RATIONAL GROUP ALGEBRAS OF FINITE GROUPS: FROM IDEMPOTENTS TO UNITS OF INTEGRAL GROUP RINGS

ERIC JESPERS, GABRIELA OLTEANU, AND ÁNGEL DEL RÍO

Abstract. We give an explicit and character-free construction of a complete set of orthogonal primitive idempotents of a rational group algebra of a finite nilpotent group and a full description of the Wedderburn decomposition of such algebras. An immediate consequence is a well-known result of Roquette on the Schur indices of the simple components of group algebras of finite nilpotent groups. As an application, we obtain that the unit group of the integral group ring $\mathbb{Z}G$ of a finite nilpotent group G has a subgroup of finite index that is generated by three nilpotent groups for which we have an explicit description of their generators. Another application is a new construction of free subgroups in the unit group. In all the constructions dealt with, pairs of subgroups (H, K), called strong Shoda pairs, and explicit constructed central elements $e(G, H, K)$ play a crucial role. For arbitrary finite groups we prove that the primitive central idempotents of the rational group algebras are rational linear combinations of such $e(G, H, K)$, with (H, K) strong Shoda pairs in subgroups of G.

1. Introduction

The investigation of the unit group $\mathcal{U}(\mathbb{Z}G)$ of the integral group ring $\mathbb{Z}G$ of a finite group G has a long history and goes back to work of Higman [Hig] and Brauer [Bra]. One of the reasons for the importance of the integral group ring $\mathbb{Z}G$ is that it is an algebraic tool that links group and ring theory. It was anticipated for a long time that the defining group G would be determined by its integral group ring, i.e. if $\mathbb{Z}G$ is isomorphic with $\mathbb{Z}H$ for some finite group H then $G \cong H$, the isomorphism problem. Roggenkamp and Scott [RS] showed that this indeed is the case if G is a nilpotent group. Weiss proved a more general result [Wei], which also confirmed a Zassenhaus conjecture. It was a surprise when Hertweck [Her] gave a counter example to the isomorphism problem. In all these investigations the unit group $\mathcal{U}(\mathbb{Z}G)$ of $\mathbb{Z}G$ is of fundamental importance. There is a vast literature on the topic. For a survey up to 1994, the reader is referred to the books of Passman and Sehgal [Pas, Seh1, Seh2]. Amongst many others, during the past 15 years, the following problems have received a lot of attention (we include some guiding references): construction of generators for a subgroup of finite index in $\mathcal{U}(\mathbb{Z}G)$ [RS1, RS2, JL1], construction of free subgroups [HP, MS2], structure theorems for $\mathcal{U}(\mathbb{Z}G)$ for some classes of groups G [JPdRRZ].

Essential in these investigations is to consider $\mathbb{Z}G$ as a $\mathbb{Z}$-order in the rational group algebra $\mathbb{Q}G$ and to have a detailed understanding of the Wedderburn decomposition of $\mathbb{Q}G$. To do so, a first important step is to calculate the primitive central idempotents of $\mathbb{Q}G$. A classical method for

2000 *Mathematics Subject Classification.* 20C05, 16S34, 16U60.

Key words and phrases. Idempotents, Group algebras, Group rings, Units.

Research partially supported by Onderzoeksraad of Vrije Universiteit Brussel, Fonds voor Wetenschappelijk Onderzoek (Flanders), IWOIB-Instituut ter bevordering van het wetenschappelijk onderzoek en de innovatie van Brussel (Belgium), the grant PN-II-RU-TE-2009-1 project ID_303, Ministerio de Ciencia y Tecnología of Spain and Fundación Séneca of Murcia.

this is to apply Galois descent on the primitive central idempotents of the complex group algebra $\mathbb{C}G$. The latter idempotents are the elements of the form $e(\chi) = \frac{\chi(1)}{|G|}\sum_{g\in G}\chi(g^{-1})g$, where χ runs through the irreducible (complex) characters χ of G. Hence the primitive central idempotents of $\mathbb{Q}G$ are the elements of the form $\sum_{\sigma\in \mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})} e(\sigma\circ\chi)$ (see for example [Yam]). Rather recently, Olivieri, del Río and Simón [OdRS1] obtained a character free method to describe the primitive central idempotents of $\mathbb{Q}G$ provided G is a monomial group, that is, every irreducible character of G is induced from a linear character of a subgroup of G. The new method relies on a theorem of Shoda on pairs of subgroups (H, K) of G with K normal in H, H/K abelian and so that an irreducible linear character of H with kernel K induces an irreducible character of G. Such pairs are called Shoda pairs of G. In Section 2 we recall the necessary background and explain the description of the primitive central idempotents of $\mathbb{Q}G$. It turns out that these idempotents can be built using the central elements $e(G, H, K)$ (see Section 2 for the definition) with (H, K) a Shoda pair of G. In case the Shoda pair satisfies some extra conditions (one calls such a pair a strong Shoda pair) then one also obtains a detailed description of the Wedderburn component associated with the central idempotent. This is an important second step towards a description of the simple components of $\mathbb{Q}G$. This method is applicable to all abelian-by-supersolvable finite groups, in particular to finite nilpotent groups.

For arbitrary finite groups G, it remains an open problem to give a character free description of the primitive central idempotents of $\mathbb{Q}G$. Only for very few groups that are not monomial, such a description has been obtained (see for example [GJ] for alternating groups). In section 3 we show that for arbitrary finite groups G the elements $e(G, H, K)$ are building blocks for the construction of the primitive central idempotents e of $\mathbb{Q}G$, i.e. every such e is a rational linear combination of $e(G, H, K)$, where (H, K) runs through strong Shoda pairs in subgroups of G. The proof makes fundamental use of Brauer's Theorem on Induced Characters. Presently we are unable to control the rational coefficients in this linear combination.

In case G is an abelian-by-supersolvable finite group, then, as mentioned above, the primitive central idempotents of $\mathbb{Q}G$ are of the form $e(G, H, K)$, with (H, K) a strong Shoda pair of G and the simple component $\mathbb{Q}Ge(G, H, K)$ is described. For nilpotent groups G we will show to have a much better and detailed control. Indeed, in Section 4 we describe a complete set of matrix units (in particular, a complete set of orthogonal primitive idempotents) of $\mathbb{Q}Ge(G, H, K)$; a third step in the description of $\mathbb{Q}G$. This allows us to give concrete representations of the projections ge of the group elements $g \in G$ as matrices over division rings. As a consequence, the recognition of the $\mathbb{Z}$-order $\mathbb{Z}G$ in the Wedderburn description of $\mathbb{Q}G$ is reduced to a linear algebra problem over the integers. We include some examples to show that the method can not be extended to, for example, finite metacyclic groups. It remains a challenge to construct a complete set of primitive idempotents for such groups.

In Section 5, we give several applications to the unit group $\mathcal{U}(\mathbb{Z}G)$ for G a finite nilpotent group. First we show that if G is a finite nilpotent group such that $\mathbb{Q}G$ has no exceptional components (see Section 5 for the definition) then $\mathcal{U}(\mathbb{Z}G)$ has a subgroup of finite index that is generated by three nilpotent finitely generated groups of which we give explicit generators. The problem of describing explicitly a finite set of generators for a subgroup of finite index in $\mathcal{U}(\mathbb{Z}G)$ has been investigated in a long series of papers. Bass and Milnor did this for abelian groups [Bas], the case of nilpotent groups so that their rational group algebra has no exceptional components was done by Ritter and Sehgal [RS1, RS2], arbitrary finite groups so that their rational group algebra has no exceptional components were dealt with by Jespers-Leal [JL1]. It was shown that the Bass cyclic units together with the bicyclic units generate a subgroup of finite index. Some cases

with exceptional components have also been considered, see for example [GS, Jes, JL2, Seh3]). In general, very little is known on the structure of the group generated by the Bass cyclic units and the bicyclic units, except that "often" two of them generate a free group of rank two (see for example [GP, GdR, Jes, JdRR, MS2, JL3]). In this paper, for G a finite nilpotent group, we not only give new generators for a subgroup of finite index, but more importantly, the generating set is divided into three subsets, one of them generating a subgroup of finite index in the central units and each of the other two generates a nilpotent group. One other advantage of our method with respect to the proofs and results given in [JL1, RS1, RS2] is that our proofs are (modulo the central units) more direct and constructive to obtain an explicit set of generators for a subgroup of finite index in the group of units of the integral group ring of a finite nilpotent group. Furthermore, we also give new explicit constructions of free subgroups of rank two.

2. Preliminaries

We introduce some useful notation and results, mainly from [JLP] and [OdRS1]. Throughout G is a finite group. If H is a subgroup of a group G, then let $\widehat{H} = \frac{1}{|H|}\sum_{h\in H} h \in \mathbb{Q}G$. For $g \in G$, let $\widehat{g} = \widehat{\langle g\rangle}$ and for non-trivial G, let $\varepsilon(G) = \prod(1 - \widehat{M})$, where M runs through the set of all minimal normal nontrivial subgroups of G. Clearly, $\widehat{H}$ is an idempotent of $\mathbb{Q}G$ which is central if and only if H is normal in G. If $K \lhd H \leq G$ 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. We extend this notation by setting $\varepsilon(K,K) = \widehat{K}$. Clearly $\varepsilon(H,K)$ is an idempotent of the group algebra $\mathbb{Q}G$. Let $e(G,H,K)$ be the sum of the distinct G-conjugates of $\varepsilon(H,K)$, that is, if T is a right transversal of $\mathrm{Cen}_G(\varepsilon(H,K))$ in G, then

$$e(G,H,K) = \sum_{t\in T} \varepsilon(H,K)^t,$$

where $\alpha^g = g^{-1}\alpha g$ for $\alpha \in \mathbb{C}G$ and $g \in G$. 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 a finite group G is a pair (H,K) of subgroups of G with the properties that $K \trianglelefteq H$, H/K is cyclic, and if $g \in G$ and $[H,g] \cap H \subseteq K$ then $g \in H$. 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. We also have, in this case, that $\mathrm{Cen}_G(\varepsilon(H,K)) = N_G(K)$ and H/K is a maximal abelian subgroup of $N_G(K)/K$ [OdRS1].

If χ is a monomial character of G then $\chi = \psi^G$, the induced character of a linear character ψ of a subgroup H of G. By a Theorem of Shoda, a monomial character $\chi = \psi^G$ as above is irreducible if and only if $(H, \mathrm{Ker}\ \psi)$ is a Shoda pair (see [Sho] or [CR, Corollary 45.4]). A strongly monomial character is a monomial character $\chi = \psi^G$ as before with $(H, \mathrm{Ker}\ \psi)$ a strong Shoda pair. 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 (see [Hup, Theorem 24.3]) and in [OdRS1] it is proved that it is even strongly monomial. We will use these results in order to study the primitive idempotents of group algebras for some abelian-by-supersolvable groups, including finite nilpotent groups. We will also use the following description of the simple component associated to a strong Shoda pair.

Theorem 2.1. [OdRS1, Proposition 3.4] *If (H, K) is a strong Shoda pair of G then*

$$\mathbb{Q}Ge(G, H, K) \cong M_r(\mathbb{Q}N\varepsilon(H, K)) \cong M_r(\mathbb{Q}(\zeta_m) *_\tau^\alpha N/H),$$

where

$$m = [H : K], \quad N = N_G(K), \quad r = [G : N]$$

and the action α and twisting τ are given by

$$\alpha(nH)(\zeta_m) = \zeta_m^i, \quad \tau(nH, n'H) = \zeta_m^j,$$

if $n^{-1}hnK = h^iK$ and $[n, n']K = h^jK$, for hK a generator of H/K, $n, n' \in N$ and $i, j \in \mathbb{Z}$.

In the above theorem, ζ_m denotes a primitive m-th root of unity and we have used the notation $L *_\tau^\alpha G$, for L a field and G a group, to denote a crossed product with action $\alpha : G \to \mathrm{Aut}(L)$ and twisting $\tau : G \times G \to L^*$ [Pas], i.e. $L *_\tau^\alpha G$ is the associative ring $\bigoplus_{g\in G} Lu_g$ with multiplication given by the following rules:

$$u_g a = \alpha_g(a)u_g, \quad u_g u_h = \tau(g, h)u_{gh}.$$

If the action of G on L is faithful then one may identify G with a group of automorphisms of L and the center of $L *_\tau^\alpha G$ is the fixed subfield $F = L^G$, so that $G = \mathrm{Gal(L/F)}$, and this crossed product is usually denoted by $(L/F, \tau)$ [Rei]. We refer to these crossed products as classical crossed products. This is the case for the crossed product $\mathbb{Q}N\varepsilon(H, K)) \cong \mathbb{Q}(\zeta_m) *_\tau^\alpha N/H$ in Theorem 2.1 which can be described as $(\mathbb{Q}(\zeta_m)/F, \tau)$, where F is the center of the algebra, which is determined by the Galois action given in Theorem 2.1.

3. Primitive central idempotents

For an irreducible character χ of G and a field F of characteristic 0, $e_F(\chi)$ denotes the only primitive central idempotent of FG such that $\chi(e) \neq 0$. In this section, using Brauer's Theorem on Induced Characters, we give a description of every primitive central idempotent $e_\mathbb{Q}(\chi)$ of a rational group algebra $\mathbb{Q}G$ corresponding to an irreducible character χ of a finite group G as a rational linear combination of elements of the form $e(G, H_i, K_i)$, with each (H_i, K_i) a strong Shoda pair in a subgroup of G, or equivalently, K_i is a normal subgroup of H_i with H_i/K_i cyclic.

Theorem 3.1 (Brauer)**.** [Bra] *Every complex character χ of a finite group G is a $\mathbb{Z}$–linear combination $\chi = \sum_i a_i\theta_i^G$, $a_i \in \mathbb{Z}$, of characters induced from linear characters θ_i of elementary subgroups M_i of G, where by an elementary subgroup of G we mean one which is a direct product of a cyclic group and a p-group for some prime p.*

In particular, the M_i's are cyclic–by–p_i-groups for some primes p_i, hence by [OdRS1] each M_i is strongly monomial. As a consequence, every irreducible character of such a subgroup M_i is an induced character $\theta_i^{M_i}$ from a linear character θ_i of a subgroup H_i of M_i. So, $\theta_i^{M_i}$ is irreducible and $(H_i, \ker(\theta_i))$ is a strong Shoda pair of M_i.

We also will use the result [OdRS1, Theorem 2.1.] that describes the primitive central idempotents $e_\mathbb{Q}(\psi^G)$ of a rational group algebra $\mathbb{Q}G$ associated to a monomial irreducible character ψ^G as

$$e_\mathbb{Q}(\psi^G) = \frac{[\mathrm{Cen}_G(\varepsilon(H, K)) : H]}{[\mathbb{Q}(\psi) : \mathbb{Q}(\psi^G)]} e(G, H, K) \tag{1}$$

where ψ is a linear character of the subgroup H of G and K is the kernel of ψ.

Proposition 3.2. *Let G be a finite group of order n and χ an irreducible character of G. Then the primitive central idempotent $e_{\mathbb{Q}}(\chi)$ of $\mathbb{Q}G$ associated to χ is of the form*

$$e_{\mathbb{Q}}(\chi) = \frac{\chi(1)}{[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\chi)]} \sum_i \frac{a_i}{[G : C_i]} [\mathbb{Q}(\zeta_n) : \mathbb{Q}(\psi_i)] e(G, H_i, K_i)$$

where $a_i \in \mathbb{Z}$, (H_i, K_i) are strong Shoda pairs of subgroups of G (equivalently H_i/K_i is a cyclic section of G), $C_i = \mathrm{Cen}_G(\varepsilon(H_i, K_i))$ and ψ_i are linear characters of H_i with kernel K_i.

Proof. As it was mentioned in the introduction, for every $\chi \in \mathrm{Irr}(G)$, we have

$$e_{\mathbb{Q}}(\chi) = \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})} e(\chi^\sigma) = \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})} \sigma(e(\chi)) = \mathrm{tr}_{\mathbb{Q}(\chi)/\mathbb{Q}}(e(\chi)),$$

where χ^σ is the character of G given by $\chi^\sigma(g) = \sigma(\chi(g))$, for $g \in G$. The interpretation of $e_{\mathbb{Q}}(\chi)$ as a trace, suggests the following useful notation for the next arguments. For any finite Galois extension F of $\mathbb{Q}$ containing $\mathbb{Q}(\chi)$, let

$$e_{\mathbb{Q}}^F = \sum_{\sigma \in \mathrm{Gal}(F/\mathbb{Q})} \sigma(e(\chi)) = \mathrm{tr}_{F/\mathbb{Q}}(e(\chi)).$$

Hence $e_{\mathbb{Q}}(\chi) = e_{\mathbb{Q}}^{\mathbb{Q}(\chi)}(\chi) = \frac{1}{[F:\mathbb{Q}(\chi)]}(e_{\mathbb{Q}}^F(\chi))$ for every finite Galois extension F of $\mathbb{Q}(\chi)$. Using Brauer's Theorem on Induced Characters, we now may write $\chi = \sum_i a_i \psi_i^G$, with ψ_i linear characters of elementary subgroups H_i with kernel K_i and $a_i \in \mathbb{Z}$. Then

$$e_{\mathbb{Q}}^{\mathbb{Q}(\zeta_n)}(\chi) = \chi(1) \sum_i \frac{a_i}{[G : H_i]} e_{\mathbb{Q}}^{\mathbb{Q}(\zeta_n)}(\psi_i^G)$$

and, for every i, we will compute $e_{\mathbb{Q}}^{\mathbb{Q}(\zeta_n)}(\psi_i^G)$, as in the proof of [OdRS1, Proposition 2.1]. (Note that $\mathbb{Q}(\zeta_n)$ contains $\mathbb{Q}(\chi)$, because it is a splitting field of G.)

Put $e_i = e(\psi_i)$. We know that $\mathcal{A} = \mathrm{Aut}(\mathbb{C})$ acts on the left and G acts on the right on ψ_i and on e_i (by composition and by conjugation respectively) and that their actions are compatible. Hence one may consider $\mathcal{A} \times G$ acting on the left on the set of irreducible characters of subgroups of G (and similarly on the e_i's) by $(\sigma, g) \cdot \psi_i = \sigma \cdot \psi_i \cdot g^{-1}$.

Let $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \{\sigma_1, \ldots, \sigma_l\}$ and $T_i = \{g_1, \ldots, g_m\}$ a right transversal of H_i in G. Denote by $C_i = \mathrm{Cen}_G(\varepsilon(H_i, K_i))$. We have that $\sum_{k=1}^m e_i \cdot g_k = e(\psi_i^G)$, hence

$$\begin{aligned} e_{\mathbb{Q}}^{\mathbb{Q}(\zeta_n)}(\psi_i^G) &= \sum_{j=1}^{l} \sigma_j e(\psi_i^G) = \sum_{j=1}^{l} \sum_{k=1}^{m} \sigma_j e_i \cdot g_k = \sum_{k=1}^{m} \mathrm{tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(e_i) \cdot g_k \\ &= \sum_{k=1}^{m} [\mathbb{Q}(\zeta_n) : \mathbb{Q}(\psi_i)] \mathrm{tr}_{\mathbb{Q}(\psi_i)/\mathbb{Q}}(e_i) \cdot g_k = \sum_{k=1}^{m} [\mathbb{Q}(\zeta_n) : \mathbb{Q}(\psi_i)] \varepsilon(H_i, K_i)^{g_k} \\ &= [\mathbb{Q}(\zeta_n) : \mathbb{Q}(\psi_i)][C_i : H_i] e(G, H_i, K_i) \end{aligned}$$

The above computations now easily yield the desired formula for $e_{\mathbb{Q}}(\chi)$. □

Remark 3.3. Notice that the formula from Proposition 3.2 for the computation of the primitive central idempotents $e_{\mathbb{Q}}(\chi)$ of $\mathbb{Q}G$ associated to an irreducible character χ of G coincides with formula (1) in case χ is a monomial irreducible character of G, that is χ is induced to G from only one linear character ψ of a subgroup H, with kernel K such that (H, K) is a Shoda pair of G.

In general, as seen in Proposition 3.2, one has to consider all strong Shoda pairs in subgroups of G that contribute to the description of a primitive central idempotent of $\mathbb{Q}G$. However, one

can reduce the search of the Shoda pairs that determine the primitive central idempotents of $\mathbb{Q}G$ to representatives given by a relation between such pairs of subgroups. Indeed, in [OdRS2, Proposition 1.4], it is proved that if (H_1, K_1) and (H_2, K_2) are two Shoda pairs of a finite group G and $\alpha_1, \alpha_2 \in \mathbb{Q}$ are such that $e_i = \alpha_i e(G, H_i, K_i)$ 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 $H_1^g \cap K_2 = K_1^g \cap H_2$.

Remark 3.4. We would like to be able to give a bound for the integers a_i used in the previous proposition and one would also like to give more information on the pairs of groups (H_i, K_i) that one has to consider in the description of $e_{\mathbb{Q}}(\chi)$.

Notice that for monomial (respectively strongly monomial) groups, all primitive central idempotents are realized as elements of the form $\alpha e(G, H, K)$, with $\alpha \in \mathbb{Q}$, for some Shoda pair (H, K) (respectively strong Shoda pair and $\alpha = 1$) in G. However, for the smallest non-monomial group, which is $\mathrm{SL}(2, 3)$, this is not true any more. Indeed, in [OdRS1, Example 5.7], the two primitive central idempotents corresponding to the non-monomial characters are $e_1 = \frac{1}{2}e(G, B, A)$, and $e_2 = \frac{1}{4}e(G, B, 1) - \frac{1}{4}e(G, B, A)$, with $G = \langle x, y\rangle \rtimes \langle a\rangle$, a semidirect product of the quaternion group $\langle x, y\rangle$ of order 8 by the cyclic group $A = \langle a\rangle$ of order 3, and with $B = \langle x^2 a\rangle$. However, e_2 can not be written as a rational linear multiple of some $e(G, H, K)$ with (H, K) a pair of subgroups of G such that $K \trianglelefteq H$.

4. Primitive idempotents for finite nilpotent groups

We start this section by showing a method to produce a complete set of orthogonal primitive idempotents of a classical crossed product with trivial twisting $\tau = 1$, i.e. $\tau(g, h) = 1$, for every $g, h \in G$. Let L be a field of characteristic zero. Observe that $(L/F, 1) \simeq M_n(F)$, with $n = [L : F]$, therefore a complete set of orthogonal primitive idempotents of $(L/F, 1)$ contains n idempotents.

Lemma 4.1. *Let $A = (L/F, 1)$ be a classical crossed product with trivial twisting and let $G = \mathrm{Gal(L/F)}$ with $n = |G|$. Let $e = \frac{1}{|G|}\sum_{g\in G} u_g$ and let $x_1, \ldots, x_n$ be non-zero elements of L. Then the conjugates of e by $x_1, \ldots, x_n$ form a complete set of orthogonal primitive idempotents of A if and only if $\mathrm{tr}_{L/F}(x_i x_j^{-1}) = 0$ for every $i \neq j$. ($\mathrm{tr}_{L/F}$ is the trace of L over F.)*

Proof. As the twisting is trivial, $\{u_g : g \in G\}$ is a subgroup of order $|G|$ of the group of units of A and hence e is an idempotent of A. Moreover $u_g e = e$ for every $g \in G$. Therefore, if $x \in L$ then $exe = \frac{1}{|G|}\sum_{g\in G} u_g xe = \frac{1}{|G|}\sum_{g\in G} x^{g^{-1}} u_g e = \frac{1}{|G|}\sum_{g\in G} x^g e = \frac{1}{|G|}\mathrm{tr}_{L/F}(x)e$. Thus, if $x \in L$ then e and xex^{-1} are orthogonal if and only if $\mathrm{tr}_{L/F}(x) = 0$ and the lemma follows. □

Examples 4.2.

(1) In the proof of Theorem 4.5 we will encounter some examples of classical crossed products with trivial twisting with a list $x_1, \ldots, x_n$ satisfying the conditions of the previous lemma.

(2) Another situation where one can find always such elements correspond to the case when L/F is a cyclic extension of order n and F contains a primitive n-th root of unity. Then L is the splitting field over F of an irreducible polynomial of $F[X]$ of the form $X^n - a$. If $\alpha \in L$ with $\alpha^n = a$ then $x_1 = 1, x_2 = \alpha, \ldots, x_n = \alpha^{n-1}$ satisfy the conditions of Lemma 4.1. Indeed, the minimal polynomial of α^i over F for $1 \leq i < n$ is of the form $X^{n/d} - a^{i/d}$ for $d = \gcd(n, i)$ and therefore $\mathrm{tr}_{L/F}(\alpha^i) = [L : F(\alpha^i)]\mathrm{tr}_{F(\alpha^i)/F}(\alpha^i) = 0$ and similarly $\mathrm{tr}_{L/F}(\alpha^{-i}) = 0$.

(3) We now construct an example where there are no elements $x_1, \ldots, x_n$ satisfying the conditions of Lemma 4.1. Consider the trivial cyclic algebra $(L = \mathbb{Q}(\zeta_7)/F = \mathbb{Q}(\sqrt{-7}), 1)$ of

degree 3. If x_1, x_2, x_3 satisfy the conditions of Lemma 4.1 then $\alpha = x_2x_1^{-1}$ and $\alpha^{-1} = x_1x_2^{-1}$ are non-zero elements of L with zero trace over F. This implies that the minimal polynomial of α over F is of the form $X^3 - a$ for some $a \in F$. But this implies that F contains a cube root of unity, a contradiction.

The groups listed in the following lemma will be the building blocks in the proof of Theorem 4.5. For n and p integers with p prime, we use $v_p(n)$ to denote the valuation at p of n, i.e. $p^{v_p(n)}$ is the maximum p-th power dividing n.

Lemma 4.3. *Let G be a finite p-group which has a maximal abelian subgroup which is cyclic and normal in G. Then G is isomorphic to one of the groups given by the following presentations:*

$$P_1 = \left\langle a, b \mid a^{p^n} = b^{p^k} = 1,\ b^{-1}ab = a^r \right\rangle, \text{ with either } v_p(r-1) = n-k \text{ or } p = 2 \text{ and } r \not\equiv 1 \mod 4.$$
$$P_2 = \left\langle a, b, c \mid a^{2^n} = 1,\ b^{2^k} = 1,\ c^2 = 1,\ bc = cb,\ b^{-1}ab = a^r,\ c^{-1}ac = a^{-1} \right\rangle, \text{ with } r \equiv 1 \mod 4.$$
$$P_3 = \left\langle a, b, c \mid a^{2^n} = 1,\ b^{2^k} = 1,\ c^2 = a^{2^{n-1}},\ bc = cb,\ b^{-1}ab = a^r,\ c^{-1}ac = a^{-1} \right\rangle, \text{ with } r \equiv 1 \mod 4.$$

Note that if $k = 0$ (equivalently, if $b = 1$) then the first case correspond to the case when G is abelian (and hence cyclic), the second case coincides with the first case with $p = 2$, $k = 1$ and $r = -1$, and the third case is the quaternion group of order 2^{n+1}.

Proof. Let A be a maximal abelian subgroup of G and assume that A is cyclic (generated by a) and normal in G. Put $|A| = p^n$. Consider the action of G on A by inner automorphisms. Since A is maximal abelian in G, the kernel of this action is A and therefore G/A is isomorphic to a subgroup of the group of automorphisms of A.

If either p is odd or $p = 2$ and $n \leq 2$ then $\mathrm{Aut}(A)$ is cyclic and otherwise $\mathrm{Aut}(A) = \langle \phi_5 \rangle \times \langle \phi_{-1} \rangle$, where ϕ_r is the automorphism of A given by $\phi_r(x) = x^r$.

Assume that G/A is cyclic, so that G has a presentation of the form

$$G = \left\langle a, b \mid a^{p^n} = 1, b^{p^k} = a^s, b^{-1}ab = a^r \right\rangle, \tag{2}$$

with $p^n \mid r^{p^k} - 1$ and $p^n \mid s(r-1)$. If $p^i \geq 3$ then $(1 + xp^i)^p \equiv 1 + xp^{i+1} \mod p^{i+2}$ for every $i \geq 1$ and $x \in \mathbb{Z}$. Using this, one deduces that if either p is odd or $p = 2$ and $r \equiv 1 \mod 4$ then $v_p(r^{p^i} - 1) = v_p(r^{p^{i-1}} - 1) + 1$, for every $i \geq 1$. Furthermore, from the assumption that A is maximal abelian in G, one deduces that $n \leq v_p(r^{p^k} - 1) = v_p(r^{p^{k-1}} - 1) + 1 \leq n$ and hence $v_p(r^{p^k} - 1) = n$ and $v_p(r-1) = n-k$. Therefore, $v_p(s) \geq n - v_p(r-1) = k = v_p\left(\frac{r^{p^k}-1}{r-1}\right) = v_p\left(1 + r + r^2 + \cdots + r^{p^k-1}\right)$ and hence there is an integer x such that $x(1 + r + r^2 + \cdots + r^{p^k-1}) + s \equiv 1 \mod p^n$. Then $(a^x b)^{p^k} = 1$ and, replacing b by $a^x b$ in (2), we obtain the presentation of P_1. We have also proved that $v_p(r-1) = n-k$ unless $p = 2$ and $r \not\equiv 1 \mod 4$. Assume $p = 2$ and $r \not\equiv 1 \mod 4$, $v_2(s) \geq n - v_2(r-1) = n-1$ and $v_2(1 + r + r^2 + \cdots + r^{2^k-1}) = v_2\left(\frac{r^{2^k}-1}{r-1}\right) \geq n-1$. If $v_2(s) \geq n$ then $G \cong P_1$. If $v_2(s) = v_2(1 + r + r^2 + \cdots + r^{2^k-1}) = n-1$ then $(ab)^{2^k} = 1$. Replacing b by ab we obtain again that $G \cong P_1$. Otherwise, $v_2(s) = n-1$ and $v_2(1 + r + r^2 + \cdots + r^{2^k-1}) = n$. Therefore $v_2(r^{2^k-1}) > n > v_2(r^{2^{k-1}} - 1)$ and by the first part of the proof (applied to $\langle a, b^2 \rangle$) this implies that $k = 2$. Then G is the quaternion group of order 2^{n+1} which is P_3 for $k = 0$.

Assume now that G/A is not cyclic, so $p = 2$ and $G/\langle a \rangle = \langle \overline{b} \rangle \times \langle \overline{c} \rangle$ with c acting by inversion on $\langle a \rangle$. This provides a presentation of G of the form

$$G = \langle a, b, c \mid a^{2^n} = 1, b^{2^k} = a^s, ca = a^{-1}c, cb = a^i bc, b^{-1}ab = a^r, c^2 = 1 \text{ or } c^2 = a^{2^{n-1}} \rangle. \tag{3}$$

Replacing b by bc if needed, one may assume that $v_2(r-1) = n-k \geq 2$ and $v_2(r^{2^k}-1) = n$. So, applying the first part of the proof to $\langle a, b\rangle$, we may assume that $b^{2^k} = 1$. Then $c = b^{2^k} c b^{-2^k} = a^{-i(1+r+\cdots+r^{2^k-1})} c$ and so $2^n \mid -i(1+r+\cdots+r^{2^k-1}) = -i\frac{r^{2^k}-1}{r-1}$. As $v_2\left(\frac{r^{2^k}-1}{r-1}\right) = k$, we have $v_2(i) \geq n-k = v_2(r-1)$. Hence, there exists an integer j so that $j(r-1) - i \equiv 0 \mod 2^n$. It is easy to verify that the commutator of b and $a^j c$ is 1. So, replacing c by $a^j c$ if needed, we may assume that b and c commute and we obtain the presentation of P_2, if $c^2 = 1$, and the presentation of P_3, if $c^2 = a^{2^{n-1}}$. □

We also need the following result on splitting of a Hamiltonian quaternion algebra $\mathbb{H}(F) = F[i, j \mid i^2 = j^2 = -1, ji + ji = 0]$.

Lemma 4.4. *Let F be a field of characteristic zero. Then the quaternion algebra $\mathbb{H}(F)$ splits if and only if $x^2 + y^2 = -1$ for some $x, y \in F$. In that case $\frac{1}{2}(1 + xi + yj)$ and $\frac{1}{2}(1 - xi - yj)$ form a complete set of primitive idempotents of $\mathbb{H}(F)$.*

Furthermore, if $F = \mathbb{Q}(\zeta_m, \zeta_{2^n} + \zeta_{2^n}^{-1})$ with m odd then -1 is the sum of two squares of F if and only if $m \neq 1$ and either $n \geq 3$ or the multiplicative order of 2 modulo m is even.

Proof. The first part can be found in [Seh1, Proposition 1.13]. Now assume that $F = \mathbb{Q}(\zeta_m, \zeta_{2^n} + \zeta_{2^n}^{-1})$ with m odd. If $m = 1$ then F is totally real and therefore -1 is not the sum of two squares of F. So assume that $m \neq 1$. If $n \leq 2$, then $F = \mathbb{Q}(\zeta_m)$ and the result is well known (see for example [Mos, FGS] or [Lam, pages 307–308]). Finally assume that $m \neq 1$ and $n \geq 3$. Then F contains $\sqrt{2}$ and, as 2 is not a square in $\mathbb{Q}_2$, the duadic completion of $\mathbb{Q}$ [Lam, Corollary 2.24], we deduce that $[F_2 : \mathbb{Q}_2]$ is even. Then -1 is a sum of squares in F_p for every place p of F and hence -1 is a sum of squares in F (see [Lam, page 304]). □

Now we are ready to show an effective method to calculate a complete set of orthogonal primitive idempotents of $\mathbb{Q}G$ for G a finite nilpotent group. Since G is abelian-by-supersolvable and hence strongly monomial, it follows from [OdRS1, Theorem 4.4] that every primitive central idempotent of $\mathbb{Q}G$ is of the form $e(G, H, K)$ with (H, K) a strong Shoda pair of G and therefore it is enough to obtain a complete set of orthogonal primitive idempotents of $\mathbb{Q}Ge(G, H, K)$ for every strong Shoda pair (H, K) of G. This is described in our main result that we state now.

Theorem 4.5. *Let G be a finite nilpotent group and (H, K) a strong Shoda pair of G. Set $e = e(G, H, K)$, $\varepsilon = \varepsilon(H, K)$, $H/K = \langle \overline{a}\rangle$, $N = N_G(K)$ and let N_2/K and $H_2/K = \langle \overline{a_2}\rangle$ (respectively $N_{2'}/K$ and $H_{2'}/K = \langle \overline{a_{2'}}\rangle$) denote the 2-parts (respectively, 2′-parts) of N/K and H/K respectively. Then $\langle \overline{a_{2'}}\rangle$ has a cyclic complement $\langle \overline{b_{2'}}\rangle$ in $N_{2'}/K$.*

A complete set of orthogonal primitive idempotents of $\mathbb{Q}Ge$ consists of the conjugates of $\widehat{b_{2'}}\beta_2\varepsilon$ by the elements of $T_{2'}T_2T_{G/N}$, where $T_{2'} = \{1, a_{2'}, a_{2'}^2, \ldots, a_{2'}^{[N_{2'}:H_{2'}]-1}\}$, $T_{G/N}$ denotes a left transversal of N in G and β_2 and T_2 are given according to the cases below.

(1) *If H_2/K has a complement M_2/K in N_2/K then $\beta_2 = \widehat{M_2}$. Moreover, if M_2/K is cyclic then there exists $b_2 \in N_2$ such that N_2/K is given by the following presentation*

$$\left\langle \overline{a_2}, \overline{b_2} \mid \overline{a_2}^{2^n} = \overline{b_2}^{2^k} = 1,\ \overline{a_2}^{\overline{b_2}} = \overline{a_2}^{r} \right\rangle,$$

and if M_2/K is not cyclic, there exist $b_2, c_2 \in N_2$ such that N_2/K is given by the following presentation

$$\left\langle \overline{a_2}, \overline{b_2}, \overline{c_2} \mid \overline{a_2}^{2^n} = \overline{b_2}^{2^k} = 1,\ \overline{c_2}^2 = 1,\ \overline{a_2}^{\overline{b_2}} = \overline{a_2}^{r},\ \overline{a_2}^{\overline{c_2}} = \overline{a_2}^{-1},\ [\overline{b_2}, \overline{c_2}] = 1 \right\rangle,$$

with $r \equiv 1 \mod 4$ *(or equivalently,* $\overline{a_2}^{2^{n-2}}$ *is central in* N_2/K*). Then*

(i) $T_2 = \{1, a_2, a_2^2, \dots, a_2^{2^k-1}\}$*, if* $\overline{a_2}^{2^{n-2}}$ *is central in* N_2/K *and* M_2/K *is cyclic; and*

(ii) $T_2 = \{1, a_2, a_2^2, \dots, a_2^{2^{k-1}-1}, a_2^{2^{n-2}}, a_2^{2^{n-2}+1}, \dots, a_2^{2^{n-2}+2^{k-1}-1}\}$*, otherwise.*

(2) *if* H_2/K *has no complement in* N_2/K *then there exist* $b_2, c_2 \in N_2$ *such that* N_2/K *is given by the following presentation*

$$\left\langle \overline{a_2}, \overline{b_2}, \overline{c_2} \mid \overline{a_2}^{2^n} = \overline{b_2}^{2^k} = 1,\ \overline{c_2}^2 = \overline{a_2}^{2^{n-1}},\ \overline{a_2}^{\overline{b_2}} = \overline{a_2}^r,\ \overline{a_2}^{\overline{c_2}} = \overline{a_2}^{-1},\ [\overline{b_2}, \overline{c_2}] = 1 \right\rangle,$$

with $r \equiv 1 \mod 4$ *and we set* $m = [H_{2'} : K]/[N_{2'} : H_{2'}]$*. Then*

(i) $\beta_2 = \widehat{b_2}$ *and* $T_2 = \{1, a_2, a_2^2, \dots, a_2^{2^k-1}\}$*, if either* $H_{2'} = K$ *or the order of* 2 *modulo* m *is odd and* $n - k \leq 2$ *and*

(ii) $\beta_2 = \widehat{b_2}^{\frac{1+xa_2^{2^{n-2}}+ya_2^{2^{n-2}}c_2}{2}}$ *and* $T_2 = \{1, a_2, a_2^2, \dots, a_2^{2^k-1}, c_2, a_2c_2, a_2^2c_2, \dots, a_2^{2^k-1}c_2\}$ *with*

$$x, y \in \mathbb{Q}\left[a_{2'}^{[N_{2'}:H_{2'}]}, a_2^{2^k} + a_2^{-2^k}\right],$$

satisfying $(1 + x^2 + y^2)\varepsilon = 0$*, if* $H_{2'} \neq K$ *and either the order of* 2 *modulo* m *is even or* $n - k > 2$*.*

Proof. We start the proof by making some useful reductions. Taking $T = T_{G/N}$ a left transversal of N in G, the conjugates of ε by elements of T are the "diagonal" elements in the matrix algebra $\mathbb{Q}Ge = M_{G/N}(\mathbb{Q}N\varepsilon)$. Hence, following the proof of [OdRS1, Proposition 3.4], one can see that it is sufficient to compute a complete set of orthogonal primitive idempotents for $\mathbb{Q}N\varepsilon = \mathbb{Q}H\,\varepsilon * N/H$ and then add their T-conjugates in order to obtain the primitive idempotents of $\mathbb{Q}Ge$. So one may assume that $N = G$, i.e. K is normal in G and hence $e = \varepsilon$ and $T = \{1\}$. Then the natural isomorphism $\mathbb{Q}G\widehat{K} \simeq \mathbb{Q}(G/K)$ maps ε to $\varepsilon(H/K)$. So, from now on we assume that $K = 1$ and hence $H = \langle a \rangle$ is a cyclic maximal abelian subgroup of G, which is normal in G and $e = \varepsilon = \varepsilon(H)$. If $G = H$ then $\mathbb{Q}Ge$ is a field, $T_2 = T_{2'} = \{1\}$ and $b_{2'} = \beta_2 = 1$; hence the result follows. So, in the remainder of the proof we assume that $G \neq H$.

The map $a\varepsilon \mapsto \zeta$ induces an isomorphism $f : \mathbb{Q}H\varepsilon \to \mathbb{Q}(\zeta)$, where ζ is a primitive $|H|$-root of unity. Using the description of $\mathbb{Q}Ge$ given in Theorem 2.1, one obtains a description of $\mathbb{Q}Ge$ as a classical crossed product $(\mathbb{Q}(\zeta)/F, \tau)$, where F is the image under f of the center of $\mathbb{Q}Ge$.

We first consider the case when G is a p-group. Then G and $H = \langle a \rangle$ satisfy the conditions of Lemma 4.3 and therefore G is isomorphic to one of the three groups of this lemma. Moreover, H has a complement in G if and only if $G \cong P_1$ or $G \cong P_2$ and, in these cases, τ is trivial. We claim that in these cases it is possible to give a list of elements $x_1, \dots, x_{p^k}$ of $\mathbb{Q}(\zeta)$ ($p^k = [G : H]$) satisfying the conditions of Lemma 4.1 and the elements $f^{-1}(x_1), \dots, f^{-1}(x_{p^k})$ correspond to the conjugating elements in G given in the statement of the theorem in the different cases. To prove this we will use the following fact: if L is a subfield of $\mathbb{Q}(\zeta)$ such that $\zeta_p \in L$, $\zeta^i \notin L$ (with $i = 1, \dots, p^k - 1$) and, moreover, $\zeta_4 \in L$ if $p = 2$ then $\mathrm{tr}_{\mathbb{Q}(\zeta)/L}(\zeta^i) = 0$. To see this notice that if d is the minimum integer such that $\zeta^{ip^d} \in L$ then $\mathbb{Q}(\zeta^i)/L$ is cyclic of degree p^d and ζ^i is a root of $X^{p^d} - \zeta^{ip^d} \in L[X]$. Then $X^{p^d} - \zeta^{ip^d}$ is the minimal polynomial of ζ^i over L. Hence $\mathrm{tr}_{\mathbb{Q}(\zeta^i)/L}(\zeta^i) = 0$ and thus $\mathrm{tr}_{\mathbb{Q}(\zeta)/L}(\zeta^i) = 0$.

Assume first that $G = P_1$ and $v_p(r-1) = n-k$ (equivalently $a_p^{p^{n-k}} \in Z(G)$), that is, either p is odd or $p = 2$ and $r \equiv 1 \mod 4$). Then F is the unique subfield of index $[G : H] = p^k$ in $\mathbb{Q}(\zeta)$ and such that if $p = 2$ then $\zeta_4 \in F$. Namely $F = \mathbb{Q}(\zeta_{p^{n-k}}) = \mathbb{Q}(\zeta^{p^k})$. If we set $x_i = \zeta^i$, for $i = 0, 1, \dots, p^k - 1$, then $x_i x_j^{-1} = \zeta^{i-j}$. If $i \neq j$ then $\zeta^{i-j} \notin F$ and hence $\mathrm{tr}_{\mathbb{Q}(\zeta)/F}(x_i x_j^{-1}) = \mathrm{tr}_{\mathbb{Q}(\zeta)/F}(\zeta^{i-j}) = 0$. Thus,

by Lemma 4.1, the conjugates of $\widehat{b}$ by $1, \zeta, \zeta^2, \ldots, \zeta^{p^k-1}$ form a complete set of orthogonal primitive idempotents of $(\mathbb{Q}(\zeta)/F, 1)$. Then the elements $f^{-1}(x_i)$ form the elements of $T_{2'}$ if p is odd or the elements of T_2, in case (1.i).

Assume now that G is still P_1, but with $p = 2$ and $r \not\equiv 1 \mod 4$ (equivalently, $a_2^{2^{n-2}}$ is not central). In this case $\zeta_4 \notin F$ and $F(\zeta_4)$ is the unique subextension of $\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta_4)$ of index $[G : H]/2 = 2^{k-1}$. That is $F(\zeta_4) = \mathbb{Q}(\zeta_{2^{n-k+1}}) = \mathbb{Q}(\zeta^{2^{k-1}})$. We take $x_i = \zeta^i$ and $x_{2^{k-1}+i} = \zeta^{2^{n-2}+i} = \zeta_4\zeta^i$, for $0 \leq i < 2^{k-1}$. Hence, if $i \neq j$ then $x_i x_j^{-1}$ is either $\zeta_4^{\pm 1}$ or $\zeta^{\pm i}$ or $\zeta_4^{\pm 1}\zeta^{\pm i}$, with $i = 1, 2, \ldots, 2^{k-1} - 1$. As $\zeta^i \notin F(\zeta_4)$, we have $\mathrm{tr}_{\mathbb{Q}(\zeta)/F(\zeta_4)}(\zeta^i) = 0$. Since

$$\mathrm{tr}_{\mathbb{Q}(\zeta)/F}(\zeta_4) = \mathrm{tr}_{F(\zeta_4)/F}\mathrm{tr}_{\mathbb{Q}(\zeta)/F(\zeta_4)}(\zeta_4) = [\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta_4)]\mathrm{tr}_{F(\zeta_4)/F}(\zeta_4) = 0,$$

$$\mathrm{tr}_{\mathbb{Q}(\zeta)/F}(\zeta^i) = \mathrm{tr}_{F(\zeta_4)/F}\mathrm{tr}_{\mathbb{Q}(\zeta)/F(\zeta_4)}(\zeta^i) = 0$$

and

$$\mathrm{tr}_{\mathbb{Q}(\zeta)/F}(\zeta_4\zeta^i) = \mathrm{tr}_{F(\zeta_4)/F}\mathrm{tr}_{\mathbb{Q}(\zeta)/F(\zeta_4)}(\zeta_4\zeta^i) = \mathrm{tr}_{F(\zeta_4)/F}(\zeta_4\mathrm{tr}_{\mathbb{Q}(\zeta)/F(\zeta_4)}(\zeta^i)) = 0,$$

we deduce that $\mathrm{tr}(x_i x_j^{-1}) = 0$ for every $i \neq j$. Then f^{-1} maps these elements to the elements of T_2 for case (1.ii).

Now assume that $G = P_2$. Then $F = \mathbb{Q}(\zeta_{2^{n-k}} + \zeta_{2^{n-k}}^{-1})$. Since $r \equiv 1 \mod 4$, $n - k \geq 2$. Then the same argument as in the previous case shows that the 2^{k+1} elements of the form $x_i = \zeta^i$ and $x_{2^k+i} = \zeta^{2^{n/2}+i} = \zeta_4\zeta^i$, for $0 \leq i < 2^k$ satisfy the conditions of Lemma 4.1. The elements $f^{-1}(x_i)$ form now the set T_2 of case (1.ii).

Now we consider the non-splitting case, i.e. $G = P_3$. Then the center of $\mathbb{Q}Ge$ is isomorphic to $F = \mathbb{Q}(\zeta)^{\langle b,c\rangle} = \mathbb{Q}(\zeta_{2^{n-k}} + \zeta_{2^{n-k}}^{-1})$ and $\widehat{b}\,\mathbb{Q}G\,\varepsilon\widehat{b} = \widehat{b}\,\mathbb{Q}\langle a, c\rangle\,\varepsilon\widehat{b}F + Fa^{2^{n-2}} + Fc + F(a^{2^{n-2}}c) \cong \mathbb{H}(F)$, which is a division algebra, as F is a real field. Then $\widehat{b}\varepsilon$ is a primitive idempotent of $\mathbb{Q}Ge$. Hence $\mathbb{Q}Ge \simeq M_{2^k}(\mathbb{H}(F))$ and from the first case one can provide the 2^k orthogonal primitive idempotents needed in this case by taking the conjugates of $\widehat{b}$ by $1, a, a^2, \ldots, a^{2^k-1}$, and this agrees with case (2.i). This finishes the p-group case.

Let us now consider the general case, where G is not necessarily a p-group. For a prime p let G_p denote the p-Sylow subgroup of G and $G_{p'}$ the p'-Hall subgroup of p. Then $G = G_2 \times G_{p_1} \times \cdots \times G_{p_r} = G_2 \times G_{2'}$, with p_i an odd prime for every $i = 1, \ldots, r$. Moreover $\varepsilon(H) = \prod_i \varepsilon(H_{p_i})$ and $(H, 1)$ is a strong Shoda pair of G if and only if $(H_{p_i}, 1)$ is a strong Shoda pair of G_{p_i}, for every $i = 0, 1, \ldots, r$, (with $p_0 = 2$). Using this and a dimension argument it easily follows that the simple algebra $\mathbb{Q}G\varepsilon(H)$ is the tensor product over $\mathbb{Q}$ of the simple algebras $\mathbb{Q}G_{p_i}\varepsilon(H_{p_i})$. On the other hand, we have seen that for $i \geq 1$, $\mathbb{Q}G_{p_i}\varepsilon(H_{p_i}) \simeq M_{p_i^{k_i}}(\mathbb{Q}(\zeta_{p_i^{n_i-k_i}}))$, for $p_i^{n_i} =\mid H_{p_i} \mid$ and $p_i^{k_i} = [G_{p_i} : H_{p_i}]$. Then $\mathbb{Q}G_{2'}\varepsilon(H_{2'}) \simeq M_{[G_{2'}:H_{2'}]}(\mathbb{Q}(\zeta_m))$, with $m =\mid H_{2'} \mid /[G_{2'} : H_{2'}]$ $(= [H_{2'} : K]/[G_{2'} : H_{2'}])$ and then a complete set of orthogonal primitive idempotents of $\mathbb{Q}G_{2'}\varepsilon(H_{2'})$ can be obtained by multiplying the different sets of idempotents obtained for each tensor factor. Observe that each G_{p_i}, with $i \geq 1$, takes the form $\langle a_i\rangle \rtimes \langle b_i\rangle$ and so $G_{2'} = \langle a\rangle \rtimes \langle b\rangle$, with $a = a_1 \ldots a_r$ and $b = b_1 \ldots b_r$. Having in mind that $a^{p_i^{k_i}}$ is central one can easily deduce, with the help of the Chinese Remainder Theorem, that the product of the different primitive idempotents of the factors from the odd part (i.e. the conjugates of $\widehat{b_i}$ by $1, a_i, a_i^2, \ldots, a_i^{p_i^{k_i}-1}$ are the conjugates of $\widehat{b}\varepsilon$ by $1, a, a^2, \ldots, a^{[G_{2'}:H_{2'}]-1}$. In the notation of the statement of the theorem, $a = a_{2'}$ and $T_{2'} = \{1, a, a^2, ..., a^{[G_{2'}:H_{2'}]-1}\}$ as wanted.

If $|G|$ is odd then the proof is finished. Otherwise we should combine the odd and even parts of G. If H_2 has a complement in G_2 then $\mathbb{Q}G_2\varepsilon(H_2)$ is split over its center and hence we can take T_2 as in the 2-group case. However, if H_2 does not have a complement in G_2 then $\mathbb{Q}G_2\varepsilon(H_2) =$

$M_{[G_2:H_2]/2}(\mathbb{H}(\mathbb{Q}(\zeta_{2^{n-k}}+\zeta_{2^{n-k}}^{-1})))$ and hence $\mathbb{Q}G\varepsilon = M_{[G:H]/2}(\mathbb{H}(F))$, with $F = \mathbb{Q}(\zeta_m, \zeta_{2^{n-k}}+\zeta_{2^{n-k}}^{-1})$. If $\mathbb{H}(F)$ is not split (equivalently the conditions of (2.i) hold) then we can also take T_2 as in the 2-group case. However, if $\mathbb{H}(F)$ is split then one should duplicate the number of idempotents, or equivalently duplicate the size of T_2. In this case -1 is a sum of squares in F. Observing that $f(a_{2'}^{[N_{2'}:H_{2'}]})$ is a primitive m-th root of unity and $f(a_2^{2^k})$ is a primitive 2^{n-k} root of unity, we deduce that there are $x, y \in \mathbb{Q}(a_{2'}^{[N_{2'}:H_{2'}]}, a_2^{2^k}+a_2^{-2^k})$ such that $(1+x^2+y^2)\varepsilon = 0$. Then we can duplicate the number of idempotents by multiplying the above idempotents by $f = \frac{1+xa_2^{2^{n-2}}+ya_2^{2^{n-2}}c_2}{2}$ and $1-f = \frac{1-xa_2^{2^{n-2}}-ya_2^{2^{n-2}}c_2}{2}$ (see Lemma 4.4). Observing that $1-f = f^{c_2}$, we obtain that these idempotents are the conjugates of $\widehat{b_2}f\varepsilon$ by $1, a_2, \ldots, a_2^{2^k-1}, c_2, a_2c_2, \ldots, a_2^{2^k-1}c_2$, as desired. □

Remark 4.6. A description of the simple algebras $\mathbb{Q}Ge$ using Theorem 2.1 can be given according to the cases listed above. Thus, $\mathbb{Q}Ge = M_{|G/H|}(\mathbb{Q}(\zeta_{[H:K]})^{N/K})$, that is a matrix algebra over the fixed field of the natural action of N/K on the cyclotomic field $\mathbb{Q}(\zeta_{[H:K]}) = \mathbb{Q}H\varepsilon(H,K)$, in cases (1) and (2.ii) of Theorem 4.5 and $\mathbb{Q}Ge = M_{\frac{1}{2}|G/H|}(\mathbb{H}(\mathbb{Q}(\zeta_{[H:K]})^{N/K}))$ in case (2.i). Using this and Lemma 4.4 one deduces that if $\mathbb{Q}Ge$ is a non-commutative division algebra then $[G:H] = 2$, $N = G$ and either $\mathbb{Q}Ge \cong \mathbb{H}\left(\mathbb{Q}\left(\zeta_{2^n}+\zeta_{2^n}^{-1}\right)\right)$ with $[H:K] = 2^n$, or $\mathbb{Q}Ge \cong \mathbb{H}(\mathbb{Q}(\zeta_m))$ with m an odd prime such that the order of 2 modulo m is odd and $[H:K] = m$ or $2m$.

As a consequence of Theorem 4.5, we get the following result on the Schur indices of the simple components of group algebras for finite nilpotent groups over fields of characteristic zero.

Theorem 4.7 (Roquette)**.** *Let G be a finite nilpotent group and F a field of characteristic zero. Then $FG \cong \bigoplus_i M_{n_i}(D_i)$, where the D_i are quaternion division algebras if not commutative, that is the Schur index of the simple components of FG is at most 2. If the Schur index of a simple component of FG is 2 then the Sylow 2-subgroup of G has a quaternion section.*

Remark 4.8. Notice that the use of Lemma 4.1 has been essential in all the cases of the proof of Theorem 4.5. We would like to be able to give a similar description to the one from Theorem 4.5 for a complete set of orthogonal primitive idempotents for rational group algebras of arbitrary finite metacyclic groups. Unfortunately, the approach of Theorem 4.5 does not apply here. For example, if $G = C_7 \rtimes C_3 = \langle a\rangle \rtimes \langle b\rangle$, with $b^{-1}ab = a^2$ and $\varepsilon = \varepsilon(\langle a\rangle)$ then there is not a complete set of orthogonal primitive idempotents of $\mathbb{Q}G\varepsilon$ formed by $\mathbb{Q}(a)$-conjugates of $\widehat{b}\varepsilon$. This is a consequence of Example 4.2 (3).

Notation 4.9. As an application of Theorem 4.5 we next will describe a complete set of matrix units in a simple component $\mathbb{Q}Ge$, where $e = e(G,H,K)$ with (H,K) a strong Shoda pair of a finite nilpotent group G. A complete set of primitive idempotents of $\mathbb{Q}Ge(G,H,K)$ is given according to the cases of Theorem 4.5. Using the notation in these different cases of Theorem 4.5, let $T_e = T_{2'}T_2T_{G/N}$ and $\beta_e = \widehat{b_{2'}}\beta_2\varepsilon$, where $\varepsilon = \varepsilon(H,K)$, $T_{G/N}$ denotes a left transversal of $N = N_G(K)$ in G; $T_{2'} = \left\{1, a_{2'}, \ldots, a_{2'}^{[N_{2'}:H_{2'}]-1}\right\}$;

$$T_2 = \begin{cases} \left\{1, a_2, \ldots, a_2^{2^k-1}\right\}, & \text{in cases (1.i) and (2.i);} \\ \left\{1, a_2, \ldots, a_2^{2^{k-1}-1}, a_2^{2^{n-2}}, a_2^{2^{n-2}+1}, \ldots, a_2^{2^{n-2}+2^{k-1}-1}\right\}, & \text{in case (1.ii);} \\ \left\{1, a_2, \ldots, a_2^{2^k-1}, c_2, a_2c_2, \ldots, a_2^{2^k-1}c_2\right\}, & \text{in case (2.ii);} \end{cases}$$

and

$$\beta_2 = \begin{cases} \widehat{M_2}, & \text{in case (1);} \\ \widehat{b_2}, & \text{in case (2.i);} \\ \widehat{b_2}\frac{1+xa_2^{2^{n-2}}+ya_2^{2^{n-2}}c_2}{2}, & \text{in case (2.ii).} \end{cases}$$

Corollary 4.10. *Let G be a finite nilpotent group. For every primitive central idempotent $e = e(G,H,K)$, with (H,K) a strong Shoda pair of G, let T_e and β_e be as in Notation 4.9. For every $t,t' \in T_e$ let*

$$E_{tt'} = t^{-1}\beta_e\, t'.$$

Then $\{E_{tt'} \mid t,t' \in T_e\}$ gives a complete set of matrix units in $\mathbb{Q}Ge$, i.e. $e = \sum_{t\in T_e} E_{tt}$ and $E_{t_1t_2}E_{t_3t_4} = \delta_{t_2t_3}E_{t_1t_4}$, for every $t_1,t_2,t_3,t_4 \in T_e$.

Moreover, $E_{tt}\mathbb{Q}GE_{tt} \cong F$, in cases (1) and (2.ii) of Theorem 4.5, and $E_{tt}\mathbb{Q}GE_{tt} = \mathbb{H}(F)$, in case (2.i) of Theorem 4.5, where F is the fixed subfield of $\mathbb{Q}(a)\varepsilon$ under the natural action of N/H.

Proof. We know from Theorem 4.5 that the set $\{E_{tt} \mid t \in T_e\}$ is a complete set of primitive idempotents of $\mathbb{Q}Ge$. From the definition of the $E_{tt'}$ it easily follows that $E_{t_1t_2}E_{t_3t_4} = \delta_{t_2t_3}E_{t_1t_4}$, for $t_i \in T_e$, $i = 1,\dots,4$. The second statement is already mentioned in Remark 4.6. □

5. Generators of a subgroup of finite index in $\mathcal{U}(\mathbb{Z}G)$

As an application of the description of the primitive central idempotents in Corollary 4.10, we now can easily explicitly construct two nilpotent subgroups of $\mathcal{U}(\mathbb{Z}G)$ (which correspond with upper respectively lower triangular matrices in the simple components). Together with the central units they generate a subgroup of finite index in the unit group. We begin by recalling a result of Jespers, Parmenter and Sehgal that gives explicit generators for a subgroup of finite index in the center.

First we recall the construction of units known as Bass cyclic units in the integral group ring $\mathbb{Z}G$ of a finite group G. Let $g \in G$ and suppose g has order n. Let k be an integer so that $1 < k < n$ and $(k,n) = 1$. Then, $k^{\varphi(n)} \equiv 1 \mod n$, where φ is the Euler φ-function, and

$$b(g,k) = \left(\sum_{j=0}^{k-1} g^j\right)^{\varphi(n)} + (1-k^{\varphi(n)})\widehat{g}$$

is a unit in $\mathbb{Z}G$. (Note that our notation slightly differs from the one used in [Seh1]; this because of our definition of $\widehat{g} = \frac{1}{n}\sum_{i=1}^{n} g^i$.) The group generated by all Bass cyclic units of $\mathbb{Z}G$ we denote by $B(G)$.

We now introduce the following units defined in [JPS]. Let Z_v denote the v-th center of G that is the v-th term of the upper central series, and suppose that G is nilpotent of class n. For any $x \in G$ and $b \in \mathbb{Z}\langle x\rangle$, put $b_{(1)} = b$ and, for $2 \le v \le n$, put

$$b_{(v)} = \prod_{g\in Z_v} b_{(v-1)}^g.$$

Note that by induction $b_{(v)}$ is central in $\mathbb{Z}\langle Z_v, x\rangle$ and is independent of the order of the conjugates in the product expression. In particular, $b_{(n)} \in Z(\mathcal{U}(\mathbb{Z}G))$. Let

$$B_{(n)}(G) = \left\langle b_{(n)} \mid b \text{ a Bass cyclic of } \mathbb{Z}G \right\rangle.$$

Proposition 5.1. [JPS, Proposition 2] *If G is a finite nilpotent group of class n, then $B_{(n)}(G)$ has finite index in $Z(\mathcal{U}(\mathbb{Z}G))$.*

The proof of the previous proposition relies on results of Bass [Bas, Lemma 2.2, Lemma 3.6, Theorem 2, Theorem 4], which states that the natural images of the Bass cyclic units in the Whitehead group $K_1(\mathbb{Z}G)$ of $\mathbb{Z}G$ generate a subgroup of finite index, and on the fact that the torsion-free rank of the abelian groups $K_1(\mathbb{Z}G)$ and $Z(\mathcal{U}(\mathbb{Z}G))$ are the same. Clearly, because $K_1(\mathbb{Z}G)$ is commutative, the natural image of a $b_{(n)}$ in $K_1(\mathbb{Z}G)$ is equal with the natural image of some power of b in $K_1(\mathbb{Z}G)$. Hence in $K_1(\mathbb{Z}G)$ the group generated by the Bass cyclic units contains the group generated by the $b_{(n)}$'s as a subgroup of finite index. So, indeed, $B_{(n)}(G)$ is of finite index in $Z(\mathcal{U}(\mathbb{Z}G))$.

If G is a finite group and e is a primitive central idempotent of the rational group algebra $\mathbb{Q}G$, then the simple algebra $\mathbb{Q}Ge$ is identified with $M_n(D)$, a matrix algebra over a division algebra D. As in [JL1], an exceptional component of $\mathbb{Q}G$ is a non-commutative division algebra other than a totally definite quaternion algebra, or a two-by-two matrix algebra over either the rationals, a quadratic imaginary extension of the rationals or a non-commutative division algebra.

Let $\mathcal{O}$ be an order in D and denote by $\mathrm{GL}_n(\mathcal{O})$ the group of invertible matrices in $M_n(\mathcal{O})$ and by $\mathrm{SL}_n(\mathcal{O})$ its subgroup consisting of matrices of reduced norm 1. For an ideal Q of $\mathcal{O}$ we denote by $E(Q)$ the subgroup of $\mathrm{SL}_n(\mathcal{O})$ generated by all Q-elementary matrices, that is $E(Q) = \langle I + qE_{ij} \mid q \in Q, 1 \leq i, j \leq n, i \neq j, E_{ij} \text{ a matrix unit}\rangle$. We recall the following celebrated theorem (see for instance [RS1] or [JL1, Theorem 2.2]).

Theorem 5.2 (Bass-Milnor-Serre-Vaserstein)**.** *If $n \geq 3$ then $[\mathrm{SL}_n(\mathcal{O}) : E(Q)] < \infty$. If $n = 2$ and D is an algebraic number field which is not rational or imaginary quadratic, then $[\mathrm{SL}_2(\mathcal{O}) : E(Q)] < \infty$.*

Because of the description of the matrix units from Corollary 4.10, we can now show that, in case G is nilpotent and does not have exceptional simple components, $\mathcal{U}(\mathbb{Z}G)$ has a subgroup of finite index that is generated by three nilpotent groups, one of which is a central subgroup contained in the group generated by the Bass cyclic units and the others are generated by the units of the form $1 + E_{tt}gE_{t't'}$, with $g \in G$ and $t, t' \in T_e$, with T_e as in Notation 4.9.

Theorem 5.3. *Let G be a finite nilpotent group of class n such that $\mathbb{Q}G$ has no exceptional components. For every primitive central idempotent $e = e(G, H, K)$, with (H, K) a strong Shoda pair of G, let $N = N_G(K)$, $\varepsilon = \varepsilon(H, K)$ and let T_e and β_e be as in Notation 4.9. Fix an order $<$ in T_e. Let $H/K = \langle \overline{a} \rangle$ and let l be the least integer such that $a^l\varepsilon$ is central in $\mathbb{Q}N\varepsilon$. Then the following two groups are nilpotent subgroups of $\mathcal{U}(\mathbb{Z}G)$:*

$$V_e^+ = \left\langle 1 + |G|t^{-1}\beta_e a^j t' \mid a^j \in \langle a^l \rangle, t, t' \in T_e, t' > t \right\rangle,$$

$$V_e^- = \left\langle 1 + |G|t^{-1}\beta_e a^j t' \mid a^j \in \langle a^l \rangle, t, t' \in T_e, t' < t \right\rangle.$$

Hence

$$V^+ = \left\langle V_e^+ \mid e = e(G, H, K) \text{ a primitive central idempotent of } \mathbb{Q}G \right\rangle = \prod_e V_e^+ \text{ and}$$

$$V^- = \left\langle V_e^- \mid e = e(G, H, K) \text{ a primitive central idempotent of } \mathbb{Q}G \right\rangle = \prod_e V_e^-$$

are nilpotent subgroups of $\mathcal{U}(\mathbb{Z}G)$. Furthermore, if $B_{(n)}(G) = \langle b_{(n)} \mid b \text{ a Bass cyclic unit of } G\rangle$, where n is the nilpotency class of G, then the group

$$\left\langle B_{(n)}(G), V^+, V^- \right\rangle$$

is of finite index in $\mathcal{U}(\mathbb{Z}G)$.

Proof. Recall that the intersection of the unit groups of two orders in a finite dimensional rational algebra are commensurable and henceforth it is enough to show that $\langle B_{(n)}, V^+, V^-\rangle$ contains a subgroup of finite index in the group of units of an order of $(1-e)\mathbb{Q}+\mathbb{Q}Ge$ for a primitive central idempotent e of $\mathbb{Q}G$. So fix such a primitive central idempotent $e = e(G,H,K)$ of $\mathbb{Q}G$.

The elements of the form $1+|G|t^{-1}\beta_e a^j t'$, with $a^j \in \langle a^l\rangle$ and $t, t' \in T_e$, project trivially to $\mathbb{Q}G(1-e)$ and by Corollary 4.10 they project to an elementary matrix of $M_n(\mathcal{O})$, for some order $\mathcal{O}$ in the division ring D, where $\mathbb{Q}Ge \simeq M_n(D)$. Since also $|G|\beta_e \in \mathbb{Z}G$, it follows that $1+|G|t^{-1}\beta_e a^j t' \in \mathcal{U}(\mathbb{Z}G)$ and by Theorem 5.2, for $t \neq t'$, these units generate a subgroup of finite index in $(1-e)+\mathrm{SL}_n(\mathcal{O})$. By Theorem 5.1, $B_{(n)}$ has finite index in $Z(\mathcal{U}(\mathbb{Z}G))$ and therefore it contains a subgroup of finite index in the center of $(1-e)+\mathrm{GL}_n(\mathcal{O})$. As the center of $\mathrm{GL}_n(\mathcal{O})$ together with $\mathrm{SL}_n(\mathcal{O})$ generate a subgroup of finite index of $\mathrm{GL}_n(\mathcal{O})$, we conclude that the group $\langle B_{(n)}, V^+, V^-\rangle$ contains a subgroup of finite index in the group of units of an order of $(1-e)\mathbb{Q}+\mathbb{Q}Ge$. Note that V_e^+ and V_e^- correspond to upper and lower triangular matrices respectively and hence they are nilpotent groups. □

The description of a set of primitive idempotents can also be used to obtain the following result of Ritter and Sehgal. Recall that the bicyclic units of $\mathbb{Z}G$ are the elements of the form $b_{g,h} = 1+(1-g)h\sum_{i=0}^{|g|-1} g^i$, where $g, h \in G$ and $|g|$ denotes the order of g.

Theorem 5.4. [RS2] *Let G be a finite nilpotent group. If $\mathbb{Q}G$ does not have exceptional simple components and every simple component of $\mathbb{Q}G$ is a matrix algebra over a field then the subgroup generated by the Bass cyclic units and the bicyclic units of G has finite index in $\mathcal{U}(\mathbb{Z}G)$.*

Proof. Let $e = e(G,H,K)$ with (H,K) a strong Shoda pair of G and let us use Notation 4.9. As in the proof of Theorem 5.3, it is enough to show that there is a positive integer m such that B, the group generated by the bicyclic units, contains all the elements of the form $1+mf'gf$, for every two different elements f and f' from the list of primitive orthogonal idempotents of $\mathbb{Q}Ge$ given in Theorem 4.5 and every $g \in G$. By Remark 4.6, the assumption on the simple components of $\mathbb{Q}G_2$ implies that the strong Shoda pair (H,K) satisfies the conditions of (1) in Theorem 4.5. Thus $\beta_e = \widehat{b_{2'}}\widehat{M_2}\varepsilon = \widehat{M}\varepsilon$, for M/K a complement of H_2/K in N/K, and hence $f = t^{-1}\widehat{M}\varepsilon t$ for some $t \in G$. Replacing (H,K) by $(t^{-1}Ht, t^{-1}Kt)$ we may assume that $f = \widehat{M}\varepsilon$. Moreover, M/K is abelian generated by at most two elements. If $M = \langle b, c, K\rangle$ then $\widehat{M} = \widehat{K}\widehat{b}\widehat{c} = \widehat{K}\widehat{c}\widehat{b}$ and $\widehat{K}\varepsilon = \varepsilon$. Hence $e - f = e - \widehat{M}\varepsilon = (e - \widehat{b}\varepsilon + (1-\widehat{c})\widehat{b}\varepsilon)$. Thus, for a sufficiently large integer n, we have

$$\begin{aligned}
1+n(e-f)gf &= (1+n(e-\widehat{b}\varepsilon)g\widehat{M}\varepsilon)(1+n(e-\widehat{c})\widehat{b}\varepsilon g\widehat{M}\varepsilon)\\
&= (1+n(1-b)(e-\widehat{b}\varepsilon)g\widehat{M}\varepsilon\widehat{b})(1+n(1-c)(e-\widehat{c})\widehat{b}\varepsilon g\widehat{M}\varepsilon\widehat{c})\\
&= \prod_{h\in G}(1+u_h(1-b)h\sum_{i=0}^{|b|-1} b^i)\prod_{h\in G}(1+v_h(1-c)h\sum_{i=0}^{|c|-1} c^i)\\
&= \prod_{h\in G} b_{b,h}^{u_h}\prod_{h\in G} b_{c,h}^{v_h},
\end{aligned}$$

for some integers u_h and v_h. Thus $1+n(e-f)gf \in B$ and, as $1+f'gf = 1+(e-f)f'gf = \prod_{h\in G} 1+q_h(e-f)hf$, with $q_h \in \mathbb{Q}$, we deduce that $1+mf'gf = \langle 1+n(e-f)gf\rangle \subseteq B$ for some integer m. □

Another application of the construction of the matrix units is that one can easily obtain free subgroups of $\mathcal{U}(\mathbb{Z}G)$ for G a finite nilpotent group.

Corollary 5.5. *Let G be a finite nilpotent group, (H,K) a strong Shoda pair of G, $\varepsilon = \varepsilon(H,K)$, $e = e(G,H,K)$ and let T_e and β_e be as in Notation 4.9. If $\mathbb{Q}Ge$ is not a division algebra (see Remark 4.6), then for every $t, t' \in T_e$ with $t \neq t'$,*

$$\left\langle 1 + |G|t^{-1}\beta_e t', 1 + |G|t'^{-1}\beta_e t \right\rangle$$

is a free group of rank 2.

Proof. By Corollary 4.10, we may write $1+|G|t^{-1}\beta_e t' = 1+|G|E_{tt'}$ and $1+|G|t'^{-1}\beta_e t = 1+|G|E_{t't}$. Hence $\left\langle 1 + |G|t^{-1}\beta_e t', 1 + |G|t'^{-1}\beta_e t \right\rangle$ is isomorphic with $\left\langle \begin{pmatrix} 1 & |G| \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ |G| & 1 \end{pmatrix} \right\rangle$. Since $|G| \geq 2$, a well known result of Sanov yields that this group is a free of rank 2. □

Remark 5.6. A well known result of Hartley and Pickel [HP] (or see for example [Seh1]) says that $\mathcal{U}(\mathbb{Z}G)$ contains a free non-abelian subgroup for any finite non-abelian group G that is not a Hamiltonian 2-group. Only in 1997, Sehgal and Marciniak in [MS1] gave a concrete construction of such a group. They showed that if $u_{g,h} = 1 + (1-g)h\widehat{g}|\langle g\rangle|$ is a non trivial bicyclic unit then $\left\langle u_{g,h}, u'_{g^{-1}h^{-1}} \right\rangle$ is a free group of rank 2. More generally, in [MS2] it is shown that if $c \in \mathbb{Z}G$ satisfies $c^2 = 0$ and $c \neq 0$ then $\langle 1 + c^*, 1 + c\rangle$ is free group of rank 2. For $c = \sum_{g\in G} z_g g$ we denote by $c^* = \sum_{g\in G} z_g g^{-1}$. So, $*$ denotes the classical involution on $\mathbb{Z}G$. The above corollary yields many more concrete elements that can be substituted for c. Since then, as mentioned in the introduction, there have been several papers on constructing free subgroups in $\mathcal{U}(\mathbb{Z}G)$ generated by Bass and/or bicyclic units.

Acknowledgements. The authors would like to thank Capi Corrales for the help with the splitting of quaternion algebras (Lemma 4.4). The second author would like to thank for the warm hospitality during the visit to Vrije Universiteit Brussel with a postdoctoral grant of Fundación Séneca of Murcia. This paper was finished during a six month visit of the third author at the Vrije Universiteit Brussel with a grant from the Brussels Capital Region (IWOIB, Belgium) BRGEOZ152.

References

[Bas] H. Bass, *The Dirichlet unit theorem, induced characters, and Whitehead groups of finite groups*, Topology **4** (1965), 391–410.

[Bra] R. Brauer, *On Artin's L-series with general group characters*, Ann. of Math. **48** (1947), 502–514.

[CR] Ch.W. Curtis, I. Reiner, *Representation theory of finite groups and associative algebras*, Wiley-Interscience, New York, 1962.

[FGS] B. Fein, B. Gordon, J.H. Smith, *On the representation of -1 as a sum of two squares in an algebraic number field*, J. Number Theory **3** (1971), 310–315.

[GJ] A. Giambruno, E. Jespers, *Central idempotents and units in rational group algebras of alternating groups*, Internat. J. Algebra Comput. **8** (1998), 467–477.

[GP] J.Z. Gonçalves, D.S. Passman, *Embedding free products in the unit group of an integral group ring*, Arch. Math. (Basel) **82** (2004), 97–102.

[GdR] J.Z. Gonçalves, Á. del Río, *Bicyclic units, Bass cyclic units and free groups*, J. Group Theory **11** (2008), 247–265.

[GS] A. Giambruno, S.K. Sehgal, *Generators of large subgroups of units of integral group rings of nilpotent groups*, J. Algebra **174** (1995), 150–156.

[HP] B. Hartley, P.F. Pickel, *Free subgroups in the unit groups of integral group rings*, Canad. J. Math. **32** (1980), 1342-1352.

[Her] M. Hertweck, *A counterexample to the isomorphism problem for integral group rings*, Ann. of Math. (2) **154** (2001), 115–138.

[Hig] G. Higman, *Units in group rings*, Ph.D. Thesis, Univsersity of Oxford, Oxford, 1940.

[Hup] B. Huppert, *Character Theory of Finite Groups*, de Gruyer Expositions in Mathematics **25**, Walter de Gruyer, 1998.
[Jes] E. Jespers, *Units in integral group rings: a survey*, Methods in ring theory (Levico Terme, 1997), 141–169, Lecture Notes in Pure and Appl. Math., **198**, Dekker, New York, 1998.
[JL1] E. Jespers, G. Leal, *Generators of large subgroups of the unit group of integral group rings*, Manuscripta Math. **78** (1993), 303–315.
[JL2] E. Jespers, G. Leal, *Units of integral group rings of some metacyclic groups*, Canad. Math. Bull. **37** (1994), 228–237.
[JL3] E. Jespers, G. Leal, *Degree* 1 *and* 2 *representations of nilpotent groups and applications to units of group rings*, Manuscripta Math. **86** (1995), no. 4, 479–498.
[JLP] E. Jespers, G. Leal, A. Paques, *Central idempotents in rational group algebras of finite nilpotent groups*, J. Algebra Appl. **2** (2003), 57–62.
[JPS] E. Jespers, M.M. Parmenter, S.K. Sehgal, *Central units of integral group rings of nilpotent groups*, Proc. Amer. Math. Soc. **124** (1996), 1007–1012.
[JPdRRZ] E. Jespers, A. Pita, Á. del Río, M. Ruiz, P. Zalesskii, *Groups of units of integral group rings commensurable with direct products of free-by-free groups*, Adv. Math. **212** (2007), 692–722.
[JdRR] E. Jespers, Á. del Río, M. Ruiz, *Groups generated by two bicyclic units in integral group rings*, J. Group Theory **5** (2002), 493–511.
[Lam] T.Y. Lam, *The algebraic theory of quadratic forms*, W.A. Benjamin, Inc, Massachusetts, 1973.
[MS1] Z. Marciniak, S.K. Sehgal, *Constructing free subgroups of integral group ring units*, Proc. Amer. Math. Soc. **125** (1997), 1005–1009.
[MS2] Z. Marciniak, S.K. Sehgal, *Units in group rings and geometry*, Methods in ring theory (Levico Terme, 1997), 185–198, Lecture Notes in Pure and Appl. Math. **198**, Dekker, New York, 1998.
[Mos] C. Moser, *Représentation de* -1 *comme somme de carrés dans un corp cyclotomique quelconque*, J. Number Theory **5** (1973) 139–141.
[OdRS1] A. Olivieri, Á. del Río, J.J. Simón, *On monomial characters and central idempotents of rational group algebras*, Comm. Algebra **32** (2004), 1531–1550.
[OdRS2] A. Olivieri, Á. del Río, J.J. Simón, *The group of automorphisms of a rational group algebra of a finite metacyclic group*, Comm. Algebra **34** (2006), 3543–3567.
[Pas] D.S. Passman, *The algebraic structure of group rings*, John Wiley, New York, 1977.
[Rei] I. Reiner, *Maximal orders*, Academic Press, 1975.
[RS1] J. Ritter, S.K. Sehgal, *Generators of subgroups of* $U(\mathbf{Z}G)$, Contemp. Math. **93** (1989), 331–347.
[RS2] J. Ritter, S.K. Sehgal, *Construction of units in integral group rings of finite nilpotent groups*, Trans. Amer. Math. Soc. **324** (1991), 603–621.
[RS] K.W. Roggenkamp, L.L. Scott, *The isomorphism problem for integral group rings of finite nilpotent groups*, Proc. Int. Conf. St. Andrews, 1985, London Math. Soc. Lect. Notes Series **121** (1986), 291–299.
[Roq] P. Roquette, *Realisierung yon Darstellungen endlicher nilpotenter Gruppen*, Archiv. Math. **9** (1958), 241–250.
[Seh1] S.K. Sehgal, *Topics in Group Rings*, Marcel Dekker, 1978.
[Seh2] S.K. Sehgal, *Units in integral group rings*, Longman Scientific & Technical, 1993.
[Seh3] S.K. Sehgal, *Group rings*, Handbook of algebra, Vol. 3, 455–541, North-Holland, Amsterdam, 2003.
[Sho] K. Shoda, *Über die monomialen Darstellungen einer endlichen Gruppe*, Proc. Phys. Math. Soc. Jap. **15** (1933), 249-257.
[Wei] A. Weiss, *Torsion units in integral group rings*, J. Reine Angew. Math. **415** (1991), 175–187.
[Yam] T. Yamada, *The Schur Subgroup of the Brauer Group*, Lecture Notes in Math. **397**, Springer–Verlag, 1974.

Department of Mathematics, Vrije Universiteit Brussel, Pleinlaan 2, 1050 Brussels, Belgium
E-mail address: efjesper@vub.ac.be

Department of Statistics-Forecasts-Mathematics, Babeş-Bolyai University, Str. T. Mihali 58-60, 400591 Cluj-Napoca, Romania
E-mail address: gabriela.olteanu@econ.ubbcluj.ro

Departamento de Matemáticas, Universidad de Murcia, 30100 Murcia, Spain
E-mail address: adelrio@um.es