

## COMPUTING THE WEDDERBURN DECOMPOSITION OF GROUP ALGEBRAS BY THE BRAUER–WITT THEOREM

GABRIELA OLTEANU

ABSTRACT. We present an alternative constructive proof of the Brauer–Witt theorem using the so-called strongly monomial characters that gives rise to an algorithm for computing the Wedderburn decomposition of semisimple group algebras of finite groups.

### 1. INTRODUCTION

The Wedderburn decomposition of a semisimple group algebra  $kG$  of a finite group  $G$  over a field  $k$ , that is, the decomposition of  $kG$  as a direct sum of simple algebras, is a helpful tool for studying several problems. For example, a good description of the Wedderburn decomposition of  $kG$  is useful for describing the automorphism group of  $kG$  [Her97], [Oli-Río-Sim06] or for studying the unit group of the integral group ring  $\mathbb{Z}G$  if  $k = \mathbb{Q}$  [Jes-Lea], [Jes-Río], [Río-Rui], [Rit-Seh], [Seh]. It also has applications in coding theory if  $k$  is a field of characteristic  $p > 0$  [Ple-Huf].

Recently in [Jes-Lea-Paq] a character-free method was given to compute the Wedderburn decomposition of  $\mathbb{Q}G$  for nilpotent groups, and this method was extended and simplified in [Oli-Río-Sim04] to groups including the abelian-by-supersolvable groups. The approach in [Oli-Río-Sim04] allowed the implementation of the package `wedderga` [Bro-Kon-Oli-Olt-Río] for the computer system GAP [GAP].

In this paper we present an algorithmic method to compute the Wedderburn decomposition of  $kG$  for  $G$  an arbitrary finite group and  $k$  an arbitrary field of characteristic 0 using the Brauer–Witt theorem. This algorithm also has been implemented for the computer system GAP, enlarging the functionality of the package `wedderga`, and it is based on a constructive approach of the Brauer–Witt theorem using strongly monomial characters (see section 2 for the definition).

The Brauer–Witt theorem ensures that each simple component of  $kG$  is similar to a cyclotomic algebra over its center. As far as we know, the precise description of this cyclotomic algebra is not obvious from the proofs of the Brauer–Witt theorem available in the literature (see e.g. [Yam]). The proof of the Brauer–Witt theorem presented in [Yam] relies on the existence, for each prime integer  $p$ , of a  $p$ -elementary subgroup of  $G$  that determines the  $p$ -part of a given simple component

---

Received by the editor February 20, 2006.

2000 *Mathematics Subject Classification*. Primary 20C15; Secondary 16S34.

*Key words and phrases*. Wedderburn decomposition, Brauer–Witt theorem, Schur index.

The author was partially supported by the D.G.I. of Spain and Fundación Séneca of Murcia.

©2007 American Mathematical Society  
Reverts to public domain 28 years from publication

up to similarity in the corresponding Brauer group. We present a slightly different approach of the proof of the Brauer–Witt theorem in which instead of using  $p$ -elementary subgroups we use strongly monomial characters or strongly monomial subgroups that allow a good description of the simple algebras. Moreover, using this approach, the number of subgroups to look for is larger, and eventually one could obtain a description of a simple component more easily or even a description in which it is not necessary to consider each prime separately as has to be done in general.

The Brauer–Witt theorem is also a standard theoretical method for computing the Schur index of a character in the above situation. See [Shi], [Her96] and [Her03] for an approach that studies this aspect of the theorem, i.e., the computation of the Schur index of the simple components.

In section 2 we establish the basic notation and we collect several results from [Oli-Río-Sim04]. In section 3 we present the algorithmic proof of the Brauer–Witt theorem in four steps and we finish with a sketch of the algorithm. Finally, in section 4 we show how the algorithm works in a couple of examples.

This paper has been written under the supervision of Ángel del Río who posed the problem and provided many useful suggestions.

## 2. MONOMIAL AND STRONGLY MONOMIAL CHARACTERS

The simple components in the Wedderburn decomposition of  $kG$  are parameterized by the complex irreducible characters of the group  $G$ . The simple component corresponding to the irreducible character  $\chi$  is the unique simple ideal  $I$  of  $kG$  such that  $\chi(I) \neq 0$ . Following [Yam], we denote this simple component by  $A(\chi, k)$ . The centre of  $A(\chi, k)$  is  $\mathbb{k} = k(\chi)$ , the field of character values of  $\chi$  over  $k$ . The simple algebra  $A(\chi, k)$  represents an element of the Schur subgroup of the Brauer group of  $\mathbb{k}$ . If  $F$  is a field extension of  $k$ , then  $A(\chi, F) = F(\chi) \otimes_{\mathbb{k}} A(\chi, k)$ , and therefore the cyclotomic structure up to similarity of  $A(\chi, k)$  determines the cyclotomic structure of  $A(\chi, F)$ . Hence, we are interested in considering  $k$  as small as possible, for instance  $\mathbb{Q}$ .

The results of this section are mostly from [Oli-Río-Sim04] and play an important role in our proof of the Brauer–Witt theorem. We begin by establishing some notation. Throughout  $G$  is a finite group,  $H$  a subgroup of  $G$ ,  $R$  a ring,  $F \leq L$  a field extension,  $\chi$  an ordinary irreducible character of  $G$ ,  $n$  an integer and  $p$  a prime number. Also, we use the following notation:

$\text{Cen}_G(H)$	centralizer of $H$ in $G$
$N_G(H)$	normalizer of $H$ in $G$
$\text{Gal}(L/F)$	Galois group of $L/F$
$\xi_n = e^{\frac{2\pi i}{n}}$	complex $n$ -th primitive root of unity
$R *_{\tau}^{\sigma} G$	crossed product of $G$ with coefficients in $R$ , action $\sigma$ and twisting or cocycle $\tau$ (see e.g. [Pas])
$\text{Br}(F)$	Brauer group of the field $F$
$\text{Br}(F)_p$	the subgroup of $\text{Br}(F)$ consisting of all classes whose exponent is a power of $p$
$\text{Res}_{F \rightarrow L}$	restriction map from $\text{Br}(F)$ to $\text{Br}(L)$
$\text{Cor}_{L \rightarrow F}$	corestriction (transfer) map from $\text{Br}(L)$ to $\text{Br}(F)$

[A]	element of the Brauer group $\text{Br}(F)$ , i.e., the equivalence class of a central simple $F$ -algebra $A$ under the similarity relation $\sim$ in $\text{Br}(F)$
$(L/F, \tau)$	crossed product algebra for a finite Galois extension $F \leq L$ and $\tau \in Z^2(\text{Gal}(L/F), L^*)$ (see e.g. [Rei])
$C(F)$	similarity classes in $\text{Br}(F)$ represented by a cyclotomic algebra
$m_F(\chi)$	Schur index of $\chi$ over the field $F$
$m_F(\chi)_p$	$p$ -part of the Schur index of $\chi$ over the field $F$
$\text{deg}(\chi)$	the degree of the character $\chi$
$\text{Lin}(H, K)$	set of linear characters of $H$ with kernel $K$ , where $K \trianglelefteq H$
$\left(\frac{a, b}{F}\right)$	quaternion algebra over $F$ , where $a, b \in F^*$ (see e.g. [Pie])
$\mathbb{H}(F)$	quaternion algebra $\left(\frac{-1, -1}{F}\right)$

If  $K \trianglelefteq H \leq G$ , then let  $\varepsilon(H, K) = \widehat{K} = \frac{1}{|K|} \sum_{k \in K} k \in \mathbb{Q}K$  if  $H = K$ , and if  $H \neq K$ , then let

$$\varepsilon(H, K) = \prod_{M/K \in \mathcal{M}(H/K)} (\widehat{K} - \widehat{M}),$$

where  $\mathcal{M}(H/K)$  denotes the set of all minimal normal subgroups of  $H/K$ . Furthermore, let  $e(G, H, K)$  denote the sum of the different  $G$ -conjugates of  $\varepsilon(H, K)$  in  $\mathbb{Q}G$ , that is, if  $T$  is a right transversal of  $\text{Cen}_G(\varepsilon(H, K))$  in  $G$ , then  $e(G, H, K) = \sum_{t \in T} \varepsilon(H, K)^t$ , where  $\text{Cen}_G(\varepsilon(H, K))$  is the centralizer of  $\varepsilon(H, K)$  in  $G$ . Clearly,  $e(G, H, K)$  is a central element of  $\mathbb{Q}G$ . If the  $G$ -conjugates of  $\varepsilon(H, K)$  are orthogonal, then  $e(G, H, K)$  is a central idempotent of  $\mathbb{Q}G$ .

A *Shoda pair* of  $G$  is a pair  $(H, K)$  of subgroups of  $G$  with the properties that  $K \trianglelefteq H$  and there is  $\psi \in \text{Lin}(H, K)$  such that the induced character  $\psi^G$  is irreducible. Using an old theorem of Shoda [Cur-Rei, Corollary 45.4] that gives a criterion for irreducibility of monomial characters, we know that a pair of subgroups of  $G$  is a Shoda pair if and only if  $K \trianglelefteq H$ ,  $H/K$  is cyclic and if  $g \in G$  and  $[H, g] \cap H \subseteq K$ , then  $g \in H$ . Furthermore, if  $(H, K)$  is a Shoda pair of  $G$ , then there is a unique rational number  $\alpha$  such that  $\alpha e(G, H, K)$  is a primitive central idempotent of  $\mathbb{Q}G$  [Oli-Río-Sim04].

It is easy to see that if  $K \trianglelefteq H \leq G$  and  $\psi_1, \psi_2 \in \text{Lin}(H, K)$ , then  $A(\psi_1^G, \mathbb{Q}) = A(\psi_2^G, \mathbb{Q})$ , and so we denote  $A(G, H, K) = A(\psi^G, \mathbb{Q})$  for any  $\psi \in \text{Lin}(H, K)$ . In other words, the sum of the different characters induced by the elements of  $\text{Lin}(H, K)$  is an irreducible rational character of  $G$  and  $A(G, H, K)$  is the simple component of  $\mathbb{Q}G$  associated to this character.

A *strong Shoda pair* of  $G$  is a Shoda pair  $(H, K)$  of  $G$  such that  $H \trianglelefteq N_G(K)$  and the different conjugates of  $\varepsilon(H, K)$  are orthogonal. If  $(H, K)$  is a strong Shoda pair, then  $e(G, H, K)$  is a primitive central idempotent of  $\mathbb{Q}G$ .

An irreducible *monomial character* (respectively *strongly monomial character*)  $\chi$  of  $G$  is a character of the form  $\chi = \psi^G$  for  $\psi \in \text{Lin}(H, K)$  and some Shoda (respectively strong Shoda) pair  $(H, K)$  of  $G$ , or equivalently  $A(\chi, \mathbb{Q}) = A(G, H, K)$  for some Shoda (respectively strong Shoda) pair  $(H, K)$  of  $G$ . Then we say that  $A(G, H, K)$  is a monomial (respectively strongly monomial) component of  $\mathbb{Q}G$ .

A finite group  $G$  is *monomial* if every irreducible character of  $G$  is monomial, and it is *strongly monomial* if every irreducible character of  $G$  is strongly monomial. It is well known that every abelian-by-supersolvable group is monomial, and

recently it was proved that it is even strongly monomial. In [Oli-Río-Sim04] it is shown that every monomial group of order less than 500 is strongly monomial. We recently found that all monomial groups of order smaller than 1000 are strongly monomial and the smallest monomial non-strongly-monomial group is a group of order 1000, the 86-th one in the library of the GAP system. However, there are irreducible monomial characters that are not strongly monomial in smaller groups. The group of the smallest order with such irreducible monomial non-strongly-monomial characters is presented in Example 10.

If  $(H, K)$  is a strong Shoda pair of a group  $G$ , then one can give a description of the structure of the simple component  $A(G, H, K)$  as a matrix algebra over a crossed product of an abelian group by a cyclotomic field with action and twisting that can be described with easy arithmetic using information from the group  $G$ . Namely, in [Oli-Río-Sim04, Proposition 3.4] it is shown that if  $(H, K)$  is a strong Shoda pair, then

$$A(G, H, K) \simeq \mathcal{M}_n(\mathbb{Q}(\xi_m) *_{\tau}^{\sigma} N/H),$$

where  $N = N_G(K)$ ,  $n = [G : N]$ ,  $m = [H : K]$ ,  $\mathbb{Q}(\xi_m) *_{\tau}^{\sigma} N/H$  is the crossed product of the group  $N/H$  with coefficients in the field  $\mathbb{Q}(\xi_m)$  with action  $\sigma$  and twisting  $\tau$  given as follows: if  $hK$  is a generator of  $H/K$  and  $n, n' \in N$ , then  $\sigma(nH) = \xi_m^i$  if  $n^{-1}hnK = h^iK$ , and  $\tau(nH, n'H) = \xi_m^j$  if  $[n, n']K = h^jK$ .

### 3. THE ALGORITHMIC PROOF OF THE BRAUER–WITT THEOREM

The Brauer–Witt theorem states that the simple component  $A(\chi, k)$  corresponding to the irreducible character  $\chi$  of the group  $G$  over the field  $k$  is a simple algebra similar to a cyclotomic algebra over its center  $\mathbb{k} = k(\chi)$ , that is, a crossed product algebra  $(\mathbb{k}(\xi)/\mathbb{k}, \tau)$ , where  $\xi$  is a root of 1 and all the values of the cocycle  $\tau$  are roots of unity in  $\mathbb{k}(\xi)$ .

In this section we present a proof of the Brauer–Witt theorem that gives a method to explicitly construct the above cyclotomic algebra. Our proof is divided into four steps that one could name as: *constructible description* for the strongly monomial case, *reduction* of the general case to the strongly monomial case, *existence* of strongly monomial characters, and *change of field*. The first step deals with the strongly monomial case, that is, the constructible description of the simple component associated to a strongly monomial character. The reduction step consists of describing the  $p$ -part of  $A(\chi, k)$  as the  $p$ -part of the algebra  $A(\theta, k)$  associated to a strongly monomial character  $\theta$  of a subgroup of  $G$ . Then we are faced with the problem of showing that the appropriate strongly monomial character  $\theta$  for every prime  $p$  does exist. One of the conditions on  $\theta$  in the reduction step is that  $\mathbb{k}(\theta) = \mathbb{k}$ , and it is not always true that such a character with this condition exists. However, there does exist a character  $\theta$  such that  $\mathbb{k}(\theta) \subseteq L_p$ , where  $L_p$  is the  $p'$ -splitting field of  $A(\chi, k)$  (see §3.2 for the definition). The proof of the existence of the desired strongly monomial character is presented in the third step. So we have gone up to each  $L_p$  to describe the  $p$ -part, and now we have to return to the initial field  $\mathbb{k}$ . The way back is the change of field part which is made through the corestriction map.

**3.1. The strongly monomial case.** The following proposition provides the constructible Brauer–Witt theorem for strongly monomial characters. It gives a precise description of the simple algebra associated to a strongly monomial character as

an algebra similar to a cyclotomic algebra. In this particular case, one obtains the description of the strongly monomial simple component at once, without the need to follow the next steps as has to be done in the general case.

**Proposition 1.** *Let  $(H, K)$  be a strong Shoda pair of the group  $G$ ,  $\psi \in \text{Lin}(H, K)$ ,  $N = N_G(K)$ ,  $m = [H : K]$ ,  $n = [G : N]$  and  $\xi_m$  a complex primitive  $m$ -th root of unity. Then  $N/H \simeq \text{Gal}(\mathbb{Q}(\xi_m)/\mathbb{Q}(\psi^G))$ .*

Furthermore, if  $k$  is a field of characteristic 0,  $\mathbb{k} = k(\psi^G)$ ,  $d = \frac{[\mathbb{Q}(\xi_m) : \mathbb{Q}(\psi^G)]}{[\mathbb{k}(\xi_m) : \mathbb{k}]}$  and  $\tau'$  is the restriction to  $\text{Gal}(\mathbb{k}(\xi_m)/\mathbb{k})$  of the cocycle  $\tau$  associated to the natural extension

$$(1) \quad 1 \rightarrow H/K \simeq \langle \xi_m \rangle \rightarrow N/K \rightarrow N/H \rightarrow 1,$$

then

$$(2) \quad A(\psi^G, k) \simeq \mathcal{M}_{nd}(\mathbb{k}(\xi_m)/\mathbb{k}, \tau').$$

*Proof.* It is proved in [Oli-Río-Sim04, Theorem 3.4] that

$$A(\psi^G, \mathbb{Q}) \simeq \mathcal{M}_n(\mathbb{Q}(\xi_m) *_{\tau}^{\sigma} N/H),$$

where the action  $\sigma$  is induced by the natural conjugation map  $f : N \rightarrow \text{Aut}(H/K) \simeq \text{Gal}(\mathbb{Q}(\xi_m)/\mathbb{Q})$  and the twisting is the cocycle  $\tau$  given by the exact sequence (1). Since  $H/K$  is maximal abelian in  $N/K$ , the kernel of  $f$  is  $H$ . The center of  $A(\psi^G, \mathbb{Q})$  is  $\mathbb{Q}(\psi^G)$ ; hence  $f(N/H) \subseteq \text{Gal}(\mathbb{Q}(\xi_m)/\mathbb{Q}(\psi^G))$  and the isomorphism holds because  $[N : H] = \frac{\text{deg}(A(\psi^G, \mathbb{Q}))}{n} = [\mathbb{Q}(\xi_m) : \mathbb{Q}(\psi^G)]$ .

Furthermore,  $[A(\psi^G, k)] = \text{Res}_{\mathbb{Q}(\psi^G) \rightarrow \mathbb{k}}([A(\psi^G, \mathbb{Q})]) = [(\mathbb{k}(\xi_m)/\mathbb{k}, \tau')]$  and

$$\frac{\text{deg}(A(\psi^G, k))}{\text{deg}(\mathbb{k}(\xi_m)/\mathbb{k}, \tau')} = \frac{[G : H]}{[\mathbb{k}(\xi_m) : \mathbb{k}]} = \frac{n[\mathbb{Q}(\xi_m) : \mathbb{Q}(\psi^G)]}{[\mathbb{k}(\xi_m) : \mathbb{k}]} = nd,$$

which yields the isomorphism  $A(\psi^G, k) \simeq \mathcal{M}_{nd}(\mathbb{k}(\xi_m)/\mathbb{k}, \tau')$ . □

*Remark 2.* Notice that the description in (2) can be given by the numerical information of a 4-tuple:

$$(3) \quad (nd, m, (o_i, \alpha_i, \beta_i)_{1 \leq i \leq l}, (\gamma_{ij})_{1 \leq i < j \leq l}),$$

where  $n$ ,  $d$  and  $m$  are as in Proposition 1 and the tuples of integers  $(\alpha_i)_{1 \leq i \leq l}$ ,  $(\beta_i)_{1 \leq i \leq l}$ ,  $(\gamma_{ij})_{1 \leq i < j \leq l}$  satisfy the relations:  $x^{g_i} = x^{\alpha_i}$ ,  $g_i^{o_i} = x^{\beta_i}$ ,  $[g_j, g_i] = x^{\gamma_{ij}}$ , for  $x$  a generator of  $H/K$ ,  $g_1, \dots, g_l \in N/K$  such that  $N_1/H = \langle \bar{g}_1 \rangle \times \dots \times \langle \bar{g}_l \rangle$  (with  $\bar{g}_i$  the image of  $g_i \in N/K$  in  $N/H$ ), where  $N_1/H$  is the image of  $\text{Gal}(\mathbb{k}(\xi_m)/\mathbb{k})$  in  $N/H$  under the isomorphism  $N/H \simeq \text{Gal}(\mathbb{Q}(\xi_m)/\mathbb{Q}(\psi^G))$  and  $o_i$  is the order of  $\bar{g}_i$ , for every  $i = 1, \dots, l$ .

Thus  $A(\psi^G, k) \simeq M_{nd}(A)$ , where  $A$  is the algebra defined by the following presentation:

$$(4) \quad A = \mathbb{k}(\xi_m)\langle g_1, \dots, g_l \mid \xi_m^{g_i} = \xi_m^{\alpha_i}, g_i^{o_i} = \xi_m^{\beta_i}, g_j g_i = g_i g_j \xi_m^{\gamma_{ij}}, 1 \leq i < j \leq l \rangle.$$

**3.2. Reduction to strongly monomial characters.** Let the finite group  $G$  have exponent  $n$  and let  $k$  be a field of characteristic 0. For every irreducible character  $\chi$  of  $G$  and every prime  $p$ , the  $p'$ -splitting field of the simple component  $A(\chi, k)$  over  $\mathbb{k} = k(\chi)$  is the unique field  $L_p$  between  $\mathbb{k}$  and  $\mathbb{k}(\xi_n)$  such that  $[\mathbb{k}(\xi_n) : L_p]$  is a power of  $p$  and  $[L_p : \mathbb{k}]$  is relatively prime to  $p$ . That is, the field  $L_p$  is the field corresponding to the Sylow  $p$ -subgroup of  $\text{Gal}(\mathbb{k}(\xi_n)/\mathbb{k})$  by the Galois correspondence.

Let  $D$  be a division algebra central over  $\mathbb{k}$  with index  $m$  that has the following factorization into prime powers  $m = p_1^{a_1} p_2^{a_2} \dots p_s^{a_s}$ . Then  $D$  is  $\mathbb{k}$ -isomorphic to the product  $D_1 \otimes D_2 \otimes \dots \otimes D_s$ , where  $D_i$  is a division algebra central over  $\mathbb{k}$  with index  $p_i^{a_i}$  for every  $i$  from 1 to  $s$ . We call the algebra class  $[D_i]$  the  $p_i$ -part of  $[D]$  and we denote it by  $[D]_{p_i}$ . If  $p \nmid m$ , then let the  $p$ -part of  $[D]$  be equal to  $[\mathbb{k}]$ , the identity in the Brauer group of  $\mathbb{k}$ . Recall that  $m_{\mathbb{k}}(\chi)$  denotes the Schur index of  $\chi$  over  $\mathbb{k}$  which coincides with the Schur index of the simple component  $A(\chi, k)$  of  $kG$  corresponding to  $\chi$ . Furthermore,  $m_{\mathbb{k}}(\chi)_p$  is the  $p$ -part of the Schur index of  $\chi$  over  $\mathbb{k}$ .

The following proposition gives the reduction part (up to similarity) of the computation of a simple  $p$ -component  $[A(\chi, k)]_p$ , for every prime  $p$ , to the computation of the  $p$ -part corresponding to a suitable subgroup of  $G$  and an irreducible character of it that verifies some additional conditions.

**Proposition 3.** [Yam, Proposition 3.8] *Let  $G$  be a finite group,  $\chi$  an irreducible character of  $G$ ,  $k$  a field of characteristic 0 and  $\mathbb{k} = k(\chi)$ . Let  $M$  be a subgroup of  $G$  and  $\theta$  an irreducible character of  $M$  such that  $k(\theta) = \mathbb{k}$ .*

*For each prime  $p$  such that  $(\chi_M, \theta)$  is coprime to  $p$ , one has*

$$[A(\chi, k)]_p = [A(\theta, k)]_p.$$

*Moreover,  $m_{\mathbb{k}}(\chi)_p = m_{L_p}(\theta)$ .*

**3.3. Existence of suitable strongly monomial characters.** Theorem 3 states that the  $p$ -part of  $A(\chi, k)$  is Brauer equivalent to the  $p$ -part of  $A(\theta, k)$  provided  $(\chi_M, \theta)$  is coprime to  $p$  and  $\chi$  and  $\theta$  take values in  $\mathbb{k}$ . If  $\theta$  is a strongly monomial character, then this  $p$ -part would be described as explained in Proposition 1. Therefore, one would like to show that such a character  $\theta$  does exist for every prime  $p$  dividing the Schur index of  $\chi$ . However, this is not true. Alternatively, using the following Proposition 4, which is a corollary of the Witt–Berman theorem [Cur-Rei, Theorem 42.3], one can find such a character  $\theta$  if  $\mathbb{k}$  is replaced by  $L_p$ , the  $p'$ -splitting field of  $A(\chi, k)$ . The Witt–Berman theorem is a generalization of Brauer’s theorem on induced characters to the case where the underlying field  $\mathbb{k}$  is an arbitrary subfield of the complex field  $\mathbb{C}$ .

**Proposition 4.** *Every  $\mathbb{k}$ -character of  $G$  is a  $\mathbb{Z}$ -linear combination  $\sum_i a_i \theta_i^G$ , where every  $a_i \in \mathbb{Z}$  and each  $\theta_i$  is an irreducible character of a strongly monomial subgroup of  $G$ .*

*Proof.* By the Witt–Berman theorem, every  $\mathbb{k}$ -character of  $G$  is a  $\mathbb{Z}$ -linear combination  $\sum_i a_i \theta_i^G$ , where the  $\theta_i$ ’s are irreducible  $\mathbb{k}$ -characters of  $\mathbb{k}$ -elementary subgroups  $H_i$  of  $G$ . In particular, the  $H_i$ ’s are cyclic-by- $p_i$ -groups for some primes  $p_i$  and by [Oli-Río-Sim04] each  $H_i$  is strongly monomial.  $\square$

The next proposition establishes the existence of a strongly monomial subgroup and character with the desired properties that appear in Theorem 3, relative to the field  $L_p$ , the  $p'$ -splitting field of  $A(\chi, k)$ .

**Proposition 5.** *Let the finite group  $G$  have exponent  $n$ ,  $\xi = \xi_n$  and  $\chi$  be an irreducible  $\mathbb{k}$ -character of  $G$ . For every prime  $p$ , there exist a strongly monomial subgroup  $M$  of  $G$  and an irreducible character  $\theta$  of  $M$  such that  $(\chi, \theta^G) = (\chi_M, \theta)$  is coprime to  $p$  and  $k(\theta) \subseteq L_p$ , where  $L_p$  is the  $p'$ -splitting field of  $A(\chi, k)$ .*

*Proof.* Let  $b$  be a divisor of  $|G|$  such that  $|G|/b$  is a power of  $p$  and  $(p, b) = 1$ . Then, by Proposition 4,  $b1_G = \sum_i c_i \lambda_i^G$ , where each  $\lambda_i$  is a  $\mathbb{k}$ -character of a subgroup  $M_i$  of  $G$  which is strongly monomial. Furthermore,

$$b\chi = \sum_i c_i \chi \lambda_i^G = \sum_i c_i (\chi_{M_i} \lambda_i)^G.$$

Moreover,  $\mathbb{k}(\chi_{M_i}) \subseteq \mathbb{k}(\chi) \subseteq \mathbb{k}$ ,  $\mathbb{k}(\lambda_i) \subseteq \mathbb{k}$  for every  $i$  and  $\mathbb{k}(\xi)$  is a splitting field of every subgroup of  $G$ . Thus if  $\theta_j$  is a constituent of  $\chi_{M_i} \lambda_i$ , that is,  $\theta_j$  appears in the decomposition of  $\chi_{M_i} \lambda_i$  as a sum of irreducible characters, then  $(\theta_j, \lambda_i)$  is a multiple of  $[\mathbb{k}(\theta_j) : \mathbb{k}]$  and therefore

$$b\chi = \sum_j d_j [\mathbb{k}(\theta_j) : \mathbb{k}] \theta_j^G,$$

where each  $\theta_j$  is an irreducible character in a group  $M'_j$  which is strongly monomial. Then

$$b = (\chi, b\chi) = \sum_j d_j [\mathbb{k}(\theta_j) : \mathbb{k}] (\chi, \theta_j^G).$$

Since  $b$  is not a multiple of  $p$ , there is  $j$  such that if  $M = M'_j$  and  $\theta = \theta_j$ , then  $[\mathbb{k}(\theta) : \mathbb{k}] (\chi, \theta^G)$  is not a multiple of  $p$ . Thus  $(\chi, \theta^G)$  is not a multiple of  $p$ . Since  $\mathbb{k} \subseteq \mathbb{k}(\theta) \subseteq \mathbb{k}(\xi)$  and  $[\mathbb{k}(\xi) : L_p]$  is a prime power, one has that  $\mathbb{k}(\theta) \subseteq L_p$ .  $\square$

Proposition 5 proves that, for each prime  $p$ , there exists a strongly monomial character  $\theta$  of a subgroup  $M$  of  $G$  that takes values in  $L_p$  and  $(\chi_M, \theta)$  is coprime to  $p$ . Hence, from Theorem 3 it follows that  $A(\chi, L_p)$  is similar to  $A(\theta, L_p)$ , because the index of  $A(\chi, L_p)$  is a power of  $p$ .

Observe that it was proved that the subgroup  $M$  in Proposition 5 can be taken to be strongly monomial. Moreover, using the Witt–Berman theorem, one can prove that  $M$  could be taken to be  $p$ -elementary. However, for practical reasons, it is better not to impose  $M$  to be  $p$ -elementary or even strongly monomial, because the role of  $M$ , or better say  $\theta$ , is to use the presentation of  $A(\theta, L_p)$  as a cyclotomic algebra given in Proposition 1 to describe the  $p$ -part of  $A(\chi, L_p)$ , which is similar to  $A(\theta, L_p)$  by Theorem 3. So, not imposing conditions on  $M$  but on  $\theta$ , a strongly monomial character in a possibly non-strongly-monomial group, the list of possible  $\theta$ 's is larger and it is easier to find the desired strongly monomial character. The proof of Proposition 5 does not provide a constructive way to find the character  $\theta$ , but this is clearly a finite computable searching problem. One only needs to compute  $L_p$ , an easy Galois theory problem, and then run on the strongly monomial characters  $\theta$  of the subgroups  $M$  of  $G$  computing  $(\chi_M, \theta)$  and  $\mathbb{k}(\theta)$  until the character satisfying the hypothesis of Proposition 5 is found. The search of the strongly monomial characters of a given group can be performed using the algorithm explained in [Oli-Río].

**3.4. Back to the initial field.** In this last step we complete the proof of the Brauer–Witt theorem. Moreover, using an explicit formula for the corestriction  $\text{Cor}_{L_p \rightarrow \mathbb{k}}$  on 2-cocycles, where  $L_p$  is the  $p'$ -splitting field of  $A(\chi, k)$ , and the description of the simple components  $A(\chi, L_p)$  as algebras similar to precise cyclotomic algebras, we obtain a good description of the simple algebra  $A(\chi, k)$ .

The proof of the Brauer–Witt theorem in standard references such as [Yam] does not pay much attention to effective computations of the corestriction  $\text{Cor}_{L_p \rightarrow \mathbb{k}}$ . Instead, we are interested in explicit computations of the cyclotomic form of an

element of the Schur subgroup. After decomposing the simple algebra  $A(\chi, k)$  into  $p$ -parts and describing every simple  $p$ -part as similar over  $L_p$  to a cyclotomic algebra  $[(\mathbb{k}(\xi)/L_p, \tau)]$ , the corestriction permits returning to the initial field  $\mathbb{k}$ . Hence, for every prime  $p$ , we have  $\text{Cor}_{L_p \rightarrow \mathbb{k}}([\mathbb{k}(\xi)/L_p, \tau]) = [(\mathbb{k}(\xi)/\mathbb{k}, \text{Cor}_{L_p \rightarrow \mathbb{k}}(\tau))]$ . A formula for the action of the corestriction on 2-cocycles is given in [Wei, Proposition 2-5-2]. This formula takes an easy form in our situation, because we only need to apply  $\text{Cor}_{L_p \rightarrow \mathbb{k}}$  to a 2-cocycle  $\tau$  that takes values in a cyclotomic extension  $\mathbb{k}(\xi)$  of  $\mathbb{k}$  such that  $[L_p : \mathbb{k}]$  and  $[\mathbb{k}(\xi) : L_p]$  are coprimes. In particular,  $H = \text{Gal}(\mathbb{k}(\xi)/L_p)$ , the Sylow  $p$ -subgroup of the abelian group  $G$ , has a complement  $H' = \text{Gal}(\mathbb{k}(\xi)/L_p')$  on  $G = \text{Gal}(\mathbb{k}(\xi)/\mathbb{k})$ . We can formulate the following proposition.

**Proposition 6.** *Let  $F/\mathbb{k}$  be a finite Galois extension and  $\mathbb{k} \leq L, L' \leq F$  fields such that  $L \cap L' = \mathbb{k}$  and  $LL' = F$ . Let  $G = \text{Gal}(F/\mathbb{k})$ ,  $H = \text{Gal}(F/L)$ ,  $H' = \text{Gal}(F/L')$  and let  $\tau \in H^2(H, F^*)$  be a 2-cocycle of  $H$ . Then  $G \simeq H \times H'$  and*

$$(5) \quad (\text{Cor}_{L \rightarrow \mathbb{k}}(\tau))(g_1, g_2) = N_{L'}^F(\tau(\pi(g_1), \pi(g_2))),$$

where  $\pi : G \rightarrow H$  denotes the projection,  $N_{L'}^F$  is the norm function of the field extension  $L' \leq F$  and  $g_1, g_2 \in G$ . In particular, if  $[(F/L, \tau)]$  is a cyclotomic algebra and  $F$  is a cyclotomic extension of  $\mathbb{k}$ , then  $\text{Cor}_{L \rightarrow \mathbb{k}}([(F/L, \tau)]) = [(F/\mathbb{k}, \text{Cor}_{L \rightarrow \mathbb{k}}(\tau))]$  is a cyclotomic algebra.

*Proof.* By [Spi, Theorem 22.17],  $H \simeq \text{Gal}(L'/\mathbb{k})$  and  $H' \simeq \text{Gal}(L/\mathbb{k})$  and the mapping  $\varphi : G \rightarrow \text{Gal}(L'/\mathbb{k}) \times \text{Gal}(L/\mathbb{k})$  given by  $\sigma \mapsto (\sigma|_{L'}, \sigma|_L)$  is an isomorphism; hence  $G \simeq H \times H'$ . Then, using  $H'$  as a transversal of  $H$  in  $G$ , the formula from [Wei, Proposition 2-5-2] for the corestriction in the particular case of the 2-cocycle  $\tau \in H^2(H, F^*)$  takes the following form, where  $\pi' : G \rightarrow H'$  denotes the projection:

$$\begin{aligned} \text{Cor}_{L \rightarrow \mathbb{k}}(\tau)(g_1, g_2) &= \prod_{t \in H'} t^{-1} \tau(tg_1 \pi'(tg_1)^{-1}, \pi'(tg_1)g_2 \pi'(tg_1g_2)^{-1}) \\ &= \prod_{t \in H'} t^{-1} \tau(\pi(tg_1), \pi(\pi'(tg_1)g_2)) \\ &= \prod_{t \in H'} t^{-1} \tau(\pi(g_1), \pi(g_2)) = N_{L'}^F(\tau(\pi(g_1), \pi(g_2))). \end{aligned}$$

□

**Theorem 7.** (Brauer–Witt) *If  $G$  is a finite group of exponent  $n$ ,  $\chi$  is an irreducible character of  $G$ ,  $k$  is a field of characteristic 0 and  $\mathbb{k} = k(\chi)$ , then the simple component  $A(\chi, k)$  is similar to a cyclotomic algebra over  $\mathbb{k}$ .*

*Proof.* Let  $p$  be an arbitrary prime. Using the restriction homomorphism, we obtain  $\text{Res}_{\mathbb{k} \rightarrow L_p}([A(\chi, k)]_p) = [A(\chi, L_p)] = [C]$ , that is, a cyclotomic algebra over  $L_p$ , the  $p'$ -splitting field of  $A(\chi, k)$ . Proposition 6 implies that  $\text{Cor}_{L_p \rightarrow \mathbb{k}}([C])$  is a class of  $\text{Br}(\mathbb{k})$  represented by a cyclotomic algebra over  $\mathbb{k}$ . Let  $[\mathbb{k}(\xi_n) : L_p] = p^\alpha$  and  $[L_p : \mathbb{k}] = m \not\equiv 0 \pmod{p}$ . Let  $a$  be an integer such that  $am \equiv 1 \pmod{p^\alpha}$ . Then, using the relation between the restriction and the corestriction given by  $\text{Cor}_{L_p \rightarrow \mathbb{k}} \circ \text{Res}_{\mathbb{k} \rightarrow L_p}([A(\chi, k)]_p) = ([A(\chi, k)]_p)^m$ , we obtain

$$\begin{aligned} (\text{Cor}_{L_p \rightarrow \mathbb{k}}([C]))^a &= (\text{Cor}_{L_p \rightarrow \mathbb{k}} \circ \text{Res}_{\mathbb{k} \rightarrow L_p}([A(\chi, k)]_p))^a \\ &= ([A(\chi, k)]_p)^{am} = [A(\chi, k)]_p. \end{aligned}$$



Because  $p$  is arbitrary and the tensor product of cyclotomic algebras over  $\mathbb{k}$  is similar to a cyclotomic algebra, we conclude that the class  $[A(\chi, k)]$  is represented by a cyclotomic algebra over  $\mathbb{k}$ .  $\square$

Notice that in the proof of Theorem 7 we mentioned that the tensor product of cyclotomic algebras over  $\mathbb{k}$  is similar to a cyclotomic algebra. The proof of this claim is also constructible, because by inflating two cyclotomic algebras say  $C_1 = [(\mathbb{k}(\xi_{n_1})/\mathbb{k}, \tau_1)]$  and  $C_2 = [(\mathbb{k}(\xi_{n_2})/\mathbb{k}, \tau_2)]$  to a common cyclotomic extension, for example  $\mathbb{k}(\xi_n)$  for  $n$  the least common multiple of  $n_1$  and  $n_2$ , one may assume that  $n_1 = n_2$  and hence  $C_1 \otimes C_2 \sim (\mathbb{k}(\xi_n)/\mathbb{k}, \tau_1\tau_2)$ .

The constructive algorithm of the cyclotomic structure of a simple component  $A(\chi, k)$  of  $kG$  given by the proof of the Brauer–Witt theorem is given below.

**Algorithm 1.** *Input:* An irreducible character  $\chi$  of the finite group  $G$  and  $k$  a field of characteristic 0.

- (1) Compute  $\mathbb{k} = k(\chi)$ , the field of character values of the character  $\chi$  over  $k$ .
- (2) Compute  $p_1, \dots, p_r$ , the prime divisors of  $\gcd(\deg(\chi), [\mathbb{k}(\xi_n) : \mathbb{k}])$ .
- (3) For every prime  $p \in \{p_1, \dots, p_r\}$  do
  - (a) Determine  $L_p$ , the  $p'$ -splitting fields of  $A(\chi, k)$ .
  - (b) Search  $\theta = \psi^M$ , a strongly monomial character of a subgroup  $M$ , where  $\psi \in \text{Lin}(H, K)$  for a strongly monomial pair  $(H, K)$  of  $M$ , such that  $(\chi_M, \theta)$  is coprime to  $p$  and  $\mathbb{k}(\theta) \subseteq L_p$  (the existence is guaranteed by Proposition 5).
  - (c) Compute the cyclotomic algebra

$$A(\theta, L_p) = (\mathbb{k}(\xi_{n_p})/L_p, \tau_p),$$

an element in  $\text{Br}(L_p)$  (using Proposition 1).

- (d) Compute  $\text{Cor}_{L_p \rightarrow \mathbb{k}}(\tau_p) = \tau'_p$  (using formula (5)).
- (e) Compute  $\alpha$  such that  $p^\alpha \mid \deg(A(\chi, k))$  and  $p^{\alpha+1} \nmid \deg(A(\chi, k))$  and the integer  $a$  such that  $am \equiv 1 \pmod{p^\alpha}$ , where  $m = [L_p : \mathbb{k}]$ .
- (4) Compute the cocycle  $\tau = (\tau'_{p_1})^{a_{p_1}} \dots (\tau'_{p_r})^{a_{p_r}}$  (after inflating to a common cyclotomic extension).

*Output:* The similarity class  $[(\mathbb{k}(\xi_n)/\mathbb{k}, \tau)]$ .

*Remark 8.* (i) For every  $p \in \{p_1, \dots, p_r\}$ ,  $\text{Cor}_{L_p \rightarrow \mathbb{k}}([(\mathbb{k}(\xi_n)/L_p, \tau_p)]) = [(\mathbb{k}(\xi_n)/\mathbb{k}, \tau'_p)]$  (Proposition 6) is a cyclotomic algebra in  $\text{Br}(\mathbb{k})$  and we have  $[(\mathbb{k}(\xi_n)/\mathbb{k}, \tau'_p)] = [A(\chi, k)]_p^m$ , where  $m = [L_p : \mathbb{k}]$ . We obtain  $[A(\chi, k)]_p$  computing  $[(\mathbb{k}(\xi_n)/\mathbb{k}, \tau'_p)]^{a_p}$ . The output  $[(\mathbb{k}(\xi_n)/\mathbb{k}, \tau)]$  is equal to  $[A(\chi, k)]$ .

(ii) Some of the primes in  $\{p_1, \dots, p_r\}$  can be covered by a common strongly monomial character. For example, if  $\chi$  is a strongly monomial character, then all the primes are covered at once by this character. See also Remark 9 below.

We finish this section with the algorithm for the computation the Wedderburn decomposition of a group algebra  $kG$ .

**Algorithm 2.** *Input:* The finite group  $G$  and a field  $k$  of characteristic zero.

- (1) Compute  $\text{Irr}(G)$ , the set of ordinary irreducible characters of  $G$  and  $n$  the exponent of  $G$ .
- (2) Take a set of representatives  $E$  of the  $k$ -equivalent classes of  $\text{Irr}(G)$ . Two characters  $\chi_1, \chi_2 \in \text{Irr}(G)$  are  $k$ -equivalent if  $\chi_2 = \sigma \circ \chi_1$  for some  $\sigma$  in  $\text{Gal}(k(\chi_1)/k)$ .

- (3) For every  $\chi \in E$  do
- (a) Apply Algorithm 1 to compute a simple algebra  $A_\chi$  similar to  $A(\chi, k)$ .
  - (b) Add  $B_\chi = \mathcal{M}_{d_1/d_2}(A_\chi)$  to the list of simple components of  $kG$ , where  $d_1$  and  $d_2$  are the degrees of  $\chi$  and  $A_\chi$ , respectively.

*Output:* The Wedderburn decomposition  $kG \simeq \bigoplus_{\chi \in E} B_\chi$ .

*Remark 9.* A more efficient algorithm from the implementation point of view is the one implemented in the `wedderga` package [Bro-Kon-Oli-Olt-Río] that, instead of considering every irreducible character and then searching for some strongly monomial characters of subgroups that give the reduction step, searches for strong Shoda pairs of subgroups that verify the conditions from step (3)(b) of Algorithm 1 running on descending order and analyzes their contribution in step (3)(c) of Algorithm 1 for the different characters and primes. Some of the strong Shoda pairs of subgroups contribute to more than one character or more than one prime.

#### 4. EXAMPLES

In this section we present a couple of examples that illustrate the performance of Algorithms 1 and 2. Some of the computations have been done using the package `wedderga` [Bro-Kon-Oli-Olt-Río] for the computer system GAP (The GAP Group, Version 4.4; 2006) [GAP]. The previous version of the package was useful to compute the Wedderburn decomposition of rational group algebras and semisimple finite group algebras of strongly monomial groups. The new version, in preparation, allows one to compute the Wedderburn decomposition of the group algebra of any finite group over any field of characteristic 0 that can be supported by the GAP system.

**Example 10.** The smallest group with a monomial non-strongly-monomial irreducible character is the group given by the following presentation:

$$G = \langle x, y, a, b \mid x^4 = a^3 = 1, x^2 = y^2 = b^2, x^y = x^{-1}, \\ x^a = y, y^a = xy, x^b = y^{-1}, y^b = x^{-1}, a^b = a^{-1} \rangle.$$

The group  $G$  is the 28-th group of order 48 in the library of small groups of the GAP system.

The output of the old function `WedderburnDecompositionInfo(QG)` of the `wedderga` package is:

```
Wedderga: Warning!! The direct product of the output is a
PROPER direct factor of the input!
[[ [ 1, 1, [ ], [ ] ], [ 1, 2, [ ], [ ] ], [ 3, 2, [ ], [ ] ],
[ 3, 2, [ ], [ ] ], [ 1, 3, [ [ 2, 2, 0 ] ], [ ] ] ].
```

The interpretation of these five 4-tuples using Remark 2 gives rise to five simple components  $\mathbb{Q}, \mathbb{Q}, \mathcal{M}_3(\mathbb{Q}), \mathcal{M}_3(\mathbb{Q})$  and  $\mathcal{M}_2(\mathbb{Q})$  corresponding to five strongly monomial characters of the group  $G$ . As can be seen from the warning message of the `wedderga` package, these are not all the simple components of  $\mathbb{Q}G$ , because the group is not strongly monomial. Moreover, the group  $G$  is not monomial, having the first five characters  $\chi_1, \chi_2, \chi_3, \chi_4, \chi_5$  (of the character table given below) strongly monomial, the character  $\chi_6$  monomial but not strongly monomial and the last two characters  $\chi_7, \chi_8$  not monomial. In order to compute the simple components given by the last three characters we apply Algorithm 1 to  $\chi_6, \chi_7$  and  $\chi_8$ .

	1	[a]	[ab]	[a <sup>2</sup> x]	[x]	[b <sup>2</sup> ]	[a <sup>2</sup> bx]	[bx]
χ <sub>1</sub>	1	1	1	1	1	1	1	1
χ <sub>2</sub>	1	1	-1	1	1	1	-1	-1
χ <sub>3</sub>	2	-1	0	-1	2	2	0	0
χ <sub>4</sub>	3	0	1	0	-1	3	-1	-1
χ <sub>5</sub>	3	0	-1	0	-1	3	1	1
χ <sub>6</sub>	4	1	0	-1	0	-4	0	0
χ <sub>7</sub>	2	-1	0	1	0	-2	-√2	√2
χ <sub>8</sub>	2	-1	0	1	0	-2	√2	-√2

The exponent of  $G$  is  $n = 24 = 2^3 \cdot 3$ ; hence  $\phi(n) = 8 = 2^3$ , where  $\phi$  is the Euler function and  $\mathbb{Q}(\xi_n) = \mathbb{Q}(\xi_{24})$ . The field of character values of  $\chi_6$  is  $\mathbb{k} = \mathbb{Q}$  and of  $\chi_7$  and  $\chi_8$  is  $\mathbb{k} = \mathbb{Q}(\sqrt{2})$ . The degrees of the characters  $\chi_6, \chi_7$  and  $\chi_8$  are 4, 2 and 2 respectively; hence the only prime to be considered in all three cases is  $p = 2$  and the 2'-splitting field  $L_2$  is  $\mathbb{Q}$  for  $\chi_6$  and  $\mathbb{Q}(\sqrt{2})$  for  $\chi_7$  and  $\chi_8$ . Notice that in all these cases it is not necessary to use the corestriction in order to return to the initial field because the 2'-splitting fields coincide with  $\mathbb{k}$ .

The character  $\chi_6$  is monomial, induced by the linear character  $\psi \in \text{Lin}(H, K)$ ,  $\psi : H \rightarrow \mathbb{C}$  given by  $\psi(a) = 1$  and  $\psi(b) = \xi_4$ , where  $(H = \langle a, b \rangle, K = \langle a \rangle)$  is a Shoda pair in  $G$ . Furthermore,  $H = N_G(K) = \text{Cen}_G(\varepsilon(H, K))$ , but the  $G$ -conjugates of  $\varepsilon(H, K)$  are not orthogonal, so  $(H, K)$  is not a strong Shoda pair.

The output of the function `WedderburnDecompositionInfo(QG)` shows that  $G$  does not have any strongly monomial character of degree 4 and, in particular,  $\chi_6$  is not strongly monomial. This can be seen also as follows. If  $\chi_6 \in \text{Lin}(H_1, K_1)$  with  $(H_1, K_1)$  a strong Shoda pair of  $G$ , then  $[G : H_1] = 4$  and  $x^2 \in Z(G) \subseteq H_1$ . Furthermore, some conjugate of  $H_1$  contains  $a$ , and thus one may assume that  $\langle a, x^2 \rangle \subseteq H_1$ . Now it is easily seen that  $H_1 = H$ . Then  $H'_1 = \langle a \rangle \subseteq K_1$  and therefore  $K_1$  can be  $\langle a \rangle, \langle a, b^2 \rangle$  or  $H$ . But, none of  $(H, \langle a \rangle), (H, \langle a, b^2 \rangle)$  or  $(H, H)$  is a strong Shoda pair of  $G$ .

However,  $(H_2 = \langle a, b^2 \rangle, K_2 = 1)$  is a strong Shoda pair of the subgroup  $M_2 = \langle a, b \rangle$  of  $G$  and this gives rise to a strongly monomial character  $\theta_2$  of  $M_2$  whose field of character values is  $\mathbb{Q}$  and  $(\chi_6|_{M_2}, \theta_2) = 1 \not\equiv 0 \pmod{2}$ . Hence  $\theta_2$  satisfies the conditions required in order to apply Theorem 3. The numerical information associated to this strong Shoda pair of  $M_2$  is

$$[ 1, 6, [ [ 2, 5, 3 ] ], [ ] ]$$

which shows that  $A(\theta_2, \mathbb{Q}) \simeq \mathbb{Q}(\xi_6)(g \mid \xi_6^g = \xi_6^{-1}, g^2 = -1)$ . The center of the algebra is  $\mathbb{Q}(\xi_6 + \xi_6^{-1}) = \mathbb{Q}$  and setting  $i = -1 + 2\xi_6$ , one obtains the generalized quaternion algebra  $A(\theta_2, \mathbb{Q}) \simeq \mathbb{Q}(i, g \mid i^2 = -3, g^2 = -1, ig = -gi) = \left(\frac{-1, -3}{\mathbb{Q}}\right)$ . We conclude that the simple component  $A(\chi_6, \mathbb{Q})$  is similar to the algebra  $\left(\frac{-1, -3}{\mathbb{Q}}\right)$  in  $\text{Br}(\mathbb{Q})$ . The degree of the algebra  $A(\chi_6, \mathbb{Q})$  is 4, given by the degree of the character  $\chi_6$ ; hence  $A(\chi_6, \mathbb{Q}) \simeq \mathcal{M}_2\left(\frac{-1, -3}{\mathbb{Q}}\right)$ .

Now we compute the simple algebras given by the characters  $\chi_7$  and  $\chi_8$ . Note that these characters are in the same orbit of the action of the automorphism group of the complex field; hence we only have to compute the simple algebra corresponding to one of these characters, for instance  $A(\chi_7, \mathbb{Q})$ . In this case the appropriate 2-elementary subgroup of  $G$  is  $M_2 = \langle b, x, y \rangle$  and a strong Shoda pair in

$M_2$  is  $(H_2 = \langle bx \rangle, K_2 = 1)$ , which gives rise to the strongly monomial character  $\theta_2$  of  $M_2$ , that has the field of character values  $\mathbb{Q}(\sqrt{2})$ , so the condition  $\mathbb{Q}(\theta_2) \subseteq L_2 = \mathbb{Q}(\sqrt{2})$  is satisfied. Furthermore,  $(\chi_7|_{M_2}, \theta_2) = 1 \not\equiv 0 \pmod{2}$ ; hence  $\theta_2$  satisfies the required conditions in order to apply Theorem 3. Now the numerical information is

$$[ 1, 8, [ [ 2, 7, 4 ] ], [ ] ]$$

which shows that  $A(\theta_2, \mathbb{Q}) \simeq \mathbb{Q}(\xi_8)(g | \xi_8^g = \xi_8^{-1}, g^2 = -1)$ . The center of the algebra is  $\mathbb{Q}(\xi_8 + \xi_8^{-1}) = \mathbb{Q}(\sqrt{2})$ ; hence  $A(\theta_2, \mathbb{Q}) \simeq \mathbb{H}(\mathbb{Q}(\sqrt{2}))$ , a quaternion algebra over  $\mathbb{Q}(\sqrt{2})$ . The degree of the algebra  $A(\chi_7, \mathbb{Q})$  is 2; hence  $A(\chi_7, \mathbb{Q}) \simeq \mathbb{H}(\mathbb{Q}(\sqrt{2}))$ .

We conclude that  $\mathbb{Q}G \simeq 2\mathbb{Q} \oplus 2\mathcal{M}_3(\mathbb{Q}) \oplus \mathcal{M}_2(\mathbb{Q}) \oplus \mathcal{M}_2\left(\frac{-1, -3}{\mathbb{Q}}\right) \oplus \mathbb{H}(\mathbb{Q}(\sqrt{2}))$ . The Wedderburn decomposition can be obtained at once with the new version of the function `WedderburnDecompositionInfo(QG)` that has the (simplified) output:

$$[ [ 1, 1 ], [ 1, 1 ], [ 1, 6, [ [ 2, 5, 0 ] ] ], [ 3, 1 ], [ 3, 1 ], [ 1, 8, [ [ 2, 7, 4 ] ] ], [ 2, 6, [ [ 2, 5, 3 ] ] ] ]$$

**Example 11.** The following example presents the description of the simple component of a group algebra  $\mathbb{Q}G$  corresponding to an irreducible character of  $G$  for which two primes are involved. Consider the group

$$G = (\langle x, y \rangle \times \langle b \rangle) \rtimes \langle a \rangle,$$

where  $\langle x, y \rangle \simeq Q_8$  is the quaternion group of order 8,  $\langle b \rangle$  is the cyclic group of order 7,  $\langle a \rangle$  is the cyclic group of order 3 and the action of  $\langle a \rangle$  on  $\langle x, y \rangle \times \langle b \rangle$  is given by  $x^a = y, y^a = xy$  and  $b^a = b^2$ .

The group  $G$  has an irreducible character  $\chi$  given by the following table, which contains in the first row a representative of each conjugacy class of  $G$ :

	1	a	a <sup>-1</sup>	ya <sup>-1</sup>	x	x <sup>-1</sup> ya	b	b <sup>-1</sup>	x <sup>2</sup>	xb	xb <sup>-1</sup>	yb	yb <sup>-1</sup>	x <sup>2</sup> b	x <sup>2</sup> b <sup>-1</sup>	xyb	xyb <sup>-1</sup>
$\chi$	6	0	0	0	0	0	$\alpha$	$\bar{\alpha}$	-6	0	0	0	0	$-\alpha$	$-\bar{\alpha}$	0	0

where  $\alpha = 2(\xi_7 + \xi_7^2 + \xi_7^4)$ . The character  $\chi$  is a monomial character induced by the linear character  $\psi \in \text{Lin}(H, K)$  given by  $\psi(x) = \xi_4$  and  $\psi(b) = \xi_7$ , where  $(H = \langle x, b \rangle, K = 1)$  is a Shoda pair in  $G$ . However,  $(H, K)$  is not a strong Shoda pair, because  $H$  is not normal in  $G = N_G(K)$  and in fact  $\chi$  is not strongly monomial.

The field of character values of  $\psi$  is  $\mathbb{Q}(\psi) = \mathbb{Q}(\xi_{4 \cdot 7})$  and the field of character values of the induced character  $\chi$  is  $\mathbb{k} = \mathbb{Q}(\psi^G) = \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{-7})$ . The exponent of the group  $G$  is  $n = 84 = 3 \cdot 4 \cdot 7$ , and the degree of the extension  $[\mathbb{Q}(\xi_n) : \mathbb{Q}]$  is given by  $\phi(n) = 24 = 2^3 \cdot 3$ . Then the prime divisors of the degree of the extension  $[\mathbb{Q}(\xi_n) : \mathbb{k}]$  are 2 and 3. The degree of the character  $\chi$  is 6; hence in order to describe  $A(\chi, \mathbb{Q})$  it is enough to describe its 2-part and 3-part.

Following the proof of the Brauer–Witt theorem, we look for characters in strongly monomial subgroups of  $G$  for the primes 2 and 3. If there exists such a character  $\theta$  on a subgroup  $M$  such that  $(\chi, \theta^G)$  is coprime with 6 and  $\mathbb{Q}(\theta) \subseteq \mathbb{k}$ , then by Proposition 3,  $[A(\chi, \mathbb{Q})] = [A(\theta, \mathbb{Q})]$ . However, a computer search has shown that such a  $\theta$  and  $M$  do not exist. The unique strongly monomial character  $\theta$  of a subgroup  $M$  such that the product  $(\chi, \theta^G)$  is coprime to 6 can be obtained with  $M = \langle x, b \rangle$ , but then the character field of  $\theta$  is  $\mathbb{Q}(\xi_{28})$ , which is not included in  $\mathbb{k} = \mathbb{Q}(\sqrt{-7})$ . Therefore, one has to deal with both primes separately.

First we study the 2-part  $[A(\chi, k)]_2$ . The 2'-splitting field is  $L_2 = \mathbb{Q}(\xi_7)$ , the appropriate strongly monomial subgroup of  $G$  is  $M_2 = \langle x, y \rangle \times \langle b \rangle$  and a strong Shoda pair in  $M_2$  is  $(H_2 = \langle x, b \rangle, K_2 = 1)$ , which gives rise to the strongly monomial

character  $\theta_2$  of  $M_2$  with  $\mathbb{Q}(\theta_2) = \mathbb{Q}(\xi_7)$  and  $(\chi|_{M_2}, \theta_2) = 1 \not\equiv 0 \pmod{2}$ . The numerical information associated to the strong Shoda pair  $(H_2, K_2)$  of the subgroup  $M_2$  is

$$[ 1, 28, [ [ 2, 15, 14 ] ], [ ] ]$$

which gives the simple algebra  $A_2 \simeq \mathbb{Q}(\xi_{28})(g \mid \xi_{28}^g = \xi_{28}^{15}, g^2 = -1)$ . The center of  $A_2$  is  $\mathbb{Q}(\xi_7)$  and  $A_2 = \mathbb{Q}(\xi_7)(i, g \mid i^2 = g^2 = -1, ig = -gi) = \left( \frac{-1, -1}{\mathbb{Q}(\xi_7)} \right) = \mathbb{H}(\mathbb{Q}(\xi_7))$ , which is a division algebra. According to Proposition 1 and Proposition 3, the algebra  $A_2$  is isomorphic to the simple component  $A(\theta_2, L_2)$  over  $L_2$  and it is similar to the algebra  $A(\chi, L_2)$  in the Brauer group  $\text{Br}(L_2)$ .

The algebra  $A_2$  can be described as a cyclotomic algebra over  $L_2$  in the following form:  $A_2 \simeq \mathbb{k}(\xi_{28}) *_{\tau_2} \text{Gal}(\mathbb{k}(\xi_{28})/L_2) = (\mathbb{Q}(\xi_{28})/\mathbb{Q}(\xi_7), \tau_2)$ , where  $\tau_2$  is the 2-cocycle in  $Z^2(\text{Gal}(\mathbb{Q}(\xi_{28})/\mathbb{Q}(\xi_7)), \mathbb{Q}(\xi_{28})^*)$  given by  $\tau_2(h, h) = -1$ , where  $H = \text{Gal}(\mathbb{Q}(\xi_{28})/\mathbb{Q}(\xi_7)) = \langle h \rangle \simeq C_2$  and  $\tau_2(h_1, h_2) = 1$  if  $(h_1, h_2) \neq (h, h)$ . Then  $\text{Gal}(\mathbb{Q}(\xi_{28})/\mathbb{Q}(\sqrt{-7})) = \langle g \rangle \simeq C_6$  with  $g^3 = h$ , and using formula (5) one obtains  $(\text{Cor}_{L_2 \rightarrow \mathbb{k}}(\tau_2))(g_1, g_2) = -1$  if  $g_1, g_2 \in \{g^3, g^4, g^5\}$  and  $(\text{Cor}_{L_2 \rightarrow \mathbb{k}}(\tau_2))(g_1, g_2) = 1$  otherwise. The integers  $\alpha$  and  $a$  from step (3)(e) of Algorithm 1 are in this case 1 and the searched 2-cocycle is  $\tau'_2 = \text{Cor}_{L_2 \rightarrow \mathbb{k}}(\tau_2)$ .

The corresponding algebra is  $\mathbb{Q}(\xi_{28})(g \mid \xi_{28}^g = \xi_{28}^r, g^6 = -1)$ , where  $r \equiv 2 \pmod{7}$  and  $r \equiv 3 \pmod{4}$ . Hence  $r = -5$ . The center of this algebra is  $\mathbb{Q}(\sqrt{-7})$  and, setting  $i = \xi_{28}^7$  and  $j = g^3$ , we obtain  $\mathbb{Q}(\sqrt{-7})(i, j \mid i^2 = j^2 = -1, ij = -ji)$ , that is, the quaternion algebra  $\mathbb{H}(\mathbb{Q}(\sqrt{-7}))$ . So, the 2-part  $[A(\chi, k)]_2$  over  $\mathbb{k} = \mathbb{Q}(\sqrt{-7})$  is the class of  $\mathbb{H}(\mathbb{Q}(\sqrt{-7}))$ , which is a division algebra because it is contained in  $\mathbb{H}(\mathbb{Q}(\xi_7))$ .

Notice that since  $[\mathbb{Q}(\xi_7) : \mathbb{Q}(\sqrt{-7})] = 3$  and  $(2, 3) = 1$ , the restriction  $\text{Res}_{\mathbb{k} \rightarrow L_2}$  is injective on the 2-part [Yam, Lemma 3.7], and because  $\text{Res}_{\mathbb{k} \rightarrow L_2}([\mathbb{H}(\mathbb{Q}(\sqrt{-7}))]) = [\mathbb{H}(\mathbb{Q}(\xi_7))]$ , one can deduce that  $[A(\chi, k)]_2$  is  $[\mathbb{H}(\mathbb{Q}(\sqrt{-7}))]$  and can avoid the use of the corestriction in this case.

Now we compute the 3-part  $[A(\chi, \mathbb{Q})]_3$ . The 3'-splitting field is  $L_3 = \mathbb{k}(\xi_3 \cdot \xi_4) = \mathbb{Q}(\sqrt{-7}, i, \xi_3)$ , the appropriate strongly monomial subgroup is  $M_3 = \langle x^2, b \rangle \rtimes \langle a \rangle$  and a strong Shoda pair in  $M_3$  is  $(H_3 = \langle x^2, b \rangle, K_3 = 1)$ , which gives rise to the strongly monomial character  $\theta_3$  that satisfies the conditions  $\mathbb{Q}(\theta_3) = \mathbb{Q}(\sqrt{-7}) \subseteq L_3$  and  $(\chi|_{M_3}, \theta_3) = 2 \not\equiv 0 \pmod{3}$ . The numerical information corresponding to  $(H_3, K_3)$  is

$$[ 1, 14, [ [ 3, 9, 0 ] ], [ ] ]$$

which gives the simple algebra  $A_3 \simeq \mathbb{Q}(\xi_{14})(g \mid \xi_{14}^g = \xi_{14}^9, g^3 = 1)$ . The center of  $A_3$  is  $\mathbb{Q}(\sqrt{-7}) = \mathbb{k}$ ; hence  $A_3 \simeq \mathcal{M}_3(\mathbb{Q}(\sqrt{-7}))$ . Notice that in this case we do not have to use the corestriction because the center of  $A_3$  is already  $\mathbb{k}$ ; hence  $[A(\psi^G, k)]_3 = [\mathcal{M}_3(\mathbb{Q}(\sqrt{-7}))] = [\mathbb{Q}(\sqrt{-7})]$ .

The tensor product over  $\mathbb{Q}(\sqrt{-7})$  of the 2-part and the 3-part gives the simple algebra  $A(\chi, \mathbb{Q})$  as a similar algebra to  $\mathbb{H}(\mathbb{Q}(\sqrt{-7})) \otimes_{\mathbb{Q}(\sqrt{-7})} \mathbb{Q}(\sqrt{-7}) \simeq \mathbb{H}(\mathbb{Q}(\sqrt{-7}))$ . The degree of the simple algebra  $A(\chi, \mathbb{Q})$  is 6, the degree of the character  $\chi$ ; hence  $A(\chi, \mathbb{Q}) \simeq \mathcal{M}_3(\mathbb{H}(\mathbb{Q}(\sqrt{-7})))$ .

*Remark 12.* Notice that the size of the matrix  $B_\chi$  in step (3)(b) of Algorithm 2 is a rational number rather than an integer. The group of smallest order for which this phenomenon occurs is the group [240, 89] in the library of the GAP system. Although this does not make literal sense, still the algorithm provides a lot of

information on the Wedderburn decomposition. This example shows how one can use this information. Let  $G$  be the mentioned group. Then the output of Algorithm 2 applied to  $\mathbb{Q}G$  provides the following numerical information for one of the simple factors of  $\mathbb{Q}G$ :

$$[ 3/4, 40, [ [ 4, 17, 20 ] , [ 2, 31, 0 ] ], [ [ 0 ] ] ].$$

Notice that the first entry of this 4-tuple is not an integer, and a formal presentation of the corresponding simple algebra is given by

$$A \simeq \mathcal{M}_{3/4}(\mathbb{Q}(\xi_{40})(g, h | \xi_{40}^g = \xi_{40}^{17}, \xi_{40}^h = \xi_{40}^{31}, g^4 = -1, h^2 = 1, gh = hg)).$$

Denote  $A = \mathcal{M}_{3/4}(B)$ . The center of the algebra  $B$  is  $\mathbb{Q}(\sqrt{2})$  and the algebras  $\mathbb{Q}(\xi_8)(h | \xi_8^h = \xi_8^{-1}, h^2 = 1) \simeq M_2(\mathbb{Q}(\sqrt{2}))$  and  $\mathbb{Q}(\xi_5)(g | \xi_5^g = \xi_5^2, g^4 = -1)$  are simple algebras in  $B$ . Furthermore,

$$\begin{aligned} B &= M_2(\mathbb{Q}(\sqrt{2})) \otimes_{\mathbb{Q}(\sqrt{2})} (\mathbb{Q}(\sqrt{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\xi_5)(g | \xi_5^g = \xi_5^2, g^4 = -1)) \\ &= M_2(\mathbb{Q}(\sqrt{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\xi_5)(g | \xi_5^g = \xi_5^2, g^4 = -1)). \end{aligned}$$

Hence, we can describe the algebra  $A$  as

$$M_{3/2}(\mathbb{Q}(\sqrt{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\xi_5)(g | \xi_5^g = \xi_5^2, g^4 = -1)),$$

and we conclude that the algebra  $A$  is isomorphic to either  $\mathcal{M}_3(D)$  for some division quaternion algebra over  $\mathbb{Q}(\sqrt{2})$  or to  $\mathcal{M}_6(\mathbb{Q}(\sqrt{2}))$ . To decide which one of these options is the correct one, one should compute the Schur index of the algebra  $\mathbb{Q}(\sqrt{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\xi_5)(g | \xi_5^g = \xi_5^2, g^4 = -1)$ . This can be done using local field theory, but this is out of the range for the methods of this paper.

#### ACKNOWLEDGMENTS

We thank Eli Aljadeff, Andrei Marcus and Juan Jacobo Simón for many helpful conversations.

#### REFERENCES

- [Bro-Kon-Oli-Olt-Río] O. Broche Cristo, A. Konovalov, A. Olivieri, G. Olteanu and Á. del Río, *Wedderga – Wedderburn Decomposition of Group Algebras, Version 4.0*; 2006 (<http://www.um.es/adelrio/wedderga.htm>).
- [Bro-Río] O. Broche Cristo and Á. del Río, *Wedderburn decomposition of finite group algebras*, *Finite Fields Appl.* **13** (2007), 71–79.
- [Cur-Rei] Ch.W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Wiley-Interscience, New York, 1962. MR0144979 (26:2519)
- [GAP] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4*; 2006, (<http://www.gap-system.org>).
- [Her96] A. Herman, *A constructive Brauer-Witt theorem for certain solvable groups*, *Canad. J. Math.* **48** (1996), No. 6, 1196–1209. MR1426900 (97j:20006)
- [Her97] A. Herman, *On the automorphism group of rational group algebras of metacyclic groups*, *Comm. Algebra*, **25** (1997), No. 7, 2085–2097. MR1451679 (98g:16022)
- [Her03] A. Herman, *Using  $G$ -algebras for Schur index computation*, *J. Algebra* **260** (2003), No. 2, 463–475. MR1967308 (2004f:20022)
- [Jes-Lea] E. Jespers and G. Leal, *Generators of large subgroups of the unit group of integral group rings*, *Manuscripta Math.* **78** (1993), 303–315. MR1206159 (94f:20010)

- [Jes-Lea-Paq] E. Jespers, G. Leal and A. Paques, *Central idempotents in rational group algebras of finite nilpotent groups*, J. Algebra Appl. **2** (2003), No. 1, 57–62. MR1964765 (2004b:20009)
- [Jes-Río] E. Jespers and Á. del Río, *A structure theorem for the unit group of the integral group ring of some finite groups*, J. Reine Angew. Math., **521** (2000), 99–117. MR1752297 (2001a:16054)
- [Oli-Río] A.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. MR1981041 (2004k:16073)
- [Oli-Río-Sim04] A.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. MR2100373 (2005i:16054)
- [Oli-Río-Sim06] A.A. Olivieri, Á. del Río and J. J. Simón *The group of automorphisms of a rational group algebra of a finite metacyclic group*, Comm. Algebra **34** (2006), no. 10, 3543–3567.
- [Pas] D.S. Passman, *Infinite Crossed Products*, Pure and Applied Mathematics, **135**, Academic Press, Inc., Boston, MA, 1989. MR979094 (90g:16002)
- [Pie] R.S. Pierce, *Associative Algebras*, Graduate Texts in Mathematics, **88**, Springer-Verlag, 1982. MR674652 (84c:16001)
- [Ple-Huf] V.S. Pless and W.C. Huffman, *Handbook of Coding Theory*, Elsevier, New York, 1998.
- [Rei] I. Reiner, *Maximal orders*, London Mathematical Society Monographs. New Series, **28**, The Clarendon Press, Oxford, 2003. MR1972204 (2004c:16026)
- [Río-Rui] Á. del Río and M. Ruiz, *Computing large direct products of free groups in integral group rings*, Comm. Algebra, **30**, (2002), No. 4, 1751–1767. MR1894041 (2003a:20007)
- [Rit-Seh] J. Ritter and S.K. Sehgal, *Construction of units in integral group rings of finite nilpotent groups*, Trans. Amer. Math. Soc. **324**, (1991), 603–621. MR987166 (91h:20008)
- [Seh] S.K. Sehgal, *Units of integral group rings*, Longman Scientific and Technical Essex, 1993.
- [Shi] M. Shirvani, *The structure of simple rings generated by finite metabelian groups*, J. Algebra **169** (1994), No. 3, 686–712. MR1302112 (95i:20005)
- [Spi] K. Spindler, *Abstract algebra with applications*, Vol. II. Rings and Fields, Marcel Dekker, Inc., New York, 1994. MR1243417 (94i:00002b)
- [Wei] E. Weiss, *Cohomology of Groups*, Pure and Applied Mathematics, **34**, Academic Press, New York-London, 1969. MR0263900 (41:8499)
- [Yam] T. Yamada, *The Schur Subgroup of the Brauer Group*, Lecture Notes in Math., **397**, Springer-Verlag, 1974. MR0347957 (50:456)

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, NORTH UNIVERSITY OF BAIÁ MARE, VICTORIEI 76, 430072 BAIÁ MARE, ROMANIA.

*Current address:* Department of Mathematics, University of Murcia, 30100 Murcia, Spain.

*E-mail address:* golteanu@um.es, olteanu@math.ubbcluj.ro