is equivalent to describe the partition  $\mathcal{A}/\sim$ .

If  $\mathcal{P}_1$  and  $\mathcal{P}_2$  are two partitions of a set then we write  $\mathcal{P}_1 \leq \mathcal{P}_2$  if  $\mathcal{P}_1$  is less or equally fine than  $\mathcal{P}_2$ , that is if every element of  $\mathcal{P}_1$  contains an element of  $\mathcal{P}_2$ . For every  $d|n$  let  $\mathcal{A}_d = \{a = (v, j, t) \in \mathcal{A} : o_v = d\}$ . Then  $\mathcal{P} = \{\mathcal{A}_1, \mathcal{A}_p, \mathcal{A}_q, \mathcal{A}_{pq}\}$  is a partition of  $\mathcal{A}$ . If  $a_1 = (v_1, j_1, t_1), a_2 = (v_2, j_2, t_2) \in \mathcal{A}$  then the degree of  $S_{a_i}$  is  $o_{v_i}$  and therefore

$$a_1 \equiv a_2 \quad \Rightarrow \quad a_1 \sim a_2 \quad \Rightarrow \quad o_{v_1} = o_{v_2}.$$

Thus  $\mathcal{P} \leq \mathcal{A}/ \sim \leq \mathcal{A}/ \equiv$  and hence describing  $\mathcal{A}/ \equiv$  and  $\mathcal{A}/ \sim$  reduces to describing  $\mathcal{A}_k/ \equiv$  and  $\mathcal{A}_k/ \sim$  for  $k|pq$ . To avoid trivialities we do not consider  $k = 1$  and by symmetry we also do not consider  $k = q$ . So in the remaining of the paper we study the partitions  $\mathcal{A}_k/ \equiv$  and  $\mathcal{A}_k/ \sim$  for  $k = p$  and  $k = pq$ .

### 3.1 $\mathcal{A}_p/ \equiv$ and $\mathcal{A}_{pq}/ \equiv$

If  $v|m$  and  $o_v = pq$  then  $n_v = 1$  and therefore

$$\mathcal{A}_{pq} = \{(v, 0, 1) : v|m, r^p \not\equiv 1 \not\equiv r^q \pmod{v}\}.$$

By Theorem 2.1,  $\mathcal{A}_{pq} = \mathcal{A}_{pq}/ \equiv$ , that is the  $\equiv$ -classes of  $\mathcal{A}_{pq}$  have one element.

For every divisor  $v$  of  $m$  let  $[v]$  denote the set of elements of  $\mathcal{A}$  whose first coordinate is  $v$  and let  $\mathcal{Q} = \{[v] : v|m, o_v = p\}$ , a partition of  $\mathcal{A}_p$ . By Theorem 2.1,  $\mathcal{Q} \leq \mathcal{A}_p/ \equiv$  and thus describing  $\mathcal{A}_p/ \equiv$  reduces to describing  $[v]/ \equiv$  for every  $v|m$  such that  $o_v = p$ .

Fix  $v|m$  such that  $o_v = p$ . A simple argument shows that

$$D_v = \begin{cases} q, & \text{if } q|v \text{ and } q|s; \\ 1, & \text{otherwise;} \end{cases} \quad \text{and} \quad n'_v = \begin{cases} 1, & \text{if } q|v; \\ q, & \text{if } q \nmid v \end{cases}$$

and therefore

$$[v] = \begin{cases} \{(v, 0, 1), (v, 0, q)\} & \text{if } q \nmid v \\ \{(v, 0, 1)\} & \text{if } q|v \text{ and } q \nmid s \\ \{(v, j, 1) : 0 \leq j < q\} & \text{if } q|v \text{ and } q|s \end{cases} \quad (3.5)$$

Let  $a = (v, j, t) \in \mathcal{A}_p$  and  $\bar{a}$  the  $\equiv$ -class containing  $a$ . By Theorem 2.1 and (3.5), if  $q \nmid s$  or  $q \nmid v$  then  $\bar{a} = \{a\}$ . Assume that  $q|s$  and  $q|v$ . Then one can take  $i_v = -s/q$  and with this choice one has  $i(a) = \frac{vj-s}{q}$ . By Theorem 2.1,  $\bar{a}$  has cardinality  $o_{v,i(a)}$ , a divisor of  $o_v = p$ . Assume first that  $q|r-1$ . Then using  $v|(r-1)s$  one has that  $o_{v,i(a)} = 1$  if and only if  $v|(r-1)i(a)$  if and only if  $v|(r-1)\frac{s}{q}$  if and only if  $q|\frac{(r-1)s}{v}$ . Therefore if  $v_q(v) < v_q((r-1)s)$  then  $[v] = [v]/ \equiv$  and otherwise  $[v]$  is formed by  $\equiv$ -classes of cardinality  $p$  and this implies that  $p = q$ , so that  $[v]/ \equiv$  has exactly one element. Assume now that  $q \nmid r-1$ , then  $o_{v,i(a)} = 1$  if and only if  $v|(r-1)i(a) = (r-1)\frac{sj-v}{q}$  if and only if  $q$  divides  $\frac{q(r-1)i(a)}{v} = (r-1)j - \frac{s(r-1)}{v}$  if and only if  $\frac{s(r-1)}{v} \equiv (r-1)j \pmod{q}$ . Therefore in this case  $[v]/ \equiv$  has exactly one element of cardinality 1, namely  $\{(v, j, 1)\}$ , where  $j$  is the solution of the equation  $(r-1)X = \frac{s(r-1)}{v}$  in  $\mathbb{Z}_q$ . This implies that  $p|q-1$  and  $[v]$  is formed by one  $\equiv$ -class of cardinality 1 and  $\frac{q-1}{p}$  classes of cardinality  $p$ .

The following proposition collects the information obtained about the description of  $\mathcal{A}_p/ \equiv$  and  $\mathcal{A}_{pq}/ \equiv$ .

**Proposition 3.1** 1.  $\mathcal{A}_{pq} = \mathcal{A}_{pq}/ \equiv$ .

2. If  $q \nmid s$  then  $\mathcal{A}_p = \mathcal{A}_p/ \equiv$ .

3. Assume that  $\mathcal{A}_p \neq \mathcal{A}_p/ \equiv$  (and so  $q|s$ ). Then every  $\equiv$ -class has either 1 or  $p$ -elements and the  $\equiv$ -classes with  $p$  elements are embedded in the sets of the form  $[v]$  with  $v|m$ ,  $o_v = p$  and  $q|v$ .

(a) If  $q|r-1$  then  $p = q$  and the  $\equiv$ -classes with  $p$  elements are the sets of the form  $[v]$  with  $v|m$ ,  $o_v = p$  and  $v_p(v) = v_p((r-1)s)$ .

- (b) If  $q \nmid r - 1$  then  $p|q - 1$  and for every  $v|m$  such that  $q|v$ ,  $[v]/\equiv$  is formed by one class with one element, namely  $\{(v, j, 1)\}$  with  $0 \leq j < q$  and  $(r - 1)j \equiv \frac{s(r-1)}{v} \pmod{q}$ , and  $(q - 1)/p$  classes with  $p$  elements.

Now we focus on the description of the  $\sim$ -classes. The Schur index of a central simple algebra  $A$  is denoted by  $\text{ind}(A)$ . The index  $\text{ind}(C)$  of an equivalence class  $C$  of  $\mathcal{A}/\sim$  is by definition  $\text{ind}(S_a)$ , for  $a$  a representative of  $C$ .

For every divisor  $v$  of  $m$  we choose  $i_v$  as follows:

$$i_v = \begin{cases} -s & \text{if } o_v = pq \text{ or } q|v, q \nmid s \text{ and } o_v = p, \\ -s/q & \text{if } q|v, q|s \text{ and } o_v = p, \\ -sy & \text{if } q \nmid v \text{ and } o_v = p \end{cases} \quad (3.6)$$

### 3.2 $\mathcal{A}_{pq}/\sim$

For every subset  $X$  of  $\mathcal{A}_{pq}$  we set  $\overline{X} = \{v : (v, 0, 1) \in X\}$ . Let  $v \in \overline{\mathcal{A}_{pq}}$ . By Theorem 2.1, and having in mind that  $n_v = 1$  and we have taken  $i_v = -s$  then

$$S_{v,0,1} \simeq \mathcal{U}(v, r, s).$$

The main result on the components of degree  $pq$  is the following.

**Theorem 3.2** *Assume that  $q \leq p$  and let  $C$  be a class of  $\mathcal{A}_{pq}/\sim$  with  $|C| \geq 2$ . Then there is an integer  $d$  such that either  $\overline{C} = \{d, 2d\}$  with  $2 \nmid d$  or  $q = 2$  and one of the following conditions holds:*

1.  $\overline{C} \subseteq \{3d, 4d, 6d\}$ , with  $\gcd(6, d) = 1$  and  $\text{ind}(C)|p$ .
2.  $2p + 1$  is prime,  $2p + 1 \nmid d|r - 1$ ,  $\text{ind}(C)|2$  and one of the following conditions holds:
  - (a)  $\overline{C} \subseteq \{2pd, (2p + 1)d, 3pd\}$  with  $2, p|d$  and if  $3pd \in \overline{C}$  then  $3 \nmid d$ . In this case  $\text{ind}(C) = 1$ .
  - (b)  $\overline{C} \subseteq \{4pd, 3pd, 6pd, (2p + 1)d, 2(2p + 1)d\}$ , with  $\gcd(2p, d) = p \neq 2$  and if  $\{3d, 6d\} \cap \overline{C} \neq \emptyset$  then  $3 \nmid d$ . Moreover if  $4pd \in \overline{C}$  then  $\text{ind}(C) = 1$ .
  - (c)  $\overline{C} \subseteq \{8d, 12d, 5d, 10d\}$  with  $p = 2$ ,  $\gcd(10, d) = 1$  and if  $12d \in \overline{C}$  then  $3 \nmid d$ . Moreover if  $8d \in \overline{C}$  then  $\text{ind}(C) = 1$ .
  - (d)  $\overline{C} \subseteq \{9d, 18d, 7d, 14d\}$ , with  $p = 3$ ,  $\gcd(21, d) = 1$  and if  $\overline{C} \cap \{18d, 14d\} \neq \emptyset \in \overline{C}$  then  $2 \nmid d$ .

As a consequence one obtains the following restrictions on the cardinalities of the  $\sim$ -classes of  $\mathcal{A}_{pq}$ .

**Corollary 3.3** *Let  $C$  be an isomorphism class of simple components of the Wedderburn decomposition of  $\mathbb{Q}G_{m,r,pq,s}$ , with  $q \leq p$  prime integers formed by simple algebras of degree  $pq$ . Then*

1.  $|C| \leq 5$  and if  $\text{ind}(C) = pq$  then  $|C| \leq 2$ .
2. If either  $m$  or  $pq$  is odd then  $|C| \leq 2$ .
3. If  $m$  is odd and  $\text{ind}(C) = pq$  then  $|C| = 1$ .
4. If  $3 \nmid m$  or  $2p + 1$  is not prime then  $|C| \leq 3$ .

5. If  $\gcd(m, 6) = 1$  then  $|C| = 1$ .

Before proving Theorem 3.2 we prove some lemmas which will be used to recognize isomorphic simple components of  $\mathbb{Q}G$ . The Euler function is denoted by  $\phi$ .

**Lemma 3.4** *If  $d|v$  are integers then*

1.  $\phi(v) = \phi(d)$  if and only either  $d = v$  or  $d$  is odd and  $v = 2d$ .
2.  $\phi(v) = p\phi(d)$  if and only if  $p = 2$ ,  $\gcd(d, \frac{v}{d}) = 1$  and  $\frac{v}{d}$  is either 3, 4 or 6.
3.  $\phi(v) = pq\phi(d)$  with  $q \leq p$  if and only if one of the following conditions holds:
  - (a)  $v = pqd$  and  $p, q|d$ .
  - (b)  $v = 2pqd$ ,  $p, q|d$  and  $\gcd(2, d) = 1$ .
  - (c)  $q = 2$  and one of the following conditions holds:
    - (c1)  $v = 4pd$ ,  $p|d$  and  $\gcd(2p, d) = p \neq 2$ .
    - (c2)  $v = 3pd$ ,  $p|d$ , and  $\gcd(3p, d) = p \neq 3$ .
    - (c3)  $v = 6pd$ ,  $p|d$ , and  $\gcd(6p, d) = p \neq 2, 3$ .
    - (c4)  $v = 8d$ ,  $p = 2$  and  $\gcd(2, d) = 1$ .
    - (c5)  $v = 12d$ ,  $p = 2$  and  $\gcd(6, d) = 1$ .
    - (c6)  $v = 9d$ ,  $p = 3$  and  $\gcd(3, d) = 1$ .
    - (c7)  $v = 18d$ ,  $p = 3$  and  $\gcd(6, d) = 1$ .
    - (c8)  $v = (2p + 1)d$ ,  $2p + 1$  prime and  $\gcd(2p + 1, d) = 1$ .
    - (c9)  $v = 2(2p + 1)d$ ,  $2p + 1$  prime and  $\gcd(2(2p + 1), d) = 1$ .

**Proof.** Write  $v = p_1^{\alpha_1} \cdots p_k^{\alpha_k} q_1^{\beta_1} \cdots q_l^{\beta_l}$  and  $d = p_1^{\gamma_1} \cdots p_k^{\gamma_k}$  with  $p_1, \dots, p_k, q_1, \dots, q_l$  different primes,  $\alpha_i \geq \gamma_i \geq 1$  for every  $1 \leq i \leq k$  and  $\beta_j \geq 1$  for every  $1 \leq j \leq l$ . Then

$$\frac{\phi(v)}{\phi(d)} = p_1^{\alpha_1 - \gamma_1} \cdots p_k^{\alpha_k - \gamma_k} q_1^{\beta_1 - 1} \cdots q_l^{\beta_l - 1} (q_1 - 1) \cdots (q_l - 1)$$

and the rest of the proof is elementary. ■

**Lemma 3.5** *Let  $V \cup \{k\}$  be a set of positive integers such that  $k = [\mathbb{Q}_v : \cap_{v \in V} \mathbb{Q}_v]$ , for every  $v \in V$  and let  $d = \gcd(V)$ .*

1.  $k = 1$  if and only if  $|V| = 1$  or  $v$  is odd and  $V = \{d, 2d\}$ .
2. If  $k = p$  is prime then  $p = 2$ ,  $\gcd(6, d) = 1$  and  $V \subseteq \{3d, 4d, 6d\}$ .
3. If  $k = pq$  with  $q \leq p$  prime integers then  $q = 2$ ,  $2p + 1$  is prime  $2p + 1 \nmid d$  and one of the following conditions holds:
  - (a)  $2, p|d$ ,  $V \subseteq \{2pd, 3pd, (2p + 1)d\}$  and if  $3pd \in V$  then  $3 \nmid d$ .
  - (b)  $\gcd(2p, d) = p \neq 2$ ,  $V \subseteq \{4pd, 3pd, 6pd, (2p + 1)d, 2(2p + 1)d\}$  and if  $\{3pd, 6pd\} \cap V \neq \emptyset$  then  $3 \nmid d$ .
  - (c)  $p = 2$ ,  $\gcd(10, d) = 1$ ,  $V \subseteq \{8d, 12d, 5d, 10d\}$  and if  $12d \in V$  then  $3 \nmid d$ .

(d)  $p = 3$ ,  $\gcd(21, d) = 1$ ,  $V \subseteq \{9d, 18d, 7d, 14d\}$  and if  $V \cap \{18d, 14d\} \neq \emptyset \in V$  then  $2 \nmid d$ .

**Proof.** Note that  $\mathbb{Q}_d = \bigcap_{v \in V} \mathbb{Q}_v$ .

1 and the sufficient conditions in 2 and 3 are consequences of Lemma 3.4. We have to prove the necessary conditions of 2 and 3.

2. Assume that  $k = p$  is prime and let  $v_1, v_2 \in V$  such that  $\mathbb{Q}_{v_1} \neq \mathbb{Q}_{v_2}$ . Then  $\mathbb{Q}_d \subseteq \mathbb{Q}_{v_1} \cap \mathbb{Q}_{v_2} \neq \mathbb{Q}_{v_i}$  and hence  $\mathbb{Q}_d = \bigcap_{v \in V} \mathbb{Q}_v$ . By Lemma 3.4,  $p = 2$  and  $V \subseteq \{3d, 4d, 6d\}$  with  $\gcd(6, d) = 1$ .

3. Assume now that  $k = pq$  with  $q \leq p$ . We claim that there are  $v_1, v_2 \in V$  such that  $[\mathbb{Q}_{v_i}, \mathbb{Q}_{v_1} \cap \mathbb{Q}_{v_2}] = pq$  for  $i = 1, 2$ . Otherwise for every  $v_1, v_2 \in V$  such that  $\mathbb{Q}_{v_1} \neq \mathbb{Q}_{v_2}$ ,  $[\mathbb{Q}_{v_i} : \mathbb{Q}_{v_1} \cap \mathbb{Q}_{v_2}]$  is either  $p$  or  $q$ , which by case 2, should be 2. Thus  $q = 2$ ,  $\mathbb{Q}_{v_1} \cap \mathbb{Q}_{v_2} = \mathbb{Q}_d$  with  $\gcd(6, d) = 1$  and one can assume that  $v_1 = 4d$  and  $v_2 \in \{3d, 6d\}$ . Then there is  $v_3 \in V \setminus \{4d, 3d, 6d\}$  and then  $[\mathbb{Q}_v : \mathbb{Q}_{v_1} \cap \mathbb{Q}_{v_2} \cap \mathbb{Q}_{v_3}] = 2p$  for every  $v \in V$ . By assumption  $[\mathbb{Q}_{v_1} : \mathbb{Q}_{v_1} \cap \mathbb{Q}_{v_3}] \neq 2p$  and hence, using 2, we deduce that  $[\mathbb{Q}_{v_1} : \mathbb{Q}_{v_1} \cap \mathbb{Q}_{v_3}] = 2$ ,  $\mathbb{Q}_{v_1} \cap \mathbb{Q}_{v_2} = \mathbb{Q}_{d'}$  with  $\gcd(6, d') = 1$  and  $v_1, v_3 \in \{4d', 3d', 6d'\}$ . Thus  $d' = d$  and this leads to a contradiction.

So let  $v_1, v_2 \in V$  be such that  $[\mathbb{Q}_{v_i}, \mathbb{Q}_{v_1} \cap \mathbb{Q}_{v_2}] = pq$ . Thus  $\mathbb{Q}_{v_1} \cap \mathbb{Q}_{v_2} = \mathbb{Q}_d$  and the pairs  $(v_1, d)$  and  $(v_2, d)$  satisfy one of the conditions (a), (b) or (c) of Lemma 3.4. This leads to a very big list of cases that can be reduced having in mind that  $\gcd(v_1/d, v_2/d) = 1$ . Obviously  $\{v_1, v_2\} \neq \{pqr, 2pqr\}$  and therefore  $q = 2$  and one of the following cases holds:

(a)  $\{v_1, v_2\} = \{2pd, (2p+1)d\}$  with  $2, p \mid d$ .

(b)  $\{v_1, v_2\} = \{4pd, (2p+1)d\}$  with  $\gcd(2p, d) = p \neq 2$ ; or  $\{v_1, v_2\} = \{3pd, (2p+1)d\}$  with  $\gcd(3p, d) = p \neq 3$ ; or  $\{v_1, v_2\} = \{3pd, 2(2p+1)d\}$  with  $\gcd(6p, d) = p \neq 2, 3$ ; or  $\{v_1, v_2\} = \{6pd, (2p+1)d\}$  with  $\gcd(6p, d) = p \neq 2, 3$ .

(c)  $\{v_1, v_2\} = \{8d, 5d\}$  with  $p = 2 \nmid d$ ; or  $\{v_1, v_2\} = \{12d, 5d\}$  with  $p = 2$  and  $\gcd(6, d) = 1$ .

(d)  $\{v_1, v_2\} = \{9d, 7d\}$  with  $p = 3 \nmid d$ ; or  $\{v_1, v_2\} = \{9d, 14d\}$  with  $p = 3$  and  $\gcd(6, d) = 1$ ; or  $\{v_1, v_2\} = \{18d, 7d\}$  with  $p = 3$  and  $\gcd(6, d) = 1$ .

If  $v \in V$  then  $[\mathbb{Q}_v, \mathbb{Q}_{v_i} \cap \mathbb{Q}_v]$  is divisor of  $2p$  and using all the previous information one easily obtains the desired conclusion. ■

Now we are ready for the

**Proof of Theorem 3.2.** Let  $C$  be a  $\sim$ -class of  $\mathcal{A}_{pq}$  with at least two elements, let  $V = \overline{C}$ ,  $d = \gcd(V)$  and write  $S_v = S_{v,0,1}$  for every  $v \in V$ .

We claim that the centre  $K_v = \{x \in \mathbb{Q}_v : \sigma_r(x) = x\}$  of  $S_v$  is the same for every  $v \in V$ . If  $v_1, v_2 \in C$  then there is a field isomorphism  $f : K_{v_1} \rightarrow K_{v_2}$ . Since  $\mathbb{Q}_{v_1}/\mathbb{Q}$  is a Galois extension,  $f$  extends to an automorphism of  $\mathbb{Q}_{v_1}$ . Thus  $K_2 \subseteq \mathbb{Q}_{v_1}$  and this implies that  $K_2 \subseteq K_1$ . By symmetry  $K_1 \subseteq K_2$ .

Let  $K$  be the common centre of all the  $S_v$  with  $v \in V$ . Then  $K$  is a subfield of index  $pq$  in  $\mathbb{Q}_v$  for every  $v \in C$  and  $k = [\mathbb{Q}_v : \bigcap_{u \in V} \mathbb{Q}_u] = \frac{pq}{[\bigcap_{u \in V} \mathbb{Q}_u : K]}$  is independent of  $v$ . If  $k = 1$  then by Lemma 3.5,  $V = \{d, 2d\}$  for some odd integer  $d$ .

In the remainder of the proof we are going to use several times Lemma 3.5 without specific mention and the following argument: If  $v_1, v_2 \in C$  and  $v = \gcd(v_1, v_2)$  then  $\xi_{v_1}^s, \xi_{v_2}^s \in K \subseteq \mathbb{Q}_{v_1} \cap \mathbb{Q}_{v_2} = \mathbb{Q}_v$  and hence  $\frac{v_1 v_2}{v} \mid 2s$ . Moreover if  $v$  is even, then the same argument shows that  $\frac{v_1 v_2}{v} \mid s$ .

Assume that  $k \neq 1$ . Then  $q = 2$  and hence  $k = 2$  or  $k = 2p$ . If  $k = 2$  then  $\gcd(6, d) = 1$  and  $4d \in V \subseteq \{4d, 3d, 6d\}$ . Then  $6 \mid s$  (because either  $3d$  or  $6d$  belongs to  $V$ ) and from  $4d, 3d \mid s(r-1)$  one deduces that  $6d \mid \frac{s}{2}(r-1)$ . By Lemma 1.2, if  $3d \in V$  then  $\text{ind}(C) = \text{ind}(\mathcal{U}(3d, r, s)) \mid p$  and if  $6d \in V$  then  $\text{ind}(C) = \text{ind}(\mathcal{U}(6d, r, s)) \mid p$ .

Assume now that  $k = pq$ , and so  $K = K_d$ , so that  $d|r - 1$ . Then  $2p + 1$  is prime and one of the cases (a)-(d) of Lemma 3.5 holds. We consider the four cases separately.

(a) Since  $2pd, (2p + 1)d \in V$ , one has  $2p(2p + 1)|s$  (here we use that  $2|d$ ), and hence  $(2p + 1)d|\frac{s}{2p}(r - 1)$ . We conclude that  $\text{ind}(C) = 1$ .

(b) If  $\{3pd, 6pd\} \cap V = \emptyset$  then  $4pd, (2p + 1)d \in V$  and hence  $4p(2p + 1)|s$  and  $(2p + 1)d|\frac{s}{2p}(r - 1)$ , concluding that  $\text{ind}(C) = 1$ . Otherwise  $V \cap \{(2p + 1)d, 2(2p + 1)d\} \neq \emptyset$  and so  $3p(2p + 1)|s$  and  $(2p + 1)d|\frac{s}{p}(r - 1)$ . If  $(2p + 1)d \in V$  then  $\text{ind}(C) = \text{ind}(\mathcal{U}((2p + 1)d, r, s))|2$ . If  $2(2p + 1)d \in V$  then  $r$  is odd and therefore  $2(2p + 1)d|\frac{s}{p}(r - 1)$ . Then we conclude that  $\text{ind}(C) = \text{ind}(\mathcal{U}(2(2p + 1)d, r, s))|2$ .

(c) In this case  $p = 2$  and  $5d \in V$ . If  $8d \in V$  then  $20|s$  and  $5d|\frac{s}{4}(r - 1)$ , so that  $\text{ind}(C) = 1$ . If  $12d \in V$  then  $30|s$  and  $5d|\frac{s}{2}(r - 1)$  concluding that  $\text{ind}(C)|2$ .

(d) Similar arguments shows that  $3|s$  and  $v|\frac{s}{3}(r - 1)$  for some  $v \in V$ , concluding that  $\text{ind}(C)|2$ .

■

By Theorem 3.2 the equivalence classes of  $\mathcal{A}_{pq}/\sim$  of index  $pq$  have at most two elements and the classes with two elements are of the form  $\{v, 2v\}$  with  $v$  odd. In fact if  $G = G_{m,r,n,s}$  with  $m$  even and  $n$  and arbitrary odd integer then for every  $v|m$  such that  $v$  is odd and  $o_v = n$  then the  $\sim$ -class containing  $a = (v, 0, 1) \in \mathcal{A}_{m,r,n,s}$  contains at least two elements. Indeed,  $a' = (2v, 0, 1) \in \mathcal{A}_{m,r,n,s}$  and using Theorem 2.1 and Corollary 1.6 it is easy to see that  $S_a \simeq \mathcal{U}(v, r, s) \simeq \mathcal{U}(2v, r, s) \simeq S_{a'}$ . This contrast with [6, Corollary 3.1] which states that if  $n = p$  is prime then every non commutative division ring appears at most once in the Wedderburn decomposition of  $\mathbb{Q}G$ . The following example contradicts this statement: Let  $G = G_{m,r,p,s}$  with  $m$  odd and  $o_m(r) = p$  odd prime and assume that  $G$  can be embedded in the group of units of a division ring. It is easy to construct such a group by using Theorem 1.5 (see Example 3.11). Then  $\mathbb{Q}G$  has a simple component that is a division ring  $D \simeq \mathcal{U}(m, r, s)$ . If  $C_2$  denotes the cyclic group of order 2, then  $G_1 = G \times C_2 \simeq G_{2m,r_1,p,2s}$  where  $r_1$  is odd and  $r_1 \equiv r \pmod{m}$ . Moreover  $\mathbb{Q}G$  has two simple components isomorphic to  $D$ , because  $\mathbb{Q}G_1 \simeq (\mathbb{Q}G)^2$ . The error in the proof of [6, Corollary 3.1] relies in an error in the proof of [6, Theorem 3] based in deducing that  $\xi_{2d}^s = \xi_d^s \xi_{2d}^{-s}$  is a norm from the existence of an isomorphism  $(\mathbb{Q}_d, \sigma, \xi_{2d}^s) \simeq (\mathbb{Q}_{2d}, \sigma, \xi_d^s)$ . This is correct if the isomorphism is an isomorphism of simple algebras but it is not if it is just a ring isomorphism (see Lemma 1.1). In fact [6, Corollary 3.1] is quite close to be true, namely a non commutative division ring appears at most twice in the Wedderburn decomposition of  $\mathbb{Q}G_{m,r,p,s}$ . This is a direct consequence of the following Theorem that can be easily proven using Theorem 2.1 and the subsequent Lemma 3.9.

**Theorem 3.6** *Let  $G = G_{m,r,p,s}$  be a metacyclic group with  $p$  prime. There is a one to one correspondence  $v \mapsto S_v = S_{v,0,1} \simeq \mathcal{U}(v, r, s)$  from  $X = \{v|m : v \nmid r - 1\}$  to the set of noncommutative simple components of the Wedderburn decomposition of  $\mathbb{Q}G$ . If  $v_1, v_2 \in X$  then  $S_{v_1} \simeq S_{v_2}$  if and only if  $\text{ind}(S_{v_1}) = \text{ind}(S_{v_2})$  and one of the following conditions holds:*

1.  $v_1 = v_2$ .
2.  $\{v_1, v_2\} = \{d, 2d\}$  with  $2 \nmid d$ .
3.  $\text{ind}(S_{v_1}) = 1$ ,  $p = 2$  and either  $\{v_1, v_2\} = \{4d, 3d\}$  or  $\{v_1, v_2\} = \{4d, 6d\}$ .

### 3.3 $\mathcal{A}_p/\sim$

In the remainder of the paper we study  $\mathcal{A}_p/\sim$ . It is clear that the index of every  $C \in \mathcal{A}_p/\sim$  is either 1 or  $p$  and therefore for every  $a \in \mathcal{A}_p$ ,  $S_a$  is either a split algebra or a division ring. The goal

is obtaining a characterization of when two elements  $a_1, a_2 \in \mathcal{A}_p$  are  $\sim$ -equivalent. By Subsection 3.1,  $\{\mathcal{A}_p^{11}, \mathcal{A}_p^{1p}, \mathcal{A}_p^{11}, \mathcal{A}_p^{1q}\}$  is a partition of  $\mathcal{A}_p$  where

$$\begin{aligned}\mathcal{A}_p^{1k} &= \{a = (v, j, t) \in \mathcal{A}_p : q|v \text{ and } o_{v,i(a)} = k\} \\ \mathcal{A}_p^{\dagger k} &= \{a = (v, j, t) \in \mathcal{A}_p : q \nmid v \text{ and } t = k\}\end{aligned}$$

In order to state the main result of this section we establish the following ordering

$$\mathcal{A}_p^{1p} < \mathcal{A}_p^{11} < \mathcal{A}_p^{\dagger 1} < \mathcal{A}_p^{\dagger q}.$$

**Theorem 3.7** *Let  $X_1 \leq X_2$  be two elements of  $\{\mathcal{A}_p^{11}, \mathcal{A}_p^{1p}, \mathcal{A}_p^{\dagger 1}, \mathcal{A}_p^{\dagger q}\}$  and let  $a_1 = (v_1, j_1, t_1) \in X_1$  and  $a_2 = (v_2, j_2, t_2) \in X_2$ . Then  $a_1 \sim a_2$  if and only if  $\text{ind}(S_{a_1}) = \text{ind}(S_{a_2})$  and one of the following conditions holds:*

1.  $X_1 = X_2$  and one of the following conditions holds:
  - (a)  $v_1 = v_2$ .
  - (b)  $\{v_1, v_2\} = \{d, 2d\}$  for  $d$  an odd integer.
  - (c)  $p = 2$ ,  $X_1 \neq \mathcal{A}_p^{1p}$ ,  $\text{ind}(S_{a_1}) = 1$  and  $\{v_1, v_2\} \subseteq \{3d, 4d, 6d\}$  for  $d$  an integer such that  $\text{gcd}(d, 6) = 1$  and  $\mathbb{Q}_d \simeq Z(S_{a_1}) \simeq Z(S_{a_2})$ .
2.  $p = 2$ ,  $X_1 = \mathcal{A}_p^{1p}$ ,  $X_2 = \mathcal{A}_p^{\dagger q}$ ,  $\text{ind}(S_{a_1}) = 1$ ,  $v_1 | (r-1)q$  and one of the following conditions holds:
  - (a)  $qv_2 = 3v_1$  and  $\text{gcd}(3, v_1) = 1$ .
  - (b)  $qv_2 = 4v_1$  and  $\text{gcd}(2, v_1) = 1$ .
  - (c)  $qv_2 = 6v_1$  and  $\text{gcd}(6, v_1) = 1$ .
  - (d)  $2qv_2 = 3v_1$  and  $\text{gcd}(12, v_1) = 2$ .
3.  $X_1 = \mathcal{A}_p^{\dagger 1}$ ,  $X_2 = \mathcal{A}_p^{\dagger q}$ ,  $q|r-1$  and one of the following conditions holds:
  - (a)  $q = 2$  and  $v_1 = v_2$ .
  - (b)  $p = 2$ ,  $q = 3$ ,  $\text{ind}(S_{a_1}) = 1$  and there is  $d|r-1$  such that  $\text{gcd}(6, d) = 1$ ,  $v_1 = 4d$  and either  $v_2 = d$  or  $v_2 = 2d$ .
4.  $X_1 = \mathcal{A}_p^{11}$  and  $X_2 = \mathcal{A}_p^{\dagger 1}$  or  $X_2 = \mathcal{A}_p^{\dagger q}$ ,  $p = q = 2 \nmid s$ ,  $\text{ind}(S_{a_1}) = 1$  and there is  $d|r-1$  such that  $\text{gcd}(6, d) = 1$ ,  $v_1 = 2d$  and  $v_2 = 3d$ .
5.  $q|s$ ,  $X_1 = \mathcal{A}_p^{11}$ ,  $X_2 = \mathcal{A}_p^{\dagger 1}$  and one of the following conditions holds:
  - (a)  $q = 2$  and  $v_1 = 2v_2$ .
  - (b)  $\text{ind}(S_{a_1}) = 1$ ,  $p = 2$  and there is  $d|r-1$  such that either  $q = 2$ ,  $v_1 = 4d$  and  $v_2 = 3d$  or  $q = 3$ ,  $v_1 = 3d$  and  $v_2 = 2d$ .
6.  $q|s, r-1$ ,  $X_1 = \mathcal{A}_p^{11}$ ,  $X_2 = \mathcal{A}_p^{\dagger q}$  and one of the following conditions holds:
  - (a)  $v_1 = qv_2$ .
  - (b)  $q \neq 2$ ,  $\{v_1, qv_2\} = \{d, 2d\}$  for some  $2 \nmid d$  and either  $\text{ind}(S_{a_1}) = 1$  or  $p \neq 2$ .

(c)  $\text{ind}(S_{a_1}) = 1$ ,  $p = 2$  and there is  $d|r - 1$  such that  $\text{gcd}(6, d) = 1$  and either  $\{v_1, qv_2\} = \{4d, 3d\}$  or  $\{v_1, qv_2\} = \{4d, 6d\}$ .

We start with a description of  $S_a$  for every  $a \in \mathcal{A}_p$ . By the election of  $i_v$  made in (3.6), for every  $a = (v, j, t) \in \mathcal{A}_p$  we have

$$i(a) = i_v t + v'_v j = \begin{cases} \frac{vj-s}{q}, & \text{if } q|v \text{ and } q|s \\ -s, & \text{if } q|v \text{ and } q \nmid s \\ -syt & \text{if } q \nmid v \end{cases}$$

We denote by  $m'$  the greatest divisor of  $m$  which is not multiple of  $q$ . We are going to fix integers  $x$  and  $y$  such that

$$xm' + yq = 1.$$

**Lemma 3.8** *Let  $a = (v, j, t) \in \mathcal{A}_p$  and  $s_1 = s/q^k$  with  $k \geq 0$  and  $q^k|s$ .*

1. *If  $q \nmid s$ ,  $cq \equiv 1 \pmod{s}$  and  $a \in \mathcal{A}_p^{\uparrow 1}$  then  $S_a \simeq \mathcal{U}(vq, 1 + (r-1)cq, s)$ .*
2. *If  $q|s$  and  $a \in \mathcal{A}_p^{\uparrow 1}$  then  $S_a \simeq \mathcal{U}(v, r, \frac{s-jv}{q})$ .*
3. *If  $a \in \mathcal{A}_p^{\uparrow p}$  then  $S_a \simeq M_p(\mathbb{Q}_v)$ .*
4. *If  $a \in \mathcal{A}_p^{\uparrow 1}$  then  $S_a \simeq \mathcal{U}(v, r, sy) \simeq \mathcal{U}(v, r, s_1)$ .*
5. *If  $a \in \mathcal{A}_p^{\uparrow q}$  then  $S_a \simeq \mathcal{U}(vq, 1 + (r-1)yq, 1 + (s-1)yq) \simeq \mathcal{U}(vq, 1 + (r-1)yq, 1 + (s_1-1)yq)$ .*

**Proof.** We are going to use Theorem 2.1 and the notation established in it without specific reference.

If  $a \in \mathcal{A}_p^{\uparrow p}$  then  $o_{v,i} = p$  and  $c_v t = 1$ . Then  $v|r^p - 1 = r^{o_{v,i}} - 1$  and so  $S_a \simeq M_p(\mathbb{Q}_v)$ .

If  $q \nmid s$ ,  $cq \equiv 1 \pmod{s}$  and  $a \in \mathcal{A}_p^{\uparrow 1}$  then  $c_v t = q$  and  $i = -s$ . Let  $c_1 = c$  and  $i_1$  be integers such that  $c_1 q = 1 + i_1 s$  and set  $v_1 = 0$  and  $i' = -s$ . Then  $c_1, i_1, v_1$  and  $i'$  satisfy the conditions of (2.3) and hence  $\mathbb{Q}e_a = \mathcal{U}(vq, 1 + (r-1)cq, s)$ .

Assume now that  $q|s$  and  $a \in \mathcal{A}_p^{\uparrow 1}$ . In this case  $c_v t = 1$  and therefore  $v_1 = i_1 = i' = 0$  and  $c_1 = 1$  satisfy the conditions of (2.3). Thus  $S_a \simeq \mathcal{U}(v, r, -i(a)) = \mathcal{U}(v, r, \frac{s-jv}{q})$ .

If  $q \nmid v$  then  $v|m'$ ,  $i = -syt$  and  $c_v t = q$ . Thus the conditions of (2.3) are satisfied setting  $v_1 = (1+i)x\frac{m'}{v}$ ,  $c_1 = (1+i)y$  and  $i_1 = i' = 1$ . Moreover  $1 + c_1 c_v t(r-1) = 1 + (1-syq)yq(r-1) \equiv 1 + yq(r-1) \pmod{vq}$  and  $i'v_1v - i = (1-syq)xm' + syt \pmod{vq}$ .

If  $a \in \mathcal{A}_p^{\uparrow 1}$  then  $t = 1$  and  $1 + c_1 c_v t(r-1) \equiv 1 + yq(r-1) \equiv r \pmod{v}$  and  $i'c_v t - i \equiv (1-syq)xm' + sy \equiv sy \pmod{v}$ . Thus  $S_a \simeq \mathcal{U}(v, r, sy)$ . Moreover, since  $\text{gcd}(q, v) = 1$ ,  $S_a \simeq \mathcal{U}(v, r, syq) \simeq \mathcal{U}(v, r, s) \simeq \mathcal{U}(v, r, s_1)$ , by Lemma 1.1.

If  $a \in \mathcal{A}_p^{\uparrow q}$  then  $t = q$  and therefore  $i'v_1v - i = (1-syq)xm' + syq \equiv xm' + syq = 1 + (s-1)yq \pmod{vq}$ . Thus  $S_a \simeq \mathcal{U}(vq, 1 + (r-1)yq, 1 + (s-1)yq)$ . Finally assume that  $q^k|s$  and let  $l = xm' + y^{k+1}q$ . Then  $\text{gcd}(qv, l) = 1$  and applying Lemma 1.1 we obtain  $S_a \simeq \mathcal{U}(qv, 1 + (r-1)yq, 1 + (s-1)yq) \simeq \mathcal{U}(qv, 1 + (r-1)yq, l(1 + (s-1)yq)) = \mathcal{U}(qv, 1 + (r-1)yq, 1 + (s_1-1)yq)$ , because  $l(1 + (s-1)yq) \equiv y^{k+1}qs = (yq)^{k+1}s_1 \equiv s_1 \equiv 1 + (s_1-1)yq \pmod{v}$  and  $l(1 + (s-1)yq) \equiv xm' \equiv 1 \equiv 1 + (s_1-1)yq \pmod{q}$ . ■

The order of a complex root of unity is its order as an element of the multiplicative group  $\mathbb{C}^*$ . It is not difficult to prove, using Lemma 1.1, that if  $\xi_v^{s_1}$  and  $\xi_v^{s_2}$  have the same order then  $\mathcal{U}(v, r, s_1) \simeq \mathcal{U}(v, r, s_2)$ .

**Lemma 3.9** *Let  $A_1 = \mathcal{U}(m_1, r_1, s_1)$  and  $A_2 = \mathcal{U}(m_2, r_2, s_2)$  be cyclic algebras of degree  $p$  and assume that  $m_1 \leq m_2$ .*

1. *If  $A_1 \simeq A_2$  then one of the following conditions holds.*

(a)  $m_1 = m_2$ .

(b)  $m_1$  is odd and  $m_2 = 2m_1$ .

(c)  $p = 2$  and there is an integer  $d$  such that  $\gcd(6, d) = 1$ ,  $r_1 \equiv r_2 \equiv 1 \pmod{d}$  and either  $\{m_1, m_2\} = \{3d, 4d\}$  or  $\{m_1, m_2\} = \{4d, 6d\}$ . Moreover in this case  $\text{ind}(A_1) = 1$ .

2. *Assume that  $r_1 = r_2$ ,  $\xi_{m_1}^{ps_1}$  and  $\xi_{m_2}^{ps_2}$  have the same order, and either  $m_1 = m_2$  or  $m_1$  and  $p$  are odd and  $m_2 = 2m_1$  then  $A_1 \simeq A_2$  if one of the following conditions holds:*

(a)  $\text{ind}(A_1) = \text{ind}(A_2)$ .

(b)  $s_1 = s_2$ .

**Proof.** 1. Let  $K_i$  be the centre of  $A_i$  ( $i = 1, 2$ ). If  $f : A_1 \rightarrow A_2$  is an isomorphism then  $f$  induces an isomorphism  $f : K_1 \rightarrow K_2$ . Since  $\mathbb{Q}_{m_1}/\mathbb{Q}$  is a Galois extension  $f$  extends to an automorphism of  $\mathbb{Q}_{m_1}$ . Thus  $K_2 \subseteq \mathbb{Q}_{m_1} \cap \mathbb{Q}_{m_2}$  and  $[\mathbb{Q}_{m_1} : K_2] = [\mathbb{Q}_{m_1} : K_1] = p = [\mathbb{Q}_{m_2} : K_2]$ . Similarly  $K_1$  is a common subfield of index  $p$  in  $\mathbb{Q}_{m_1}$  and  $\mathbb{Q}_{m_2}$ . Thus  $[\mathbb{Q}_{m_1} : \mathbb{Q}_{m_1} \cap \mathbb{Q}_{m_2}] = [\mathbb{Q}_{m_2} : \mathbb{Q}_{m_1} \cap \mathbb{Q}_{m_2}]$  and this number, denoted  $k$ , is either 1 or  $p$ . By Lemma 3.5, if  $k = 1$  then either  $m_1 = m_2$  or  $m_1$  is odd and  $m_2 = 2m_1$  and if  $k = p$  then  $p = 2$  and there is an integer  $d$  such that either  $\{m_1, m_2\} = \{3d, 4d\}$  or  $\{m_1, m_2\} = \{4d, 6d\}$ .

In the latter case  $\mathbb{Q}_{m_1} \cap \mathbb{Q}_{m_2} = \mathbb{Q}_d = K_1 = K_2$  and therefore  $r_i \equiv 1 \pmod{d}$ . If  $m_i = 4d$  then  $r_i \equiv -1 \pmod{4}$  and if  $m_i = 3d$  or  $6d$  then  $r_i \equiv -1 \pmod{3}$ . By changing  $r_1$  and  $r_2$  if needed one may assume that  $r_1 = r_2$ , denote  $r$  to this number, and hence  $r \equiv -1 \pmod{12}$ . By means of contradiction assume that  $A_1$  is a division ring, and hence so is  $A_2$ . By Corollary 1.6,  $m_1$  and  $m_2$  are even and therefore  $m_1 = 4d$  and  $m_2 = 6d$ . Since  $A_i$  is a division ring,  $\xi_{2d} = -\xi_d \notin N_{\mathbb{Q}_{m_i}/\mathbb{Q}_d}^*$ . However  $\xi_d = \xi_{2d}^2 \in N_{\mathbb{Q}_{m_i}/\mathbb{Q}_d}^*$ , and therefore  $-1 \notin N_{\mathbb{Q}_{m_i}/\mathbb{Q}_d}^*$ ,  $A_1 \simeq \mathcal{U}(4d, r, 2) \simeq \mathcal{U}(4d, r, 2d) = (\mathbb{Q}_{2d}, \sigma_r, -1)$  and  $A_2 \simeq \mathcal{U}(6d, r, 3) \simeq \mathcal{U}(6d, r, 3d) = (\mathbb{Q}_{6d}, r, -1)$ . On the other hand,  $A_2$  can be rewritten as  $(\mathbb{Q}_{6d}, \sigma_r, -1) = (\mathbb{Q}_{4d}, \sigma_r, -3)$ . Now we use statement 6 of Lemma 1.1. First notice that  $A_1$  and  $A_2$  are simple quotients of rational group algebras. Indeed,  $A_1$  is a simple quotient of  $\mathbb{Q}G_{4d, r, 2, 2}$  and  $A_2$  is a simple quotient of  $\mathbb{Q}G_{6d, r, 2, 3}$ . If  $f : A_1 \rightarrow A_2$  is an isomorphism then  $f(\xi_2) = f(-1) = -1 = \xi_2$ . Thus  $3 = (-3)(-1)^{-1} \in N_{\mathbb{Q}_{4d}/\mathbb{Q}_d}^*$ . We are going to see that this leads to a contradiction. Using Theorem 1.5 one deduces that  $o_d(2)$  and  $o_d(3)$  are odd. Let  $f = o_d(3)$ ,  $p$  a prime of  $\mathbb{Q}_d$  above 3 and  $q$  a prime of  $\mathbb{Q}_{4d}$  above  $p$ . It is well known that  $f$  is the residue class degree of  $p$  relative to the extension  $\mathbb{Q}_d/\mathbb{Q}$  [9]. Since  $f$  is odd, the residue class degree of  $q$  relative to the extension  $\mathbb{Q}_{4d}/\mathbb{Q}$  is  $2f$  and this shows that the completion  $F$  of  $\mathbb{Q}_d$  at  $p$  (resp. the completion  $E = F[i]$  of  $\mathbb{Q}_{4d}$  at  $q$ ) is the unique unramified extension of the completion of  $\mathbb{Q}$  at 3, of degree  $f$  (resp.  $2f$ ). Since the value of 3 at  $p$  is 1 and  $[E : F] = 2$ , one has that  $3 \notin N_{E/F}^*$  [14, Theorem 14.1] and so  $3 \notin N_{\mathbb{Q}_{4d}/\mathbb{Q}_d}^*$ , which is the contradiction searched.

2. Assume that the conditions of 2 holds. If  $s_1 = s_2$  then  $A_1 \simeq A_2$  by Corollary 1.6. Assume that  $\text{ind}(A_1) = \text{ind}(A_2)$ . If  $m_1$  is odd then  $\mathcal{U}(m_1, r, s_1) = \mathcal{U}(2m_1, r, 2s_1)$  and  $\xi_{2m_1}^{2s_1} = \xi_{m_1}^{s_1}$  have the same order. Therefore it is enough to prove the statement under the assumption that  $m_1 = m_2$ , denote this number by  $m$ . The centres of  $A_1$  and  $A_2$  are equal (call it  $K$ ) and hence the statement is obvious if  $A_1$  and  $A_2$  are split. So assume that  $A_1$  and  $A_2$  are division rings. By Lemma 1.1,  $a_i = \xi_m^{s_i} \notin N_{\mathbb{Q}_m/K}^*$ , while  $a_i^p \in N_{\mathbb{Q}_m/K}^*$ . By assumption  $\langle a_1^p \rangle = \langle a_2^p \rangle$  and therefore if the order of  $a_1^p$

is  $w$  then  $a_1$  and  $a_2$  have order  $pw$ . Thus there exists  $t$  coprime with  $pw$  such that  $a_2 = a_1^t$ . By the Chinese Remainder Theorem one may assume that  $\gcd(t, m)$  and so  $A_1 \simeq A_2$ , by Lemma 1.1. ■

Before proving Theorem 3.7 we need one more ingredient that is of interest in itself.

**Proposition 3.10** *Let  $v$  a divisor of  $m$  such that  $o_v = p$  and  $C = [v] \cap X$  with  $X \in \{\mathcal{A}_p^{[1]}, \mathcal{A}_p^{[p]}, \mathcal{A}_p^{[1]}, \mathcal{A}_p^{[q]}\}$ .*

1. *One of the following conditions holds:*

- (a) *All the elements of  $C$  are  $\sim$ -equivalent.*
- (b)  *$p = q$ ,  $q|r - 1$ ,  $1 \leq v_q(v) \leq v_q(s)$ ,  $X = \mathcal{A}_p^{[1]}$ ,  $C = [v]$  and is formed by exactly two  $\sim$ -classes  $C_1$  and  $C_2$ :  $C_1 = \{(v, k, 1)\}$  where  $s \equiv vk \pmod{q \gcd(s, v)}$ . Moreover  $S_a$  is split if  $a \in C_1$  and  $S_a$  is a division ring if  $a \in C_2$ .*

2. *Assume that  $q|s$ ,  $q|v$ ,  $m$  is even and  $v$  is odd.*

- (a) *if  $2 \neq p \neq q$  then all the elements of  $[v] \cap \mathcal{A}_p^{[1]}$  and  $[2v] \cap \mathcal{A}_p^{[1]}$  are  $\sim$ -equivalent.*
- (b) *If  $p = q$  then there is a bijection  $f : [2v] \cap \mathcal{A}_p^{[1]} \rightarrow [v] \cap \mathcal{A}_p^{[1]}$  such that  $a \sim f(a)$  for every  $a \in [2v]$ .*

**Proof.** 1. Assume that  $C/\sim$  has at least two elements. By Proposition 3.1 and Lemma 3.8,  $X = \mathcal{A}_p^{[1]}$ ,  $q|s$ ,  $q|v$  and  $q|r - 1$  and therefore  $C = [v]$ . If  $p \neq q$  and  $a = (v, j, t) \in C$  then using Lemma 1.1 one obtains  $S_a \simeq \mathcal{U}(v, r, s_j = \frac{s-vj}{q}) \simeq \mathcal{U}(v, r^q, s)$ , that is all the elements of  $C$  are  $\sim$ -equivalent, a contradiction. Thus  $p = q$  and the degree of  $S_a$  is  $p = q$  and  $\xi_v^{s_j p} = \xi_v^s$ , does not depend on  $j$ . By Lemma 3.9, the cardinality of  $[v]/\sim$  is at most two (and so it is exactly two) and  $[v]/\sim$  is formed by a class of split algebras and another of (isomorphic) division rings.

Let  $0 \leq j < p$  such that  $S_{v, j, 1} \simeq \mathcal{U}(v, r, \frac{s-vj}{p})$  is not split. Since  $\xi_v^s = \left( \xi_v^{\frac{s-vj}{p}} \right)^p = N_{\mathbb{Q}_v/K}(\xi_v^{\frac{s-vj}{p}})$ ,

where  $K$  denotes the centre of  $S_{v, j, 1}$ , if  $w$  is the order of  $\xi_v^s$  then the order of  $\xi_v^{\frac{s-vj}{p}}$  is  $pw$ . Therefore  $\langle \xi_{pw} \rangle \cap N_{\mathbb{Q}_v/K}^* = \langle \xi_w \rangle$ , because  $[\langle \xi_w \rangle : \langle \xi_{pw} \rangle] = p$ . Hence, if  $d = \gcd(v, s)$  then  $S_{v, k, 1}$  is split if and only if  $\left( \xi_v^{\frac{s-vk}{p}} \right)^w = 1$  if and only if  $v | \frac{s-vk}{p} \frac{v}{d}$  if and only if  $s \equiv vk \pmod{pd}$ , if and only if  $\frac{s}{d} \equiv \frac{v}{d} k \pmod{q}$ . Since  $[v]/\sim$  has two elements then  $\frac{v}{d}$  is not a multiple of  $q$ , that is  $v_q(v) \leq v_q(s)$ , and therefore there is exactly one  $k \in \mathbb{Z}_q$  for which  $S_{v, k, 1}$  is split.

2. Assume that the conditions of 2 holds. Since  $v$  is odd then  $q \neq 2$  and hence  $v_q(v) = v_q(2v)$ . By Proposition 3.1,  $[v] \cap \mathcal{A}_p^{[1]}$  and  $[2v] \cap \mathcal{A}_p^{[1]}$  have the same cardinality ( $q$ , if  $q|r - 1$  and  $v_q(v) < v_q((r - 1)s)$ , 0 if  $q|r - 1$  and 1 if  $v_q(v) < v_q((r - 1)s)$ ). Moreover, if  $a_1 = (v, j_1, 1) \in [v] \cap \mathcal{A}_p^{[1]}$  and  $a_2 = (2v, j_2, 1) \in [2v] \cap \mathcal{A}_p^{[1]}$  then  $S_{a_1} \simeq \mathcal{U}(v, r, \frac{s-vj_1}{q})$  and  $S_{a_2} \simeq \mathcal{U}(v, r, \frac{s-2vj_2}{q})$ .

(a) If  $2 \neq p \neq q$  then  $S_{2v, j_1, 1} \simeq \mathcal{U}(2v, r^q, s) \simeq \mathcal{U}(v, r^q, s) \simeq S_{v, j_2, 1}$ , for every  $0 \leq j_1 < q$ , by Corollary 1.6.

(b) If  $p = q$  then the map  $f : [2v] \rightarrow [v]$  given by  $f(2v, j, 1) = (v, j_1, 1)$  where  $j_1$  is the remainder of  $2j$  module  $q$  satisfies statement (ii) by Corollary 1.6. ■

**Proof of Theorem 3.7.** Write  $S_i = S_{a_i}$ . If  $a_1 \sim a_2$  then  $\text{ind}(S_1) = \text{ind}(S_2)$ . So in the remainder of the proof we assume  $\text{ind}(S_1) = \text{ind}(S_2) = i$ .

We first show that  $a_1 \sim a_2$  if one of the cases 1-6 holds. Notice that if  $i = 1$  then to prove  $a_1 \sim a_2$  it is enough to show that the centres of  $S_1$  and  $S_2$  are isomorphic.

In case 1(a),  $S_1 \simeq S_2$  is a consequence of Proposition 3.10.

In case 1(b),  $q \neq 2$  because if  $X_1 = \mathcal{A}_p^{11}$  or  $\mathcal{A}_p^{1p}$  then  $q|d$  and otherwise  $q \nmid 2d$ . Thus  $qd$  is odd and if  $v_1 = d$  then by using Lemma 3.8 one has that  $S_1 \simeq \mathcal{U}(m_1, r_1, s_1)$  and  $S_2 = \mathcal{U}(2m_1, r_1, s_1) \simeq S_1$  with  $m_1$  odd. Thus  $Z(S_1) \simeq Z(S_2)$  and hence one may assume that  $i = p$ . Then  $p$  is odd and  $S_1 \simeq S_2$  by Corollary 1.6.

In case 1(c) the centres of  $S_1$  and  $S_2$  are isomorphic to  $\mathbb{Q}_d$ .

2. In this case  $Z(S_1) = \mathbb{Q}_{v_1}$  and  $\mathbb{Q}_{v_1} \subseteq Z(S_2) \subseteq \mathbb{Q}_{qv_2}$  by Lemma 3.8 and the hypothesis  $v_1|(r-1)yg$ . Moreover the hypothesis (a)-(d) imply that  $[\mathbb{Q}_{qv_2} : \mathbb{Q}_{v_1}] = 2 = p = [\mathbb{Q}_{qv_2} : Z(S_2)]$  and hence  $Z(S_2) = \mathbb{Q}_{v_1}$ .

3. Let  $s_1 = s/q^{v_q(s)}$ . By Lemma 3.8,  $S_1 \simeq \mathcal{U}(v_1, r, s_1)$  and  $S_2 \simeq \mathcal{U}(qv_1, 1 + (r-1)qy, 1 + (s_1 - 1)qy) \simeq \mathcal{U}(qv_1, r, 1 + (s_1 - 1)qy)$ , where the last isomorphism is a consequence of  $v|m'|qy - 1$  and the hypothesis  $q|r - 1$ . In case (b),  $Z(S_1) \simeq \mathbb{Q}_d \simeq Z(S_2)$ . To prove that  $S_1 \simeq S_2$  in case (a) notice that  $1 + (s_1 - 1)qy = 1 + 2(s_1 - 1)y \equiv s_1 \pmod{2v_1}$  because  $v_1|m'|2y - 1$  and  $s_1$  is odd.

4. By Lemma 3.8 in this case  $S_1 \simeq \mathcal{U}(4d, r, s)$ ,  $S_2 \simeq \mathcal{U}(3d, r, s)$  if  $X_2 = \mathcal{A}_p^{11}$  and  $S_2 \simeq \mathcal{U}(6d, 1 + 2(r-1)y, 1 + 2(s-1)y)$  if  $X_2 = \mathcal{A}_p^{1q}$ . Since  $2|v_1|m$  then  $r$  is odd and hence  $1 + (r-1)qy \equiv r \pmod{6d}$ . Thus  $S_1$  and  $S_2$  have the same centre (namely  $\mathbb{Q}_d$ ) and so they are isomorphic.

5(a). In this case  $v_2$  is odd,  $S_1 \simeq \mathcal{U}(v_1, r, \frac{s-jv_1}{2})$  and  $S_2 \simeq \mathcal{U}(2v_2 = v_1, r, s/2)$  by Lemma 3.8. Thus  $Z(S_1) \simeq Z(S_2)$  and so one may assume that  $i = p$ . Thus implies that  $p$  is odd, by Corollary 1.6, and applying Lemma 1.1(1) with  $k = 2$  one obtains  $S_1 \simeq \mathcal{U}(v_1, r^2, s) \simeq S_2$ .

5(b). In this case it is easy to prove that  $Z(S_1) \simeq \mathbb{Q}_d \simeq Z(S_2)$ .

6. In this case  $S_1 \simeq \mathcal{U}(v_1, r, \frac{s-jv_1}{q})$ . Since  $q|s, r-1$  then  $S_2 \simeq \mathcal{U}(qv_2, 1 + (r-1)qy, 1 + (s-1)qy) \simeq \mathcal{U}(qv_2, r, 1 + (s-1)qy)$ . This implies that  $Z(S_1) \simeq Z(S_2)$ . Thus one may assume that  $i = p$  and so either  $v_1 = qv_2$  or  $p, q \neq 2$  and  $\{v_1, qv_2\} = \{d, 2d\}$  for some integer  $d$ . We claim that if  $v|m$  with  $v_q(v) = 1$  and  $\text{ind}(T_1) = \text{ind}(T_2) = p$  for  $T_1 = \mathcal{U}(v, r, \frac{s-jv}{q})$  and  $T_2 = \mathcal{U}(v, r, 1 + (\frac{s}{q} - 1)qy)$  then  $T_1 \simeq T_2$ . To prove the claim first notice that  $\frac{v}{q}|m'|qy - 1$  and hence  $q(1 - (\frac{s}{q} - 1)qy) \equiv s \pmod{v}$ . If  $p \neq q$  then applying Lemma 1.1(1) for  $k = q$  one obtains  $T_1 \simeq \mathcal{U}(v, r^q, s) \simeq T_2$ . Otherwise  $\xi_v^{\frac{s-jv}{q}} = \xi_v^s = \xi_v^{q(1 - (\frac{s}{q} - 1)qy)}$  and  $T_1 \simeq T_2$  by Lemma 3.9. The claim implies that  $S_1 \simeq S_2$  if  $v_1 = qv_2$ . In the second case  $S_1 \simeq S_2$  follows by applying the claim for  $v = d$  combined with the isomorphism  $\mathcal{U}(d, r, s) \simeq \mathcal{U}(2d, r, s)$  (Corollary 1.6).

Conversely assume that  $S_1 \simeq S_2$ . We have to prove that one of the conditions 1-6 holds.

If  $X_1 = X_2 = \mathcal{A}_p^{1p}$  then  $S_{a_1} \simeq M_2(\mathbb{Q}_{v_1})$  and  $S_{a_1} \simeq M_2(\mathbb{Q}_{v_1})$  (Lemma 3.8) and hence either condition 1(a) or 1(b) holds. If  $X_1 = X_2 \neq \mathcal{A}_p^{1p}$  then using Lemmas 3.8 and 3.9 one deduces that one of the conditions of 1 holds.

In the remainder of the proof we assume that  $X_1 \neq X_2$  and so  $X_2 \neq \mathcal{A}_p^{1p}$ . We write  $S_2 \simeq \mathcal{U}(n_2, r_2, s_2)$  with  $n_2, r_2$  and  $s_2$  taken as in the isomorphisms in Lemma 3.8.

Assume that  $X_1 = \mathcal{A}_p^{1p}$  and in particular  $q|s$  and  $q|v_1$ . Then the centre of  $S_2$  is isomorphic to  $\mathbb{Q}_{v_1}$  and therefore  $\mathbb{Q}_{v_1}$  is a subfield of index  $p$  of  $\mathbb{Q}_{n_2}$  and  $r_2 \equiv 1 \pmod{v_1}$ . Since  $o_{v_1} = p$ ,  $r \not\equiv 1 \pmod{v_1}$  and therefore  $X_2 = \mathcal{A}_p^{1q}$  which implies that  $r_2 = 1 + (r-1)qy$  and  $n_2 = qv_2$ . Thus  $v_1|(r-1)qy$ . Furthermore,  $\phi(n_2) = p\phi(v_1)$ ,  $v_1|2n_2$  and if  $n_2$  is even then  $v_1|n_2$ . By Lemma 3.4,  $p = 2$ . If  $n_2$  is even then  $\frac{n_2}{v_1}$  is either 3, 4 or 6 and  $\text{gcd}(v_1, n_2/v_1) = 1$  and if  $n_2$  is odd then  $\frac{2n_2}{v_1}$  is either 3, 4 or 6 and  $\text{gcd}(v_1, 2n_2/v_1) = 1$ . This implies that one of the conditions 2(a)-2(d) holds.

In the remainder of the proof we assume that  $X_1 \neq \mathcal{A}_p^{1p}$  and write  $S_1 \simeq \mathcal{U}(n_1, r_1, s_1)$  with  $n_1, r_1$  and  $s_1$  taken as in the isomorphisms in Lemma 3.8. Since  $X_1 < X_2 \leq \mathcal{A}_p^{1q}$  one can take  $r_1 = r$ . By Lemma 3.9, one of the following conditions holds:

(A)  $n_1 = n_2$ .

(B)  $\{n_1, n_2\} = \{d, 2d\}$  with  $d$  odd.

(C)  $i = 1$ ,  $p = 2$  and there exists an integer  $d$  such that  $\gcd(6, d) = 1$ ,  $r_i \equiv 1 \pmod{d}$  and either  $\{n_1, n_2\} = \{3d, 4d\}$  or  $\{n_1, n_2\} = \{4d, 6d\}$ .

We claim that if  $X_2 = \mathcal{A}_p^{\dagger q}$  then  $q|r - 1$ . Indeed, if  $f : S_1 \rightarrow S_2$  is an isomorphism then  $a = f^{-1}(\xi_{n_2}^{1+(s-1) yq})$  is a central root of unity of  $S_1$  and therefore  $a^r = a$ . Applying  $f$  to this equality one deduces that  $qv_2 = n_2|(r-1)(1+(s-1) yq)$  and hence  $q|r - 1$ .

Assume that  $X_1 = \mathcal{A}_p^{\dagger 1}$  and hence  $X_2 = \mathcal{A}_p^{\dagger q}$ . Then  $v_q(n_2) = 1$  and  $q \nmid n_1$  and in particular  $n_1 \neq n_2$ . If condition (B) holds then  $q = 2$ ,  $n_1 = v_1 = v_2 = d$  and  $n_2 = 2d$ . If condition (C) holds then  $q = 3$ ,  $v_1 = n_1 = 4d$  and  $n_2$  is either  $3d$  or  $6d$ . Thus one of the conditions of 3 holds.

In the remainder of the proof we assume that  $X_1 = \mathcal{A}_p^{\dagger 1}$  and hence  $X_2$  is either  $\mathcal{A}_p^{\dagger 1}$  or  $\mathcal{A}_p^{\dagger q}$ . Thus  $q|v_1$  and  $q \nmid v_2$ .

Assume first that  $q \nmid s$ . Then  $q^2|n_1 = qv_1$  and  $q^2 \nmid n_2$ . This is not compatible with either (A) or (B) and hence  $i = 1$ ,  $p = q = 2$  and there is an integer  $d$  satisfying the conditions of (C) such that  $n_1 = 2v_1 = 4d$  and  $n_2 = v_2 = 3d$  if  $X_2 = \mathcal{A}_p^{\dagger 1}$  and  $n_2 = 2v_2 = 6d$  if  $X_2 = \mathcal{A}_p^{\dagger p}$ . Thus  $v_1 = 2d$  and  $v_2 = 3d$  and so condition 4 holds.

It remains to consider the case  $q|s$ . Then  $n_1 = v_1$  and  $s_1 = \frac{s-v_1}{q}$ . Suppose that  $X_2 = \mathcal{A}_p^{\dagger 1}$ , so that  $n_2 = v_2$  and  $r_2 = r$  and  $s_2 = sy$ . Then  $q \nmid n_2$  and hence  $n_1 \neq n_2$ . If  $S_1 \simeq S_2$  and (B) holds then  $q = 2$  and  $v_1 = 2v_2$ . If (C) holds then  $p = 2$  and either  $q = 2$ ,  $v_1 = 4d$  and  $v_2 = 3d$  or  $q = 3$ ,  $v_1 = 3d$  and  $v_2 = 4d$ . Thus one of the conditions of 5 holds.

Finally assume that  $X_2 = \mathcal{A}_p^{\dagger q}$ , so that  $n_2 = qv_2$ ,  $r_2 = 1 + (r-1) yq$  and  $s_2 = 1 + (s-1) yq$ . We have seen above that  $q|r - 1$  and hence one may assume that  $r_2 = r$ . If (A) holds then  $v_1 = qv_2$ . If (B) holds then  $\{v_1, qv_2\} = \{d, 2d\}$  with  $d$  odd. This implies that  $q \neq 2$  and if  $i \neq 1$  then  $p \neq 2$ , by Corollary 1.6. If (C) holds then either  $\{v_1, qv_2\} = \{4d, 3d\}$  or  $\{v_1, qv_2\} = \{4d, 6d\}$ . So one of the conditions of 6 holds. ■

We finish with one example that shows how one can obtain finite metacyclic groups with different isomorphic components with prescribed properties.

**Example 3.11** If  $r = 6$ ,  $p = 5$ ,  $d = 5 \cdot 311 = \frac{r^p - 1}{p}$  and  $s = -311 = -\frac{d}{\gcd(r-1, d)}$  then  $D = \mathcal{U}(d, r, s)$  is a division algebra of degree  $p$  by Theorem 1.5 and  $\mathbb{Q}G_{2d, r, p, s}$  has two different simple components that are isomorphic to  $D$  (Theorem 3.6).

Let now  $D = \mathcal{U}(d, r, s)$  be an arbitrary cyclic division algebra of prime degree  $p$  and assume that  $\gcd(6, d) = 1$  (for example take  $d, r, s$  and  $p$  as in the previous paragraph). Since  $\gcd(6, d) = 1$  one has  $\mathcal{U}(d, r, s) \simeq \mathcal{U}(d, r^{12}, 12s)$  and therefore one may assume that  $12|s$ . By the Chinese Remainder Theorem there is an integer  $r_1$  such that  $r_1 \equiv r \pmod{d}$ ,  $r_1 \equiv -1 \pmod{12}$ . By changing  $r$  by  $r_1$  one may assume that  $r \equiv -1 \pmod{12}$ .

Let  $G = G_{12d, r, 2p, s}$  and  $\mathcal{A} = \mathcal{A}_{12d, r, 2p, s}$ . By the conditions above  $12|r^2 - 1$  and  $d|r^p - 1$ , while  $3 \nmid r - 1$ ,  $4 \nmid r - 1$  and  $d \nmid r - 1$ . Then  $a_1 = (3d, 0, 1)$ ,  $a_2 = (4d, 0, 1) \in \mathcal{A}_{2p}$  and  $a_1 \not\cong a_2$  by Theorem 2.1. Moreover  $A_1 = S_{a_1} \simeq \mathcal{U}(3d, r, s)$  and  $A_2 = S_{a_2} \simeq \mathcal{U}(4d, r, s)$ . We claim that  $M_2(D) \simeq S_{a_1} \simeq S_{a_2}$ , that is  $a_1 \not\cong a_2$ ,  $a_1 \sim a_2$  and  $S_{a_1}$  is neither a split algebra nor a division ring.

First notice that the degrees of the three algebras coincides. Indeed, the degree of  $M_2(D)$  is  $2p$  and the degrees of  $A_1$  and  $A_2$  are  $o_{3d}(r)$  and  $o_{4d}(r)$  respectively. Since  $\gcd(6, d) = 1$ ,  $o_{3d}(r) = \text{lcm}(o_3(r), o_d(r)) = 2p$ , because  $r \equiv -1 \pmod{3}$  and the degree of  $D$  is  $p$ . Similarly  $o_{4d}(r) = 2p$ . Let  $u$  be a unit of  $D$  such that  $D = \mathbb{Q}_d[u|\xi_d u = u\xi_d^r, u^p = \xi_d^s]$  and set

$$x = \xi_d^2 \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \quad y = \xi_d^2 \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{and} \quad u_1 = u \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Notice that  $x$  is a  $3d$ -th root of unity and  $y$  is a  $4d$ -th root of unity. Thus  $\mathbb{Q}_{3d}$  and  $\mathbb{Q}_{4d}$  are strictly maximal subfields of  $M_2(D)$ . Then  $M_2(D) = \mathbb{Q}(x)[u_1] = \mathbb{Q}(y)[u_1]$  and it is easy to see that  $xu_1 = u_1x^r$ ,  $yu_1 = u_1y^r$  and  $u_1^{2p} = \xi_d^{2s} = x^s = y^s$ , because  $s$  is multiple of 12. This proves the claim.

## References

- [1] S.A. Amitsur, *Finite subgroups of division rings*, Trans. Amer. Math. Soc. **80** (1955), 361–386.
- [2] M. Benard and M.M. Schacher, The Schur subgroup II, J. Algebra 22 (1972), 378–385.
- [3] S. Coelho and C. Polcino Milies, The automorphism group of the group algebra of a dihedral group, Boll. Un. Mat. Ital. A(7) 9 (1955), n° 3, 541–548.
- [4] S. Coelho, E. Jespers and C. Polcino Milies, The automorphism group of the group algebra of certain metacyclic groups, Comm. Algebra 24 (1996) 4135–4145.
- [5] Ch.W. Curtis and I. Reiner, Representation theory of finite groups and associative algebras. Wiley-Interscience, New York, 1962.
- [6] A. Herman, On the automorphism groups of rational group algebras of metacyclic groups, Comm. Algebra 25 (1997) 2085–2097.
- [7] I.M. Isaacs, Character theory of finite groups, Academic Press, 1976.
- [8] G.J. Janusz, Automorphism group of simple algebras and group algebras. In "Representation Theory of Algebras. Philadelphia, 1976". Lecture Notes in Pure and Applied Mathematics, Vol 37, 381–388.
- [9] D.A. Marcus, Number fields, Springer 1977.
- [10] A. Olivieri and Á. del Río, An algorithm to compute the primitive central idempotents and the Wedderburn decomposition of a rational group algebra, J. Symbolic Comput., 35 (2003) 673–687.
- [11] 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.
- [12] D. Passman, Infinite Crossed Products, Academic Press, 1989.
- [13] R.S. Pierce, Associative Algebras, Springer-Verlag, 1982.
- [14] I. Reiner, Maximal orders, Academic Press 1975, reprinted by LMS 2003.
- [15] S.K. Sehgal, Units in integral group rings, Longman Scientific & Technical, Pitman Monographs, Surveys in Pure and Applied Mathematics 69, 1993.